RDW Dienst Wegverkeer CPS

RDW Certification Practice Statement

RDW
Europaweg 205
2711 ER ZOETERMEER
Postbus 777
2700 AT ZOETERMEER

Oktober 2020

Pagina opzettelijk leeg gelaten.

Titel:	RDW Dienst Wegverkeer Certification Practice Statement
Versie/datum:	*16* / Oktober 2020
Autorisatie:	Directie RDW
Datum ingang:	1 oktober 2006
Onderhoud:	RDW
Classificatie:	openbaar
Aantal pagina's:	38

Inhoudsopgave

1. Inleiding 7
1.1 Algemeen 7
1.2 Documentnaam en Identificatie 7
1.3 Bij RDW-PKI betrokken partijen 7
1.3.1 Certification Authority 7
1.4 Toepasbaarheid 8
1.5 Contact gegevens 9
1.6 Definities en acroniemen 9
2. Publicatie en repository verplichtingen 9
2.1 Repository 9
2.2 Publicatie van certificaat informatie 9
2.3 Tijd of frequentie van publicatie 9
2.4 Toegangscontrols van repositories 9
3. Identificatie en authenticatie 10
3.1 Naamgeving 10
3.2 Initiële validatie van de identiteit 10
3.3 Identificatie en authenticatie voor vervanging van een certificaat 12
3.4 Identificatie en authenticatie voor verzoek tot intrekking 12
4. Operationele vereisten voor de certificaat levenscyclus 13
4.1 Certificaat aanvraag 13
4.2 Certificaat aanvraag verwerking 13
4.3 Certificaat uitgifte 13
4.4 Certificaat acceptatie 14
4.5 Sleutelpaar en certificaat toepassing 14
4.6 Certificaat heruitgifte 14
4.7 Certificaat vervanging 15
4.8 Certificaat aanpassing 15
4.9 Certificaat intrekking en suspensie 16
4.10 Certificaat status services 18
4.11 Einde van de vermelding als certificaathouder 18
4.12 Sleutel Escrow en herstel 18
5 Algemene, fysieke en operationele beheersmaatregelen 18
5.1 Fysieke beheersmaatregelen 18
5.2 Procedurele beheersmaatregelen 19
5.3 Personele beheermaatregelen 20
5.4 Audit logging procedures 20
5.5 Archivering van documenten 21
5.6 Verstrekken van RDW PKI Sleutels 21
5.7 Compromitteren van de privé-sleutel en calamiteitenbeheersing 21
5.8 CA beëindiging 22
6 Technische beveiliging 22
6.1 Genereren en installeren sleutelpaar 22
6.2 Bescherming van privésleutels 23
6.3 Overige aspecten van sleutelbeheer 24
6.4 Activeringsdata 24
6.5 Computer beveiligingsmaatregelen 24
6.6 Technische beheersmaatregelen in de levenscyclus 24

6.7 Netwerk beveiliging beheersmaatregelen 24
6.8 Tijdstempelen 25
7. Certificaat- en CRL-profiel. 25
7.1 Certificaatprofiel 25
7.2 CRL-profiel 28
7.3 OCSP-profiel 29
8 Compliance audit en overige analyses 29
8.1 Frequentie en redenen van audit 29
8.2 Identiteit/Kwaliteit van auditor 29
8.3 Relatie tussen auditor en object van audit 29
8.4 Onderwerpen van audit 29
8.5 Acties naar aanleiding van onvolkomenheid 29
8.6 Communicatie van resultaten 29
9 Overige ondernemings- en wettelijke zaken 29
9.1 Kosten 29
9.2 Financiële verantwoordelijkheid 30
9.3 Vertrouwelijkheid 30
9.4 Privacy van persoonlijke informatie 30
9.5 Intellectuele eigendomsrechten 31
9.6 Vertegenwoordiging en waarborg 31
9.7 Disclaimers van waarborgen 31
9.8 Uitsluiting van aansprakelijkheid 32
9.9 Compensatie 32
9.10 Geldigheidsduur en beëindiging 32
9.11 Individuele toelichting en communicatie met betrokkenen 32
9.12 Amendementen 32
9.13 Beslechting van geschillen 33
9.14 Toepasselijk recht 33
9.15 Positie binnen bestaande wetgeving 33
10. Formele goedkeuring 34
11. Bijlagen 35
11.1 Gebruikte afkortingen 35
11.2 Verklarende woordenlijst 35

1. Inleiding

1.1 Algemeen

Dit Certification Practice Statement is opgesteld als raamwerk voor de toepassing van certificaten die worden uitgegeven door de *"RDW Dienst Wegverkeer PKI"*.

Dit CPS beschrijft de procedures, technieken en juridische randvoorwaarden die de RDW hanteert bij het beheer van de *"RDW Dienst Wegverkeer PKI"*.

De structuur van dit CPS is in overeenstemming met de internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647).

Een verklarende woordenlijst is opgenomen als bijlage.

1.2 Documentnaam en Identificatie

De naamgeving van dit CPS is de *"RDW Dienst Wegverkeer Certification Practice Statement"*. Er is een object identifier aan dit CPS toegekend en wel 2.16.528.1.1010.2.1.6.2.

1.3 Bij RDW-PKI betrokken partijen

1.3.1 Certification Authority

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

- RDW Dienst Wegverkeer Root CA 02
- RDW Issuing CA 02
- RDW Acc Issuing CA 02

De RDW Dienst Wegverkeer Root 02 is de CA die het eerste certificaat uitgeeft binnen een certificaatketen. De RDW Dienst Wegverkeer Root CA ondertekent de certificaten van de onderliggende CA's binnen de RDW Dienst Wegverkeer PKI.
De RDW Issuing CA 02 is de CA die certificaten uitgeeft aan eindentiteiten binnen de RDW Dienst Wegverkeer PKI. Deze CA wordt in de rest van dit document de Issuing CA genoemd. De RDW Acc Issuing CA 02 is ingericht overeenkomstig de RDW Issuing CA 02 en wordt gebruikt om na een wijziging de correcte werking van de PKI te testen.

1.3.2 Registration Authority

Binnen de RDW zijn de volgende Registration Authorities actief:

Unit Rijbewijzen
voor certificaten die worden uitgegeven aan gemeenteambtenaren ten behoeve van beveiligde gegevensuitwisseling en toegang tot het rijbewijzen register.

Unit Servicecentrum Erkenningen
voor certificaten die worden uitgegeven aan (erkende) bedrijven en verzekeringsmaatschappijen ten behoeve van toegang tot RDW applicaties.
Unit Informatieverstrekking

voor certificaten die worden uitgegeven aan diverse organisaties die een relatie met de RDW hebben ten behoeve van het opzetten van een beveiligde verbinding tussen de organisatie en de RDW.

Unit Parkeren
voor certificaten die worden uitgegeven aan diverse organisaties ten behoeve van dienstverlening omtrent het Nationaal Parkeerregister.

1.3.3 Eindentiteiten

Als eindentiteiten binnen de RDW Dienst Wegverkeer PKI worden aangemerkt: aanvragers en certificaathouders. De binnen de RDW PKI operationele eindentiteiten zijn:

1 **Aanvragers**
   i. Alle gemeenteambtenaren die online toegang wensen tot RDW applicaties.
   ii. Alle organisaties die erkend zijn door de RDW of op andere wijze als klant van de RDW worden benoemd die toegang wensen tot RDW applicaties.
   iii. Alle organisaties die als klant van de RDW worden benoemd die een beveiligde verbinding met de RDW op willen zetten.
   iv. Alle RDW medewerkers die toegang wensen tot RDW applicaties.

2 **Certificaathouders**
   i. De aanvragers aan wie door de RDW een certificaat is uitgegeven.

1.3.4 Relying parties

Binnen de RDW wordt 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.

1.3.5 Overige betrokken partijen

Er zijn geen overige partijen betrokken.

1.4 Toepasbaarheid

1.4.1 Bedoelde toepassing

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

1 Productiecertificaten uitgegeven door de RDW Issuing CA 02
   De Issuing CA gebruikt zijn privésleutel uitsluitend voor het uitgeven van certificaten en het digitaal ondertekenen van CRL's zoals in dit CPS is omschreven.
   De uitgegeven productiecertificaten ten behoeve van eindentiteiten binnen de RDW PKI zijn uitsluitend bedoeld voor identificatie, authenticatie en digitale ondertekening van en door de eindentiteit ten behoeve van:
   1.1 toegang tot RDW-applicaties,
   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,
   1.3 het beveiligen van gegevensuitwisseling tussen eindentiteiten en de RDW.

