

KPN TELECOM

CERTIFICATION PRACTICE STATEMENT  
VOOR  
KLASSE 3 SERVER CERTIFICATEN

IN SAMENWERKING MET  
VERISIGN™

VERSIE 1.0  
DATUM VAN PUBLICATIE: 30 APRIL 1999

ALLE RECHTEN VOORBEHOUDEN

**© KPN Telecom BV en VeriSign, Inc. (1999)**

**Alle rechten voorbehouden**

**Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de rechthebbende. Het vorenstaande is eveneens van toepassing op gehele of gedeeltelijke bewerking.**

**De rechthebbende is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor kopiëren als bedoeld in artikel 17, tweede lid, Auteurswet 1912 en het K.B. van 20 juni 1974 (Stb.351) zoals gewijzigd bij het K.B. van 23 augustus 1985 (Stb.471) ex artikel 16b Auteurswet 1912, te innen en/of daartoe in en buiten rechte op te treden.**

**Voor het overnemen van delen van deze uitgave ex artikel 16 Auteurswet 1912 dient men zich tot de rechthebbende te wenden.**

**© KPN Telecom BV and VeriSign, Inc (1999)**

**All rights reserved.**

**No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without the prior written permission from the publisher.**

# OVERZICHT BELANGRIJKSTE ONDERDELEN CPS

---

**Dit overzicht is incompleet in die zin, dat in de CPS nog verschillende andere zaken worden beschreven die voor certificaathouders danwel derde partijen van belang (kunnen) zijn en waarvan zij zich op de hoogte dienen te stellen. Voor nadere details wordt derhalve verwezen naar de volledige tekst van deze CPS.**

---

## 1. Doelstelling CPS

Deze Certification Practice Statement (CPS) regelt de toepassing en het gebruik van klasse 3 server certificatie diensten door KPN Telecom – waaronder:

- certificaataanvragen
- validatie van aanvragen
- uitgifte en acceptatie van certificaten
- gebruik van certificaten
- blokkering en intrekking van certificaten

## 2. Kennisniveau gebruiker

Het wordt de gebruiker aangeraden om zich op adequate wijze op de hoogte te stellen van de werkwijze, toepassingen en gebruiksmogelijkheden van een Public Key Infrastructuur (PKI) alvorens een klasse 3 server certificaat aan te vragen bij KPN Telecom. Documentatie-, trainings- en opleidingsmateriaal met betrekking tot digitale handtekeningen, certificaten en de Public Key Infrastructuur zijn verkrijgbaar bij KPN Telecom.

## 3. Server software geschikt voor digitale sleutels

Tijdens het aanvragen van een klasse 3 server certificaat moet de gebruiker met behulp van zijn server software een digitaal sleutelpaar genereren. Om van de in deze CPS beschreven diensten gebruik te kunnen maken, is het derhalve noodzakelijk dat de gebruikte server software in een dergelijke functionaliteit voorziet (hetgeen onder andere het geval is bij Microsoft IIS 3.0 en hoger, Netscape Enterprise 3.0 en hoger en bij Lotus Domino 4.6.2 en hoger).

## 4. Gevolgen acceptatie certificaat

De gebruiker dient zijn certificaat te accepteren voordat hij het ter beschikking stelt aan anderen. Door het certificaat te accepteren is de gebruiker gebonden aan de daarop betrekking hebbende verplichtingen uit het contract en deze CPS.

## 5. Eigen verantwoordelijkheid relying party

Diegene die als ontvanger van een elektronisch bericht vertrouwt op een daarin gebruikte digitale handtekening of een daaraan verbonden certificaat dat is uitgegeven onder deze CPS, is zelf verantwoordelijk voor de mate van vertrouwen die wordt gesteld in de daaraan voorafgegane validatieprocedure. Alvorens enig vertrouwen op een digitale handtekening of certificaat te

baseren, wordt een relying party aangeraden om middels de repository het volgende te controleren

- is het certificaat geldig?
- is het certificaat ingetrokken of geblokkeerd?
- is de digitale handtekening gezet tijdens de geldigheidsduur van het certificaat?
- is de digitale handtekening gezet met de geheime sleutel die correspondeert met de in het certificaat opgenomen publieke sleutel
- is het bericht dat digitaal is ondertekend onveranderd gebleven?