2 Acceptatiecertificaten worden uitgegeven door de RDW Acc Issuing CA 02
   Acceptatiecertificaten worden uitsluitend gebruikt om te testen na een wijziging. Testen vinden nooit op de productie-omgeving plaats maar op de acceptatie-omgeving.

1.4.2 Niet toegestane toepassing

Alle toepassingen die afwijken van de genoemde toepassingen in 1.4.1 zijn niet toegestaan.

1.5 Contact gegevens

1.5.1 Verantwoordelijke organisatie

De RDW is verantwoordelijk voor het beheer van dit CPS.

1.5.2 Contactpersoon

Het volgende organisatieonderdeel is bij de RDW verantwoordelijk voor het beheer (onderhoud en interpretatie) van dit CPS.
RDW CA
Unit Cards & Brieven
Postbus 30000
9640 RA Veendam

1.5.3 Persoon die toepasbaarheid CPS bepaalt voor 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.

1.5.4 CPS instemmingprocedures

De CA en RA's hebben ingestemd met dit CPS.

1.6 Definities en acroniemen

Een lijst met gebruikte definities is opgenomen in paragraaf 11.2.

2. Publicatie en repository verplichtingen

2.1 Repository

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

2.2 Publicatie van certificaat informatie

Documenten inzake het gedetailleerde beheer van de RDW PKI worden door de RDW als vertrouwelijk bestempeld en zullen niet worden geopenbaard aan het publiek. De lijst met uitgegeven certificaten wordt niet gepubliceerd of beschikbaar gesteld aan partijen buiten de RDW.

2.3 Tijd of frequentie van publicatie

1. De Issuing CA publiceert een CRL iedere keer als een eindentiteit certificaat wordt ingetrokken en minimaal één keer per uur. Volgens de ETSI normering moet dit minimaal 1x per dag. De CRL heeft een geldigheidsduur van 7 dagen.
2. De publicatie van de CPS geschiedt volgens de bepalingen in paragraaf 9.12.
3. Indien de CPS gewijzigd wordt zullen alle entiteiten binnen de RDW PKI, met inachtneming van paragraaf 9.12 hiervan op de hoogte worden gesteld.

2.4 Toegangscontrols van repositories

Deze zijn niet van toepassing buiten de RDW, binnen de RDW zijn hiervoor interne procedures opgesteld.

3. Identificatie en authenticatie

3.1 Naamgeving

3.1.1 Type namen

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. Zie voor de certificaatprofielen paragraaf 7.1.

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 uniek identificeerbaar met de entiteit.

3.1.3 Anonimiteit of pseudonimiteit van subscribers

Niet van toepassing.

3.1.4 Regels voor het interpreteren van de naamgeving

Zie paragraaf. 3.1.1.

3.1.5 Unieke naamgeving

Alle gecertificeerde namen zijn uniek.

3.1.6 Herkenning, authenticatie en de rol van merkenrechten

Voor regels ten aanzien van merkenrechten en geschillenbeslechting ten aanzien van naamgeving geldt de procedure zoals beschreven in paragraaf 9.13 en 9.14.

3.2 Initiële validatie van de identiteit

3.2.1 Aantonen bezit van een privésleutel

De privésleutel als onderdeel van het certificaat zal na het aanvragen:

1. Persoonlijk aan de eindentiteit worden overhandigd in het geval de eindentiteit een RDW medewerker is.
2. Via beveiligd transport worden verzonden naar de 1e actuele ABR in geval de eindentiteit een ABR of RYA is (zie paragraaf 4.3). De ABR overhandigt de privésleutel persoonlijk aan de RYA.
3. Voor bedrijven die een certificaat op usb-stick aanvragen ten behoeve van toegang tot RDW-diensten wordt de usb-stick verzonden naar de RDW contactpersoon van het betreffende bedrijf.
4. Voor klanten die een smartcard aanvragen voor selfservice of een usb-stick ten behoeve van het opzetten van een beveiligde verbinding, wordt deze toegezonden aan de opgegeven contactpersoon van de betreffende organisatie.

Voor alle eindentiteiten wordt vermoed dat de entiteit binnen twee weken na verzending van het certificaat in het bezit is van de privésleutel.

3.2.2 Authenticatie van de organisatie

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 gemeente ambtenaren ten behoeve van de afgifte van rijbewijzen

De initiële authenticatie van de aanvrager door de RA vindt plaats als onderdeel van de procedure die wordt gehanteerd in het geval een gemeente in aanmerking wenst te komen

voor beveiligde gegevensuitwisseling en toegang tot het rijbewijzen register. De vaststelling van de identiteit en authenticiteit van de aanvrager geschiedt op basis van een kopie van het legitimatiebewijs, een pasfoto en ondertekening door een bevoegd persoon en de certificaathouder zelf. Een bevoegd persoon is degene die toestemming mag geven voor het aanvragen van een certificaat. In het geval van een certificaat voor een ABR is de bevoegd persoon de burgemeester van de betreffende gemeente. In het geval van een certificaat voor een RYA is de bevoegd persoon een ABR van de betreffende gemeente.

2 Authenticatie van bedrijven ten behoeve van toegang tot RDW diensten
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 RDW erkenning. De vaststelling van de identiteit en authenticiteit van de aanvrager geschiedt op basis van inschrijving in de Kamer van Koophandel en eventueel een bezoek aan het bedrijf door een toezichthouder bedrijven van de RDW.

3 Authenticatie van organisaties ten behoeve van een beveiligde verbinding met de RDW
De initiële authenticatie van de aanvrager door de RA vindt plaats als onderdeel van de procedure die wordt gehanteerd in het geval een organisatie in aanmerking wenst te komen voor een beveiligde verbinding met de RDW. De vaststelling van de identiteit en authenticiteit van de aanvrager geschiedt op basis van de kenmerken van het verzoek en beoordeling van het type organisatie. Deze organisaties kunnen kiezen voor een certificaat op smartcard waarmee via selfservice een servicecertificaat gedownload kan worden of voor een servicecertificaat op usb-stick.

4 Authenticatie van aanvragers intern de RDW
De authenticatie van de aanvragers van certificaten die uitgegeven worden aan medewerkers van de RDW, vindt plaats op basis van opdrachtverstrekking door een bevoegd persoon (manager of gemandateerde).

5. Authenticatie aanvragers NPR
De initiële authenticatie van de aanvrager door de RA vindt plaats als onderdeel van de procedure die wordt gehanteerd in het geval een organisatie in aanmerking wenst te komen voor een NPR dienstverlening. De vaststelling van de identiteit en authenticiteit van de aanvrager geschiedt op basis van de beoordeling van de RA of op aangeven van de coöperatie Servicehuis Parkeer- en Verblijfsrechten (SHPV)

3.2.3 Authenticatie van natuurlijke personen
Er worden certificaten uitgegeven aan natuurlijke personen, mits deze als medewerker verbonden zijn aan een Nederlandse gemeente of de RDW.

3.2.4 Niet-geverifieerde certificaathouder informatie
De certificaathouder verklaart de gegevens zoals die door hem verstrekt zijn aan de RDW naar waarheid te hebben opgegeven.

3.2.5 Validatie van de autoriteit
De RA controleert of de persoon of organisatie die zelf een certificaat aanvraagt of die toestemming geeft voor het aanvragen van een certificaat, hiertoe bevoegd is.

Dit betekent dat in het geval van een ABR certificaat de bevoegd persoon daadwerkelijk de burgemeester van de betreffende gemeente is. In het geval van een RYA certificaat wordt bepaald of de bevoegd persoon daadwerkelijk bekend is als ABR van de betreffende gemeente.

Wanneer het een erkend bedrijf, verzekeringsmaatschappij of gevolmachtigde betreft, moet deze als erkenninghouder of zakelijke klant geregistreerd zijn bij de RDW.
Bij een overige organisatie moet deze voldoen aan de door de RDW gestelde voorwaarden zoals vastgelegd in procedures van het betreffende organisatieonderdeel.

Voor RDW medewerkers is de bevoegd persoon de teammanager of hoofd keuringsstation of een door die personen bevoegde gemandateerde.

3.2.6 Criteria voor inter-operatie
Niet van toepassing.

3.3 Identificatie en authenticatie voor vervanging van een certificaat

3.3.1 Identificatie en authenticatie voor routinematige vervanging
Vervanging van een certificaat betekent het genereren van een nieuw sleutelpaar en certificaat voorafgaand aan het verstrijken van de geldigheidsduur van een certificaat. Bij certificaten voor gemeenteambtenaren en organisaties die selfservice uitvoeren geldt: Onverminderd de eigen verantwoordelijkheid van de certificaathouder voor het tijdig aanvragen van een nieuw certificaat, waarschuwt de RDW CA de certificaathouder tijdig voorafgaand aan het verstrijken van de geldigheidsduur van het bestaande certificaat, zodat de certificaathouder het certificaat kan vervangen conform de procedure voor initiële registratie (zie paragraaf 3.2).

In geval van certificaten voor (erkende) bedrijven, gemeenten, verzekeringsmaatschappijen, gevolmachtigden en organisaties die een servicecertificaat op usb-stick ontvangen geldt: De RDW CA vervangt het certificaat tijdig voorafgaand aan het verstrijken van de geldigheidsduur van het bestaande certificaat, zonder de certificaathouder hiervan op de hoogte te stellen anders dan door het verzenden van het nieuwe certificaat, tenzij de betreffende RA hiertoe besluit. De routinematige vervangingen zullen doorgaan zolang de certificaathouder nog als actieve gebruiker of klant bij RDW geregistreerd staat.

3.3.2 Identificatie en authenticatie voor vervanging na intrekking
Vervanging na de intrekking van een certificaat betekent het genereren van een nieuw sleutelpaar en certificaat nadat het certificaat is ingetrokken.
De RDW kan een certificaat intrekken in het kader van het toezicht op de verwerking van gegevens in het register, 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 vervanging zal dan plaatsvinden conform de procedure voor initiële registratie (zie paragraaf 3.2).Intrekking op verzoek van de certificaathouder kan worden gevolgd door een vervanging. Deze vervanging zal plaatsvinden conform de procedure voor initiële registratie.

3.4 Identificatie en authenticatie voor verzoek tot intrekking
1. De RDW kan in het kader van het toezicht op de verwerking van gegevens in het register of op de uitvoering van de wettelijke regeling(en) een certificaat intrekken.
2. De RDW kan een certificaat intrekken in het geval een eindentiteit niet langer voldoet aan de wettelijke regelingen ten aanzien van de door de RDW aan hem gestelde eisen en voorwaarden of een certificaat intrekken om procedurele en/of technische redenen.
3. De RDW kan een certificaat intrekken in het kader van de interne procedures als opgesteld voor certificaten welke vallen onder de beheersregeling(en).
4. Een eindentiteit kan ook zelf een verzoek indienen tot intrekking van zijn certificaat, bijvoorbeeld indien zijn privésleutel is gecompromitteerd.

5. Aanvragen voor intrekking moeten altijd schriftelijk, via een fax of via een e-mail bij de RA worden ingediend.

4. Operationele vereisten voor de certificaat levenscyclus

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.

4.1.1 Mogelijke aanvragers van een certificaat

Een aanvraag voor een certificaat kan worden ingediend door:
- een gemeenteambtenaar, waarbij altijd toestemming gegeven moet worden door een bevoegd persoon binnen de betreffende gemeente.
- een organisatie die erkend is door de RDW of op andere wijze als klant van de RDW wordt benoemd die toegang wenst tot RDW applicaties.
- een organisatie die als klant van de RDW wordt benoemd die een beveiligde verbinding met de RDW op wil zetten.
- een medewerker van de RDW. De uitgifte van certificaten aan medewerkers van de RDW is vastgelegd in interne procedures.

4.1.2 Registratie proces en verantwoordelijkheden

Een binnenkomende aanvraag wordt door de RA beoordeeld en geregistreerd.

4.2 Certificaat aanvraag verwerking

4.2.1 Uitvoeren identificatie en authenticatie functies

De RA beoordeelt of de aanvraag volledig is ingevuld en indien van toepassing, is ingediend met toestemming van een bevoegd persoon.

4.2.2 Goedkeuring of afwijzing van de certificaat aanvraag

Bij goedkeuring van de aanvraag zal deze verder in behandeling worden genomen door de CA. Wanneer de aanvraag wordt afgewezen, zal de RA de aanvraag tezamen met een begeleidend schrijven retour sturen.

4.2.3 Tijd voor het verwerken van de certificaat aanvraag

Een aanvraag voor een certificaat zal binnen 6 werkdagen worden afgehandeld. Indien dit niet mogelijk blijkt te zijn, zal de aanvrager hiervan op de hoogte worden gebracht door de RA.

4.3 Certificaat uitgifte

4.3.1 CA activiteiten bij certificaat uitgifte

Als onderdeel van de certificaat uitgifte voor eindentiteiten wordt een publiek / privaat sleutelpaar gegenereerd, waarna een certificaat wordt geproduceerd op basis van de publieke sleutel en de aanvraag gegevens van de entiteit. Het moment waarop de Issuing CA een certificaat aanmaakt, geldt als de datum en het tijdstip van afgifte van het certificaat en blijkt uit de logbestanden van het afgifteproces.
Na het genereren van het certificaat geeft de Issuing CA het certificaat uit. De uitgifte vindt plaats doordat het certificaat en het gegenereerde publiek / privaat sleutelpaar vastgelegd worden op een

usb-stick of een smartcard of in een pfx-bestand online beschikbaar wordt gesteld. Het sleutelpaar wordt door een Hardware Security Module (HSM) gegenereerd, de privésleutel wordt hieruit geëxporteerd en tijdelijk in een PKCS#12 opgeslagen. De usb-stick, smartcard en het pfx-bestand worden beveiligd met een pincode die na het vastleggen van het certificaat en het sleutelpaar wordt gegenereerd.

In geval van een ABR en een RYA wordt de smartcard via beveiligd transport persoonlijk afgegeven aan de 1e actuele ABR van de gemeente. In geval van een RYA is de ABR is er verantwoordelijk voor dat de aan hem verstrekte smartcard aan de juiste, op de smartcard vermelde, certificaathouder wordt afgegeven. Hiertoe zal de ABR zich, vóór afgifte van de smartcard, van de identiteit van de certificaathouder moeten vergewissen.
In geval van een organisatie die erkend is door de RDW wordt de usb-stick met daarop het clientcertificaat of de usb-stick met het servicecertificaat per post aan de geregistreerde aanvrager toegestuurd. Wanneer de organisatie zelf het servicecertificaat wil kunnen downloaden, wordt de daarvoor benodigde smartcard per post aan de geregistreerde aanvrager verzonden.

4.4 Certificaat acceptatie

4.4.1 Certificaat acceptatie

De aanvrager ontvangt het certificaat dat is vastgelegd op een smartcard of usb-stick. De aanvrager heeft bij het aanvragen van de smartcard reeds verklaard akkoord te zijn met de gebruikersvoorwaarden die van toepassing zijn op het gebruik van het certificaat. De gebruikersvoorwaarden zijn beschikbaar via de website van de RDW.
De privésleutel op de smartcard is beschermd door een initiële pincode. Voordat de smartcard wordt ontvangen, ontvangt de aanvrager de initiële pincode. Bij een certificaat op smartcard moet voor het eerste gebruik de initiële pincode door de certificaathouder worden gewijzigd.
De privésleutel op de usb-stick is beschermd door een installatie wachtwoord. Het installatie wachtwoord wordt 1 werkdag na het versturen van de usb-stick naar de aanvrager verzonden.
De privésleutel van het servicecertificaat dat gedownload wordt, is beschermd door een door de aanvrager zelf gekozen pincode.

4.4.2 Publicatie van het certificaat door de CA

Uitgegeven certificaten zullen niet door de CA worden gepubliceerd.

4.4.3 Kennisgeving van de certificaat uitgifte door de CA aan andere entiteiten

De CA zal andere entiteiten niet op de hoogte brengen van de certificaat uitgifte.