## **6. Bescherming geheime sleutel gebruiker**

De gebruiker dient zijn geheime sleutel op adequate wijze te beschermen tegen inbreuk, manipulatie of misbruik . De gebruiker dient KPN Telecom direct in kennis te stellen van enige vorm van inbreuk op danwel manipulatie of misbruik van zijn geheime sleutel, volgens de procedure als in deze CPS beschreven.

## **7. Juridische aspecten**

Aan het gebruik van klasse 3 server certificaten van KPN Telecom zijn een aantal juridische (rand)voorwaarden verbonden, zoals beschreven in de gebruikersovereenkomst, de voorwaarden voor gebruik van de repository en deze CPS. Elk van deze documenten kan worden ingezien op de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>) en kan worden opgevraagd bij de klantenservice ([info@certificaat.kpn.com](mailto:info@certificaat.kpn.com)). In geval van strijd tussen deze CPS en de gebruikersovereenkomst zal de overeenkomst voorgaan. In geval van strijd tussen deze CPS en de voorwaarden voor gebruik van de repository zullen de voorwaarden voorgaan.

---

**Voor meer informatie zie de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>) of raadpleeg de klantenservice ([info@certificaat.kpn.com](mailto:info@certificaat.kpn.com))**

---

# TOTSTANDKOMING EN OPBOUW CPS

## 1. Totstandkoming

Deze CPS is gebaseerd op de oorspronkelijk engelstalige CPS van VeriSign Inc (VS) en aangepast aan de diensten van KPN Telecom, in zoverre die door VeriSign Inc. worden gefaciliteerd. Het is geen directe een-op-een vertaling van het oorspronkelijke document, maar werd door KPN Telecom met goedkeuring van VeriSign Inc. waar nodig gemodificeerd naar de specifieke aspecten van de betrokken diensten en aangepast voor gebruik binnen Nederland. Het oorspronkelijke document kan worden betrokken op de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>) alsmede op de website van VeriSign (<https://www.VeriSign.com/repository/CPS>)

## 2. Opbouw

Deze CPS is als volgt opgebouwd:

- **Hoofdstuk 2** beschrijft de infrastructuur die KPN Telecom en VeriSign gebruiken voor klasse 3 server certificaten. Beschreven wordt onder meer de algemene TTP infrastructuur, de klassen server certificaten die KPN Telecom uitgeeft, welke standaarden worden toegepast en de opbouw van de VeriSign PKI hiërarchie.
- **Hoofdstuk 3** beschrijft de basis voor de server certificatiedienst, zoals financiële verantwoordelijkheid, audits en personeelsbeleid. Ook wordt aangegeven welke vormen van beveiliging worden toegepast alsmede hoe wordt omgegaan met het eventuele stoppen van de certificatiedienst door KPN Telecom.
- **Hoofdstuk 4** beschrijft de procedure voor het aanvragen van een server certificaat en de daarvoor benodigde gegevens.
- **Hoofdstuk 5** beschrijft de manier waarop KPN Telecom een aanvraag controleert en uiteindelijk tot validatie van de aanvraag overgaat.
- **Hoofdstuk 6** beschrijft de procedure die wordt gevolgd bij het uitgeven van een server certificaat door KPN Telecom.
- **Hoofdstuk 7** beschrijft de wijze waarop het certificaat geaccepteerd wordt en de gevolgen die dit met zich meebrengt.
- **Hoofdstuk 8** beschrijft het gebruik van certificaten voor digitale handtekeningen.
- **Hoofdstuk 9** beschrijft de procedures die worden gevolgd voor blokkering en intrekking van server certificaten.
- **Hoofdstuk 10** beschrijft de procedure die wordt gevolgd wanneer de looptijd van een certificaat verstrijkt.
- **Hoofdstuk 11** beschrijft de (juridische) verplichtingen van KPN Telecom en VeriSign, zoals aansprakelijkheden en vrijwaringen.
- **Hoofdstuk 12** geeft een overzicht van diverse (juridische) bepalingen die nog resteren, bijvoorbeeld over aanpassing van deze CPS.