4.5 Sleutelpaar en certificaat toepassing

4.5.1 Certificaathouder privé sleutel en certificaat toepassing

De certificaathouder zorgt voor een adequate bescherming van zijn certificaat met privé sleutel en de bijbehorende pincode. De certificaathouder zal het certificaat en het hierbij behorende sleutelpaar uitsluitend gebruiken voor het doel zoals omschreven in paragraaf 1.4 (toepasbaarheid).

4.6 Certificaat heruitgifte

4.6.1 Redenen voor heruitgifte certificaat

Heruitgifte van certificaten zal niet plaats vinden.

4.6.2 Mogelijke aanvragers voor certificering van een nieuwe publieke sleutel

Niet van toepassing.

4.6.3 Verwerken aanvragen voor heruitgifte certificaat
Niet van toepassing.

4.6.4 Kennisgeving van heruitgifte certificaat aan de eindentiteit
Niet van toepassing.

4.6.5 Acceptatie van een heruitgegeven certificaat
Niet van toepassing.

4.6.6 Publicatie van het heruitgegeven certificaat door de CA
Niet van toepassing.

4.6.7 Kennisgeving van uitgifte nieuw certificaat door de CA aan andere entiteiten
Niet van toepassing.

4.7 Certificaat vervanging

4.7.1 Redenen voor vervanging certificaat
Vervanging kan plaats vinden bij wijziging van certificaatgegevens, bij naderend einde van de geldigheid, wanneer het certificaat of de pincode niet zijn ontvangen of vermist zijn.

4.7.2 Mogelijke aanvragers voor vervanging
Een aanvraag voor vervanging van een certificaat kan worden ingediend door de certificaathouder zelf (in geval van certificaathouder 2 en 3 in paragraaf 3.2.2) of door de bevoegd vertegenwoordiger van een certificaathouder (in geval van certificaathouder 1 en 4 in paragraaf 3.2.2).

4.7.3 Verwerken aanvragen voor vervanging certificaat
Het verwerken van een aanvraag voor vervanging van een certificaat zal plaatsvinden overeenkomstig de verwerking van een eerste aanvraag voor een certificaat (zie paragraaf 3.2). Dit betekent dat de RA de aanvraag voor vervanging zal beoordelen en registreren en dat de Issuing CA het vervangende certificaat uitgeeft.

4.7.4 Kennisgeving van uitgifte nieuw certificaat aan eindentiteit
De certificaathouder zal op de hoogte worden gebracht van de uitgifte van het nieuwe certificaat door het ontvangen van dit nieuwe certificaat.

4.7.5 Acceptatie van een vervangingscertificaat
Zie paragraaf 4.4.1.

4.7.6 Publicatie van het vervangingscertificaat door de CA
Uitgegeven certificaten zullen niet door de CA worden gepubliceerd.

4.7.7 Kennisgeving van uitgifte nieuw certificaat door de CA aan andere entiteiten
De CA zal andere entiteiten niet op de hoogte brengen van de certificaat uitgifte.

4.8 Certificaat aanpassing

4.8.1 Redenen voor aanpassing certificaat
Indien de inhoud van een certificaat en/of voor de inhoud van het certificaat relevante gegevens niet (meer) overeenkomen met de werkelijkheid (bijvoorbeeld na naamswijziging), moet de certificaathouder of de organisatie die voor deze certificaathouder verantwoordelijk is, dit aangeven

bij de RA middels het indienen van een verzoek tot vervanging van het certificaat. Het is de verantwoordelijkheid van de certificaathouder om de RA hiervan op de hoogte te stellen. Bij een aanpassing van de gegevens zal het volledige certificaat vervangen worden, van aanpassing van het bestaande certificaat is dus geen sprake.

4.8.2 Mogelijke aanvragers voor aanpassing van het certificaat
Niet van toepassing.

4.8.3 Verwerken aanvragen voor aanpassing certificaat
Niet van toepassing.

4.8.4 Kennisgeving van uitgifte nieuw certificaat aan de eindentiteit
Niet van toepassing.

4.8.5 Acceptatie van een aangepast certificaat
Niet van toepassing.

4.8.6 Publicatie van het aangepaste certificaat door de CA
Niet van toepassing.

4.8.7 Kennisgeving van uitgifte nieuw certificaat door de CA aan andere entiteiten
Niet van toepassing.

4.9 Certificaat intrekking en suspensie
De CA is verantwoordelijk voor de intrekking van certificaten. Intrekking vindt plaats doordat de Issuing CA het ingetrokken certificaat toevoegt aan de CRL. De certificaathouder wordt niet op de hoogte gesteld van de intrekking van het certificaat, tenzij de betreffende RA hiertoe besluit. Suspensie is niet van toepassing.

4.9.1 Redenen voor intrekking
Geldige redenen voor de intrekking van een certificaat zijn:

1. De certificaathouder of een daartoe bevoegde persoon of organisatie wenst geen gebruik meer te maken van de dienstverlening.
2. Compromittering of verlies van de privésleutel of van de pincode die in samenhang met de privésleutel toegang geven tot de RDW applicaties of een verbinding met de RDW. Na compromittering moet het gebruik van de privésleutel onmiddellijk en permanent worden gestaakt.
3. Op verzoek van de certificaathouder: bij vermissing of beschadiging van de drager van het certificaat of blokkade van de pincode.
4. Door de voor de certificaathouder verantwoordelijke organisatie, indien de houder van het certificaat niet langer namens die organisatie mag optreden bijv. na een functiewijziging of het beëindigen van het dienstverband.
5. Het door de eindentiteit niet langer voldoen aan de door de RDW aan hem gestelde eisen en voorwaarden of om procedurele en/of technische redenen.
6. De certificaathouder voldoet niet aan zijn verplichtingen zoals beschreven in dit CPS; intrekking vindt in deze situatie slechts plaats nadat de certificaathouder in de gelegenheid is gesteld zijn zienswijze daarover kenbaar te maken.

De certificaathouder is in alle gevallen aansprakelijk voor de schade die is ontstaan door het te laat intrekken of vervangen van een certificaat, ongeacht of de noodzaak tot het intrekken of vervangen aan hem kan worden toegerekend.

4.9.2 Mogelijke aanvragers voor intrekking 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. de voor een certificaathouder verantwoordelijke organisatie of gemandateerde persoon.

4.9.3 Procedure voor een verzoek tot intrekking

De entiteit die een verzoek tot intrekking van een certificaat indient kan dit alleen doen door middel van het indienen van een schriftelijk verzoek of per e-mail aan de betreffende RDW RA. In geval van certificaathouder 1 en 4 uit paragraaf 3.2.2. geldt dat bij een verzoek tot intrekking van het eigen certificaat, de RA het schriftelijke verzoek zal verifiëren door de certificaathouder terug te bellen op het bij de RA bekende telefoonnummer. Een certificaathouder die in het bezit is van een smartcard voor self-service is zelf verantwoordelijk voor het intrekken van een certificaat dat via download is verkregen.

De RA geeft onverwijld kennis van een gehonoreerd verzoek tot intrekking van het certificaat aan de CA en verzoekt met bekwame spoed van de intrekking melding te maken in de CRL. Het vermelden van de intrekking in de CRL geeft de datum en het tijdstip van intrekking van het certificaat aan.

4.9.4 Geldigheidsperiode van een verzoek tot intrekking

De RDW behandelt een verzoek tot intrekking zo spoedig mogelijk na ontvangst van het verzoek. Bij mogelijke compromittering zal de RDW, na ontvangst van het verzoek, het verzoek tot intrekking terstond afhandelen (op werkdagen).

4.9.5 Tijd waarin de CA de aanvraag voor intrekking moet verwerken

De CA verwerkt de aanvraag voor intrekking zo spoedig mogelijk, maar uiterlijk binnen 1 werkdag na ontvangst van het verzoek.

4.9.6 Vereisten voor online checken van intrekking voor relying party

Het certificaat op smartcard uitgegeven door de Issuing CA bevat een CRL Distribution Point (CDP).

4.9.7 CRL uitgifte frequentie

De CRL wordt na iedere intrekking bijgewerkt en ieder uur gedistribueerd.

4.9.8 Maximum potentieel voor CRL

De CRL is niet gebonden aan een maximum aantal.

4.9.9 Online intrekking

Niet van toepassing.

4.9.10 Vereisten voor online checken van intrekking

De server die de CRL beschikbaar stelt, is minimaal dubbel uitgevoerd op twee verschillende locaties. Deze server is 7 dagen per week en 24 uur per dag beschikbaar. De CRL is te raadplegen op: http://www-diensten.rdw.nl/crl/rdwissuingca02.crl

4.9.11 Andere vormen van publiceren intrekkingstatus

Niet van toepassing.

4.9.12 Speciale vereisten bij heruitgifte na compromittering
Niet van toepassing.

4.9.13 Redenen voor schorsing
Schorsing van het certificaat is niet mogelijk.

4.9.14 Mogelijke aanvragers voor schorsing
Niet van toepassing.

4.9.15 Procedure voor een verzoek tot schorsing
Niet van toepassing.

4.9.16 Beperkingen op de schorsingsperiode
Niet van toepassing.

4.10 Certificaat status services

4.10.1 Operationele kenmerken
De status van een certificaat is alleen opvraagbaar wanneer er sprake is van intrekking. Afgezien van de CRL vindt publicatie van de status niet plaats.

4.10.2 Beschikbaarheid van de service
Zie paragraaf 4.9.10.

4.10.3 Operationele eigenschappen
Niet van toepassing.

4.11 Einde van de vermelding als certificaathouder
Na intrekking van het certificaat is men niet meer als certificaathouder aan de Issuing CA verbonden.

4.12 Sleutel Escrow en herstel

4.12.1 Sleutel escrow en herstel beleid
Er vindt geen escrowing plaats van privé sleutels van CA of eindentiteiten.

4.12.2 Sessie sleutel inkapseling en herstel beleid en praktijk
Niet van toepassing.

5 Algemene, fysieke en operationele beheersmaatregelen

5.1 Fysieke beheersmaatregelen
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 Issuing 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 bevindingen zullen worden gepubliceerd in het RDW jaarverslag.

Fysieke toegang wordt alleen verleend aan personen die verantwoordelijk zijn voor het aanmaken van certificaten. Deze personen zijn werkzaam bij de RDW en in het bezit van een certificaat om afgifte van certificaten aan eind-entiteiten mogelijk te maken. De ruimte waarin de certificaten worden aangemaakt is afgesloten.
De server(s) waarop het certificaat management systeem en de Issuing CA staan, staan in een fysiek beveiligde computerruimte voorzien van noodstroom, airconditioning, brandmelder, brandblusinstallatie enz. De RDW Dienst Wegverkeer Root CA 02 staat offline op een appliance, de appliance staat in een high secure ruimte en kan alleen opgestart worden met meerdere passen en meerder personen waaronder een auditor. Passen liggen verspreid over meerdere kluizen.

De smartcards die nodig zijn voor het beheer van de CA's zijn gekoppeld aan personen. De back-up van de Issuing CA is versleuteld en wordt op twee externe RDW-locaties bewaard. De back-up van de RDW Dienst Wegverkeer Root CA 02 wordt in versleutelde vorm op een externe locatie in een beveiligde ruimte in een kluis bewaard.

5.2 Procedurele beheersmaatregelen

Onderstaande rollen worden onderscheiden:

1. Eigenaar van de RDW Dienst Wegverkeer PKI
2. PKI-administrator belast met het technisch beheer van de PKI-omgeving inclusief het Certificaat Management Systeem
3. CA smartcardhouders, van de smartcards waarover het sleutelmateriaal van de RDW Dienst Wegverkeer Root CA en Issuing CA is verdeeld (split key)
4. Security Manager
5. IT-auditor; voert in opdracht van de eigenaar c.q. directie IT-audits uit op de RDW Dienst Wegverkeer PKI
6. Medewerkers belast met het functioneel beheer van het certificaat management systeem incl. het toekennen van autorisaties
7. Kwaliteitsmedewerkers belast met de noodzakelijke operationele controles

Voor het uitvoeren van onderstaande acties zijn minimaal 3 personen noodzakelijk, ieder met een eigen smartcard die benodigd is. Dit betreft:

1. inrichten en door de RDW Dienst Wegverkeer Root CA signen van een onderliggende Issuing CA
2. starten van de PKI-services (booten)
3. terugzetten van de back-up van het sleutelmateriaal
4. laden van het sleutelmateriaal van de admin smartcards in een (nieuwe) HSM

Voor alle niet hiervoor genoemde beheerhandelingen zijn minimaal 2 personen noodzakelijk (dual control), waarvan 1 PKI-administrator en 1 getuige. Voor het uitvoeren van deze handelingen is een administrator certificaat noodzakelijk. Dit certificaat wordt bewaard op een cryptotoken. De procedure voor gebruik van dit administrator certificaat borgt dat altijd twee personen aanwezig zijn.

In het certificaat management systeem worden de volgende rollen onderscheiden:

1. PKI-administrator, belast met het technisch beheer van het certificaat management systeem.

2. RA medewerker, verantwoordelijk voor beoordelen van aanvragen, registreren van organisatie en/of persoonsgegevens, aanmaken van verzoeken voor certificaatuitgifte en certificaatintrekking.
3. CA medewerker, verantwoordelijk voor uitgifte en intrekking van certificaten en verzending van certificaten en pincodes.
4. Functioneel beheerder, verantwoordelijk voor functioneel beheer van het certificaat management systeem.
5. Operator, verantwoordelijk voor het aanmaken van usb-stick met certificaten.
6. Helpdeskmedewerker, heeft toegang tot het raadplegen van gegevens van certificaathouders en ingetrokken certificaten.

5.3 Personele beheermaatregelen

Alle medewerkers die een rol invullen genoemd in paragraaf 5.2 hebben voldoende kennis en ervaring om de opgedragen taken adequaat in te vullen en hebben een geheimhoudingsverklaring ondertekent. Via contracten en toezicht wordt geborgd dat bovenstaande ook geldt voor personeel van betrokken leveranciers.

5.4 Audit logging procedures

5.4.1 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 eindentiteit werd geauthentiseerd
  – aanpassing van persoonlijke gegevens van een certificaathouder
  – de generatie van een publiek / privaat sleutelpaar voor een eindentiteit
  – 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, back-up, recovery en vernietiging
  – beveiligingsrelevante gebeurtenissen rond de gebruikte HSM, 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
- Beveiligingsrelevante gebeurtenissen bij het certificaat management systeem
  – succesvolle en geweigerde aanlogpogingen
  – opvoeren gebruikers en opvoeren en wijzigen van autorisaties en alle beveiligingsrelevante parameters en instellingen

Gebeurtenissen gaan vergezeld met elementen waaruit het volgende kan worden afgeleid:
– datum en tijd van de gebeurtenis
– identiteit van de bron die de gebeurtenis veroorzaakt
– identiteit van de bron die de gebeurtenis logt

De logs worden twee jaar bewaard. Audit logs zijn beschermd tegen ongeautoriseerde inzage, wijziging, verwijdering en vernietiging door gebruik te maken van een combinatie van fysieke en logische toegangsbeveiliging. Van de digitale audit logs wordt een back-up gemaakt.

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

In het kader van de beoordeling van de audit logs 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.

5.5 Archivering van documenten

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.

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 eindentiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

Alle gebeurtenissen zoals beschreven in paragraaf 5.4.1 worden voorzien van een tijdsmarkering.

Alle gearchiveerde gebeurtenissen worden intern opgeslagen.

De zaken genoemd in paragraaf 5.4.1 worden periodiek gecontroleerd op integriteit. Deze controles vinden jaarlijks plaats in het kader van de reguliere IT-audit.

5.6 Verstrekken van RDW PKI Sleutels

De publieke sleutels die deel uit maken van de RDW PKI (trust certificaten) worden bij het aanmaken van de drager van het certificaat hieraan toegevoegd. Bij een eventuele wijziging van de publieke sleutels is paragraaf 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 Dienst Wegverkeer Root CA of Issuing CA. Dit betekent dat er een tijdstip ontstaat dat de certificaten van de bovenliggende CA's nog wel geldig zijn, maar dat er geen nieuwe eindentiteit certificaten kunnen worden uitgegeven. Tijdig voor dit tijdstip zal de RDW zorg dragen dat de betreffende CA sleutels worden vervangen. 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.

5.7 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 eindentiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

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.