# INHOUDSOPGAVE

<b>OVERZICHT BELANGRIJKSTE ONDERDELEN CPS.....</b>	<b>III</b>
1. DOELSTELLING CPS.....	III
2. KENNISNIVEAU GEBRUIKER .....	III
3. SERVER SOFTWARE GESCHIKT VOOR DIGITALE SLEUTELS .....	III
4. GEVOLGEN ACCEPTATIE CERTIFICAAT .....	III
5. EIGEN VERANTWOORDELIJKHEID RELYING PARTY .....	III
6. BESCHERMING GEHEIME SLEUTEL GEBRUIKER .....	IV
7. JURIDISCHE ASPECTEN .....	IV
<b>TOTSTANDKOMING EN OPBOUW CPS.....</b>	<b>V</b>
1. TOTSTANDKOMING .....	V
2. OPBOUW .....	V
<b>1. INLEIDING .....</b>	<b>1</b>
1.1 INHOUD VAN DE CPS .....	1
1.2 STRUCTUUR VAN DE CPS .....	1
1.3 PUBLICATIE .....	2
1.4 VERWIJZINGEN NAAR DE CPS.....	2
1.5 BEVEILIGING .....	2
1.6 VERONDERSTELDE KENNIS .....	2
<b>2. CERTIFICATIE-INFRASTRUCTUUR.....</b>	<b>3</b>
2.1 INFRASTRUCTUUR OP BASIS VAN ‘TRUSTED THIRD PARTIES’ .....	3
2.1.1 Algemene beschrijving van certificaten en rol KPN Telecom.....	3
2.1.2 Algemene beschrijving uitgifteprocedure en certificaatbeheer.....	4
2.1.3 Certificatiediensten als beveiligingssysteem.....	4
2.1.4 Gebruikte standaard voor certificatiediensten.....	4
2.2 KLASSE 3 SERVER CERTIFICATEN.....	4
2.3 EIGENSCHAPPEN CERTIFICAATKLASSEN .....	5
2.3.1 Bevestiging van de identiteit van de gebruiker .....	5
2.3.2 Ondertekening geheime sleutel UA.....	6
2.3.3 Unieke verbinding publieke en geheime sleutel .....	6
2.3.4 Operationele infrastructuur .....	6
2.4 HIËRARCHIE VAN DE PUBLIC KEY INFRASTRUCTURE (PKI) .....	6
2.4.1 Root.....	7
2.4.2 Primaire Certificatie-Autoriteiten (PCA’s).....	8
2.4.3 Certificatie-Autoriteiten (CA’s).....	8
2.4.4 Lokale Registratie-Autoriteiten (LRA’s) .....	9
2.4.5 Naamgevende autoriteit .....	9
2.4.6 Repository .....	10
2.4.7 Openbaarmaking in de repository .....	10
<b>3. BASIS VOOR CERTIFICATIE-ACTIVITEITEN.....</b>	<b>11</b>
3.1 RECHT VAN VERISIGN OM ONDERZOEK TE DOEN INZAKE INBREUK .....	11
3.2 NALEVING VAN DE CPS.....	11
3.3 BETROUWBAARHEID.....	11
3.4 FINANCIËLE VERANTWOORDELIJKHEID .....	11
3.5 GEGEVENS MET BETREKKING TOT NALEVING VAN DE CPS.....	12