In geval van compromittering van de privésleutel van de RDW Dienst Wegverkeer Root CA of de Issuing CA zal de RDW zich inspannen om zo spoedig mogelijk alle entiteiten binnen de RDW PKI in te lichten. De eindgebruiker moet het gebruik van de openbare sleutel van de Issuing CA dan onmiddellijk en permanent staken.
In geval van compromittering of verlies van de privésleutel van een eindentiteit zal deze zo spoedig mogelijk een verzoek tot intrekking van het certificaat indienen bij de RA.

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 eindentiteit of de organisatie waar deze toe behoort. Kennisgeving zal slechts plaatsvinden indien de RDW dit noodzakelijk acht.

5.8 CA beëindiging

Bij beëindigen van de Issuing CA's activiteiten draagt deze CA zorg voor de volgende handelingen:
1. De Issuing CA informeert de RDW Dienst Wegverkeer Root CA van het voornemen om haar activiteiten als CA te staken,
2. De CA stelt alle entiteiten binnen de RDW PKI op de hoogte van haar voornemen om haar activiteiten als Issuing CA te staken, minimaal 60 werkdagen voorafgaand hieraan.
3. Alle niet verlopen certificaten uitgegeven door de Issuing CA worden ingetrokken conform de procedures genoemd in paragraaf 4.9.
4. De CA dient een verzoek in ter intrekking van het Issuing CA certificaat bij de RDW Dienst Wegverkeer Root CA.

6 Technische beveiliging

6.1 Genereren en installeren sleutelpaar

6.1.1 Genereren sleutelpaar

1. De sleutelparen van de CA's binnen de RDW PKI worden in een HSM gegenereerd en bewaard.
2. De sleutelparen van de eindentiteiten worden in een HSM gegenereerd en tijdelijk opgeslagen in een database als PKCS#12 bestand. Nadat de sleutelparen op de usb-stick of de smartcard zijn gezet, worden deze in de database gewist.

6.1.2 Aflevering van privésleutel aan eindentiteit

Zie paragraaf 3.2.1. De privésleutel is beveiligd met een initiële pincode die minimaal een dag voor het verzenden van de smartcard of minimaal 1 dag na het verzenden van de usb-stick, per post aan de eindentiteit zal worden toegestuurd. De initiële pincode is voor de RDW niet zichtbaar en niet reproduceerbaar.

6.1.3 Aflevering van publieke sleutel aan de CA

Niet van toepassing. Eindentiteiten hoeven hun publieke sleutel niet naar de CA te sturen.

6.1.4 Aflevering van de publieke sleutel van de CA aan eindentiteiten

De publieke sleutel van de CA wordt op dezelfde wijze afgeleverd als de privésleutel van de eindentiteit.

6.1.5 Sleutellengten

Zie paragraaf 7.1.

6.1.6 Parameters ten behoeve van het genereren van publieke sleutels en controle kwaliteit

Zie paragraaf 7.1

6.1.7 Gebruik publieke sleutels

De publieke sleutel behorende bij het certificaat van een eindentiteit is uitsluitend bestemd voor doelen zoals beschreven in paragraaf 1.4.1. In de extensie van het certificaat zijn deze doelen vastgelegd.

6.2 Bescherming van privésleutels

1. Algemeen
   1.1 De RDW Dienst Wegverkeer Root CA en de Issuing CA zorgen voor adequate bescherming van de privésleutels.
   1.2 Het genereren, beschermen en eventueel vernietigen van CA privésleutels vindt plaats door middel van een HSM, volgens FIPS 140-2 level 3 of gelijkwaardig. Toegang is alleen mogelijk met behulp van de sleutelparen op minimaal 2 uit 8 smartcards.
   1.3 De CA privésleutels worden gegenereerd in de cryptografische module (HSM) waarin ze worden gebruikt. Slechts in het geval van recovery is er sprake van invoer van een privésleutel. 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. De privésleutel komt nooit buiten de HSM. Hiertoe dienen naast de PKI administrator en een getuige minimaal drie CA smartcardhouders aanwezig te zijn. FIPS level 3 of gelijkwaardig blijft altijd gewaarborgd.
   1.4 Privésleutels van de CA's worden alleen vernietigd bij het beëindigen van de dienstverlening van de RDW Dienst Wegverkeer Root CA. Dit vindt plaats door de HSM's te initialiseren en alle back-ups te vernietigen. Hiervan zal een protocol worden opgesteld onder toezicht van een getuige.
   1.5 Beheer van privésleutels van CA's is slechts mogelijk in de fysieke aanwezigheid van minimaal drie daartoe geautoriseerde RDW PKI medewerkers. Zie paragraaf 5.2.
   1.6 Er vindt geen escrowing van privésleutels van CA of eindentiteiten plaats.
   1.7 Van CA privésleutels is een back-up gemaakt in versleutelde vorm, die alleen weer teruggezet kan worden met behulp van drie CA smartcardhouders waarvan 1 PKI administrator.
2. Eindentiteit
   2.1 De eindentiteit is exclusief verantwoordelijk voor het beschermen van zijn privésleutel, zoals deze op de drager van het certificaat staat, door middel van een pincode. De privésleutel van de eindentiteit kan gebruikt worden op het moment dat de juiste pincode is ingevoerd. De eindentiteit dient de drager van het certificaat zorgvuldig te bewaren en de pincode geheim te houden. Verlies, mogelijke compromittering of beschadiging van de drager van het certificaat of bijbehorende pincode of beëindiging van functie dient terstond aan de RA te worden gemeld (zie paragraaf 1.5.2).
   De pincode is willekeurig en bestaat voor certificaten op smartcard uit 5 cijfers, voor clientcertificaten op usb-stick uit 6 cijfers, voor download servicecertificaten uit 8 cijfers en voor servicecertificaten op uit 10 cijfers, waarbij gekozen wordt uit de cijfers 0 tot en met 9.
   2.2 Vernietigen van de privésleutels van eindentiteiten kan alleen door de certificaathouder zelf worden uitgevoerd, door het feitelijk vernietigen van de usb-stick of smartcard.

2.3 Van de privésleutel van de eindentiteiten wordt geen back-up gemaakt.
2.4 De privésleutels van eindentiteiten worden niet opgeslagen in de cryptografische module, maar op de usb-stick of smartcard voor eindentiteiten.

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 eindentiteiten worden gearchiveerd.

6.3.2 Periode van gebruik sleutels

1. De geldigheidsduur van het RDW Dienst Wegverkeer Root CA certificaat bedraagt 15 jaar.
2. De geldigheidsduur van het Issuing CA certificaat bedraagt 15 jaar.
3. De geldigheidsduur van het certificaat van een eindentiteit op een smartcard bedraagt 5 jaar.
4. De geldigheidsduur van het certificaat van een eindentiteit op een usb-stick of gedownload bedraagt 2 jaar.

6.4 Activeringsdata

6.4.1 Generatie en installatie

De privésleutels van eindentiteiten zijn beveiligd door een pincode op het PKCS#12 bestand en na plaatsing op de usb-stick of smartcard door de pincode van de usb-stick of smartcard. Eindentiteiten dienen bij de eerste ingebruikname van de smartcard hun privésleutels te beveiligen met een door hen zelf te kiezen pincode. Ook een gedownload servicecertificaat dient te worden beveiligd middels een zelfgekozen pincode.

6.4.2 Bescherming van activeringsdata

De pincode die dient ter beveiliging van de privésleutel dient uniek en onvoorspelbaar te zijn en van een zodanige lengte zodat deze in verhouding staat met de sleutel die beveiligd wordt. De pincode van certificaten op smartcard moet uit 5 karakters bestaan. De pincode van clientcertificaten op usb-stick moet uit 6 karakters bestaan. Voor download servicecertificaten geldt 8 karakters en voor servicecertificaten op usb-stick 10 karakters. Deze karakters kunnen zijn: de cijfers 0 t/m 9.
De initiële pincode behorende bij de usb-stick of smartcard voor een eindentiteit wordt uitsluitend geprint op een pinmailer en afzonderlijk van de usb-stick of smartcard naar de certificaataanvrager gezonden.

6.5 Computer beveiligingsmaatregelen

De specifieke technische beveiligingsmaatregelen zijn beschreven in interne procedures van de RDW. Computersystemen worden ingericht en beheerd conform procedures die waarborgen dat het vereiste beveiligingsniveau wordt geborgd.

6.6 Technische beheersmaatregelen in de levenscyclus

OTAP-, Change- en Securitymanagement procedures borgen dat bij wijzigingen het vastgestelde beveiligingsniveau blijft gehandhaafd.

6.7 Netwerk beveiliging beheersmaatregelen

Beveiligingsmaatregelen op netwerkniveau borgen dat toegang tot de CA-server alleen mogelijk is voor geautoriseerde protocollen en vanaf expliciet geautoriseerde werkplekken en servers.

6.8 Tijdstempelen

Niet van toepassing.

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:

Inhoud RDW Dienst Wegverkeer Root CA certificaat

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Dienst Wegverkeer Root CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	15 jaar
Keylength	4096
Subject Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Dienst Wegverkeer Root CA 02 RDW Groningen NL
CDP	nvt
Subject Key Identifier (SKI)	keyIdentifier
Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Basic Constraint (Critical) CA Pathlength	 True 1
Public key	RSA 4096 bits
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

Inhoud RDW Issuing CA 02 certificaat

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Dienst Wegverkeer Root CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	15 jaar
Keylength	4096
Subject Common Name (CN) Organisation (O)	 RDW Issuing CA 02 RDW

Locality (L) Country (C)	Groningen NL
CDP	http://www-diensten.rdw.nl/crl/RDWDienstWegverkeerRootCA02.crl
Subject Key Identifier (SKI)	keyIdentifier
Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Basic Constraint (Critical) CA Pathlength	 True 0
Public key	RSA 4096 bits
Key Usage (Critical)	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

Inhoud van certificaten van RDW-medewerkers op smartcard (RDW Smartcard Intern)

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Issuing CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	5 jaar
Keylength	2048
Subject Common Name (CN) Organisation (O) Country (C)	 <initials + lastname > RDW NL
CDP	n.v.t.
Subject Key Identifier (SKI)	keyIdentifier
Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Public key	RSA 2048 bits
Key Usage (Critical)	Digital Signature, Key encipherment, Data encipherment, Key agreement (b8)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

Inhoud certificaten van eindentiteiten op smartcard (RDW Smartcard)

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Issuing CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	5 jaar
Keylength	2048
Subject Common Name (CN) Organisation (O) Country (C) Serial Number	 <initials + lastname > <Organization name> NL <BSN>
CDP	http://www-diensten.rdw.nl/crl/rdwissuingca02.crl
Subject Key Identifier (SKI)	keyIdentifier

Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Public key	RSA 2048 bits
Key Usage (Critical)	Digital Signature, Key encipherment, Data encipherment, Key agreement (b8)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

Inhoud clientcertificaten van eindentiteiten op usb-stick (RDW Client)

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Issuing CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	2 jaar
Keylength	2048
Subject Common Name (CN) Organisation (O) Country (C)	 RDW Diensten - <KVK><CRWAM-CODE> <Organisatie ID (rdw-nl-id)> NL
CDP	n.v.t.
Subject Key Identifier (SKI)	keyIdentifier
Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Public key	RSA 2048 bits
Key Usage (Critical)	Digital Signature, Key encipherment, Data encipherment (b0)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

Inhoud servicecertificaten van eindentiteiten op usb-stick (RDW Services)

Versie	V3
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Issuing CA 02 RDW Groningen NL
SERIALNUMBER	Positive Integer (b.v. 00 c5 c8 4e 05 0a 27 36 dc 99 8a 1d 21 e5 66 e8 3e)
Life time	2 jaar
Keylength	2048
Subject Common Name (CN) Organisation (O) Organizational Unit (OU) Serial Number Country (C)	 <RDW Service> <Company of Organisation Name> <Department Name> <Organization ID> NL
CDP	n.v.t.
Subject Key Identifier (SKI)	keyIdentifier
Authority Key Identifier (AKI)	keyIdentifier (gelijk aan de SubjectKeyIdentifier)
Public key	RSA 2048 bits
Key Usage (Critical)	Digital Signature, Key encipherment, Data encipherment (b0)
Certificate Policy	OID::= 2.16.528.1.1010.2.1.6.2

7.1.1 Versie nummers
De CA genereert X.509 versie 3 certificaten.

7.1.2 Certificaat extensies
De certificaten binnen de RDW PKI bevatten X.509v3-extensies. Zie paragraaf 7.1.

7.1.3 Algoritme object identifiers
Niet van toepassing.

7.1.4 Vormen van de naamgeving
Zie paragraaf 3.1 en verder.

7.1.5 Beperkingen aan de naamgeving
Zie paragraaf 3.1 en verder.

7.1.6 Certificaat beleid object identificatie
Niet van toepassing.

7.1.7 Gebruik van beleid beperkingen extensie
Deze extensie wordt niet gebruikt.

7.1.8 Beleid beperkingen syntaxis en betekenis
Niet van toepassing.

7.1.9 Betekenis voor de afhandeling van kritieke certificaat beleid extensie
Niet van toepassing.

7.2 CRL-profiel

Versie	V2
Issuer Distinguished Name Common Name (CN) Organisation (O) Locality (L) Country (C)	 RDW Issuing CA 02 RDW Groningen NL
Signature Algoritme	Sha256WithRSAEncryption
Signature	Sha256
thisUpdate	Ingangsdatum
nextUpdate	7 dagen later
revokedCertificates	Lijst met ingetrokken serienummers
cRLNumber	01 (= oplopend nummer voor opvolgende CRL's)
authorityKeyIdentifier	De SKI van de CSCA
CRL Expire Period	7 dagen
CRL issue interval	1 uur
CRL overlap time	0
Delta CRL Period	0

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.

7.3 OCSP-profiel

Niet van toepassing.

8 Compliance audit en overige analyses

8.1 Frequentie en redenen van audit

Jaarlijks vindt een audit plaats waarbij wordt nagegaan of de bepalingen in dit CPS door de CA en RA worden nageleefd.

8.2 Identiteit/Kwaliteit van auditor

De audit zal worden uitgevoerd door een onafhankelijke IT-Auditor (RE).

8.3 Relatie tussen auditor en object van audit

De auditor zal volledig onafhankelijk zijn en op geen enkele wijze verbonden zijn aan de partij die het voorwerp is van de audit.

8.4 Onderwerpen van audit

De naleving van dit CPS en de bijbehorende procedures en technieken in opzet, bestaan en werking zijn het object van de audit.

8.5 Acties naar aanleiding van onvolkomenheid

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. Nadat herstel van de onvolkomenheden of gebreken heeft plaatsgevonden zal er opnieuw een audit plaatsvinden.

8.6 Communicatie van resultaten

De relevante resultaten van de audit zijn terug te vinden in het jaarverslag van de RDW.

9 Overige ondernemings- en wettelijke zaken

9.1 Kosten

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

9.2 Financiële verantwoordelijkheid

9.2.1 Vrijwaring door relying parties
Niet van toepassing.

9.2.2 Vertrouwde relaties
Niet van toepassing.

9.2.3 Administratieve procedures
Niet van toepassing.

9.3 Vertrouwelijkheid

9.3.1 Vertrouwelijke informatie
Onder vertrouwelijke informatie wordt verstaan:

1.1. persoonsgegevens,
1.2. correspondentie met eindentiteiten
1.3. privésleutels en de hierbij behorende pincodes,
1.4. gegevens over de certificaathouder zoals de RDW die registreert,
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.

9.3.2 Niet vertrouwelijke informatie
Als niet vertrouwelijke informatie wordt alle overige informatie aangemerkt.

9.3.3 Verantwoordelijkheid om vertrouwelijke informatie te beschermen
Vertrouwelijke informatie wordt niet vrijgegeven, tenzij hiertoe een wettelijke plicht bestaat.

9.4 Privacy van persoonlijke informatie

9.4.1 Privacy plan
De verwerking van persoonsgegevens door de RA en de Issuing CA geschiedt conform de Wet bescherming persoonsgegevens.

9.4.2 Informatie gekwalificeerd als privé
Certificaathouders die inzage wensen in hun organisatie- of persoonsgegevens, dienen hiertoe een verzoek in te dienen bij de RDW. Het verzoek dient schriftelijk naar de RA te worden gestuurd.

9.4.3 Informatie niet gekwalificeerd als privé
Alle informatie die niet gerelateerd is aan de organisatie- of persoonsgegevens van certificaathouders.

9.4.4 Verantwoordelijkheid om privé informatie te beschermen
De RDW is verantwoordelijk voor het beschermen van privé informatie.

9.4.5 Signaleren en goedkeuren gebruik privé informatie
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.

9.4.6 Overige redenen voor vrijgeven van informatie

Niet van toepassing.

9.5 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.

9.6 Vertegenwoordiging en waarborg

9.6.1 CA vertegenwoordiging en waarborgen

De CA garandeert zijn dienstverlening uit te voeren conform dit CPS. De CA verklaart dat de informatie in het certificaat correct is, voor zover deze bij de CA bekend is.

9.6.2 RA vertegenwoordiging en waarborgen

De RA en de namens de RA optredende organisatieonderdelen garanderen hun dienstverlening uit te voeren conform dit CPS. De RA verklaart dat een certificaat niet wordt uitgereikt zonder een aanvraag daartoe. De RA verricht de noodzakelijke validatie- en authenticatieprocedures en zal hierbij de gegevens in de certificaataanvraag, die de RA heeft ontvangen van de aanvrager, correct weergeven.

9.6.3 Eindentiteit vertegenwoordiging en waarborgen

De eindentiteit dient het aanvraagformulier naar waarheid in te vullen, de smartcard strikt persoonlijk te gebruiken en de usb-stick alleen voor de aanvragende organisatie. De certificaathouder is aansprakelijk voor schade voortvloeiend uit aan hem toerekenbaar handelen in strijd met zijn verplichtingen zoals beschreven in paragraaf 1.4.

9.6.4 Relying party vertegenwoordiging en waarborgen

De RDW als relying party is verplicht na te gaan of een eindentiteit certificaat geldig is, door:

- Verificatie van de digitale handtekening op het eindcertificaat en van de certificaten in het certificatie pad waaronder het eindcertificaat is afgegeven.
- Verificatie dat het eindcertificaat niet ingetrokken is door gebruik te maken van een geldige CRL verstrekt door de RDW, zie paragraaf 2.3.

De relying party accepteert door het gebruik van een RDW eindentiteit certificaat de limitering van aansprakelijkheid en garanties zoals beschreven in dit CPS, alsmede de bepalingen uit de gebruikersvoorwaarden en de overige bij de uitreiking van het certificaat verstrekte informatie. De relying party vertrouwt er op dat de informatie zoals deze in het certificaat is opgenomen, correct is.

9.6.5 Vertegenwoordiging en waarborgen van andere betrokkenen

Niet van toepassing.

9.7 Disclaimers van waarborgen

Expliciete waarborgen zullen niet worden gegarandeerd.

9.8 Uitsluiting van aansprakelijkheid

De 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 paragraaf 1.4). De RDW is niet aansprakelijk voor vertraging en gebreken in de uitvoering van de werkzaamheden die te wijten zijn aan (technische) storingen zoals transmissiefouten, storingen aan apparatuur en systeemprogrammatuur, defecten in de apparatuur en programmatuur, opzet zoals fraude, illegaal gebruik van programmatuur, sabotage, diefstal van gegevens en bedieningsfouten door derden, fouten van derden met als gevolg netwerkuitval, stroomuitval, brand, blikseminslag, aanzienlijke waterschade, een breuk in een telefoonkabel, oorlogsgeweld of natuurrampen en meer in het algemeen oorzaken die niet de redelijk in acht te nemen zorg van de RDW betreffen.

9.9 Compensatie

In het geval schade geleden wordt door een derde partij, zal op basis van de bepalingen in dit CPS worden bepaald wie hiervoor verantwoordelijk gesteld moet worden. Indien dit niet mogelijk is, zal de bevoegde rechtbank te Groningen uitspraak doen.

9.10 Geldigheidsduur en beëindiging

9.10.1 Geldigheidsduur

Zie paragraaf 7.1.

9.10.2 Beëindiging

Na het verstrijken van de geldigheidsduur zal het certificaat worden beëindigd. De certificaathouder zal tijdig op de hoogte worden gesteld van het bereiken van het einde van de geldigheidsduur.

9.10.3 Effect van beëindiging en voortbestaan

Bij beëindiging van het certificaat van een eindentiteit, heeft deze de mogelijkheid om middels het aanvragen van een vervangend certificaat te kunnen voortbestaan als certificaathouder.

9.11 Individuele toelichting en communicatie met betrokkenen

Wanneer een individuele toelichting gewenst is, kan contact worden opgenomen met de CA (zie paragraaf 1.5).

9.12 Amendementen

9.12.1 Procedure voor amendement

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 organisatieonderdelen van de RDW aan wie de uitvoering van de CA of RA taken conform dit CPS is opgedragen dan wel organisatieonderdelen ten behoeve waarvan de Issuing CA 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 voor inwerkingtreding voorafgaande in kennis stelling 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 RDW bekend is gemaakt door publicatie op de internetsite van de RDW.

9.12.2 Kennisgevingmechanisme en periode

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 op de internetsite van de RDW.

9.12.3 Omstandigheden waaronder Oject Identifier veranderd moet worden

Voor wat betreft wijziging van bepalingen van het CPS die geen materiële 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.

9.13 Beslechting van geschillen

Alle geschillen voortvloeiend uit of verband houdend met CPS en/of gebruikersvoorwaarden worden beslecht door de bevoegde rechtbank te Groningen. Alvorens een geschil voor te leggen aan de bevoegde rechtbank zullen partijen proberen om samen in goed overleg tot een oplossing te komen.

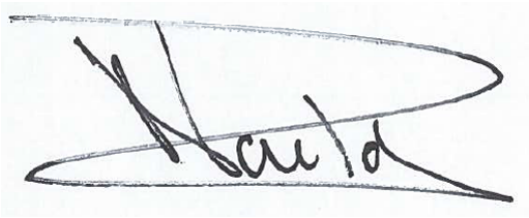
9.14 Toepasselijk recht

Op de bepalingen in dit CPS en op de RDW gebruikersvoorwaarden is Nederlands recht van toepassing. 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.

9.15 Positie binnen bestaande wetgeving

Alle betrokken partijen binnen de RDW-PKI dienen zich te houden aan specifieke wetgeving met betrekking tot PKI's zoals deze is opgenomen in het Nederlands recht.

10. Formele goedkeuring



Akkoord directeur RDW:

Datum: 14.12.2020

11. Bijlagen

11.1 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

11.2 Verklarende woordenlijst

Aanvrager
Een entiteit die een certificaat aanvraagt bij een RA.

ABR
Autorisatie Bevoegd medewerker Rijbewijzen, certificaathouder die bevoegd is om andere medewerkers die in het bezit zijn van een ABR of RIJA smartcard te autoriseren voor toegang tot RDW systemen.

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 eindentiteit 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 identiteitvan deze entiteit en dat de geldigheid van de corresponderende privésleutel aanduidt. Een certificaat biedt waarborgen omtrent de identiteit van eindentiteiten door het gebruik van een gegenereerd sleutelpaar bestaande uit een privésleutel en een publieke sleutel. Deze gewaarborgde identiteit wordt onder meer gebruikt bij het vaststellen van bevoegdheden bij elektronische (data)communicatie.

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

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

Certificaathouder
De eindentiteit, CA of RA die in het bezit is van de privésleutel 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 eindentiteiten, certificaten van CA's die de certificaten van eindentiteiten 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 eindentiteit die aanvragen doet bij de webserver.

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

Distinguished name
Een set van gegevens die een eindentiteit identificeren.

Eindentiteit
Een certificaathouder of een aanvrager, die geen CA of RA is.

Gebruikersvoorwaarden
Document met de verplichtingen voor de eindentiteit die als geaccepteerd wordt beschouwd zodra het certificaat wordt aangevraagd.

Genereren van een sleutelpaar
Het proces van het creëren van een publieke en privésleutel.

Identificatie
Het proces ter bevestiging van de identiteit van een eindentiteit.

Object identifier
Een uniek nummer dat gekoppeld kan worden aan dit CPS.

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

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

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 eindentiteiten. 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 online 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.

RYA
Medewerker Rijbewijs Afgifte, wordt door de ABR geautoriseerd voor het verkrijgen van toegang tot RDW systemen ten behoeve van afgifte van rijbewijzen.

Service certificaat
Een RDW-certificaat gekoppeld aan een server om zekerheid te geven omtrent de identiteit van de server van de wederpartij.

Sleutelpaar
Een publieke sleutel en een hierbij behorende privésleutel.

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).

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.