3.6	DATUMSTEMPELS .....	12
3.7	BEWAREN VAN GEGEVENS .....	12
3.8	AUDITS .....	12
3.9	RAMPENPLANNEN.....	13
3.10	BESCHIKBAARHEID VAN CERTIFICATEN KPN TELECOM .....	13
3.11	PUBLICATIE DOOR KPN TELECOM.....	13
3.12	VERTROUWELIJKE INFORMATIE .....	13
3.13	PERSONEELSBELEID .....	14
3.13.1	<i>Vertrouwensposities.....</i>	14
3.13.2	<i>Onderzoek en naleving.....</i>	14
3.13.3	<i>Ontheffing van taken van personen in vertrouwensposities.....</i>	14
3.14	ACCREDITATIES.....	14
3.14.1	<i>Goedkeuring van software en hardware.....</i>	14
3.14.2	<i>Personeel in vertrouwensposities.....</i>	15
3.15	GENEREREN VAN SLEUTELS DOOR KPN TELECOM .....	15
3.16	GEDEELDE GEHEIMHOUDING .....	15
3.16.1	<i>Gebruik van beveiligde hardware.....</i>	15
3.16.2	<i>Waarborgen .....</i>	15
3.16.3	<i>Acceptatie van geheime delen door houders van geheime delen.....</i>	15
3.16.4	<i>Bescherming van het geheime deel .....</i>	16
3.16.5	<i>Beschikbaarheid en vrijgave van geheime delen .....</i>	16
3.16.6	<i>Registratie van activiteiten.....</i>	16
3.16.7	<i>Verplichtingen van de houder van een geheim deel.....</i>	17
3.16.8	<i>Vrijwaring door de verstrekker van een geheim deel.....</i>	17
3.17	BEVEILIGING.....	17
3.17.1	<i>Beveiliging van de communicatie.....</i>	17
3.17.2	<i>Beveiliging van de te gebruiken voorzieningen.....</i>	17
3.18	EISEN TEN AANZIEN VAN MEDEWERKERS VAN REGISTRATIE-AUTORITEITEN .....	17
3.19	BEËINDIGING VAN ACTIVITEITEN DOOR KPN TELECOM .....	18
3.19.1	<i>Voorwaarden aan beëindiging.....</i>	18
3.19.2	<i>Heruitgifte van certificaten door een nieuwe UA.....</i>	18
<b>4.</b>	<b>AANVRAAGPROCEDURE CERTIFICAAT.....</b>	<b>20</b>
4.1	ALGEMENE BESCHRIJVING PROCEDURES .....	20
4.2	GENEREREN EN BEHEREN VAN SLEUTELS .....	20
4.2.1	<i>Verplichtingen ten aanzien van sleutelparen .....</i>	20
4.2.2	<i>Overdracht van verantwoordelijkheid geheime sleutel(s).....</i>	21
4.3	INFORMATIE EN COMMUNICATIE MET BETREKKING TOT CERTIFICAATAANVRAGEN .....	21
<b>5.</b>	<b>VALIDATIE VAN CERTIFICAATAANVRAGEN.....</b>	<b>22</b>
5.1	DOELSTELLING VALIDATIE .....	22
5.2	EENMALIG KARAKTER VALIDATIE .....	22
5.3	EISEN VALIDATIE .....	22
5.3.1	<i>Bevestiging door derden van bestaan en benaming zakelijke entiteiten.....</i>	23
5.3.2	<i>Bevestiging InterNIC domeinnaam.....</i>	23
5.4	GOEDKEURING VAN AANVRAGEN .....	23
5.5	AFWIJZING VAN EEN CERTIFICAATAANVRAAG.....	23
<b>6.</b>	<b>UITGIFTE VAN CERTIFICATEN .....</b>	<b>24</b>
6.1	ALGEMENE PROCEDURE .....	24
6.2	TOESTEMMING VAN DE GEBRUIKER VOOR UITGIFTE .....	24
6.3	WEIGERING TOT UITGIFTE VAN EEN CERTIFICAAT.....	24
6.4	VERPLICHTINGEN VAN KPN TELECOM BIJ UITGIFTE .....	24

6.4.1	<i>Verplichtingen van KPN Telecom tegenover de gebruiker</i>	24
6.4.2	<i>Verplichtingen van KPN Telecom tegenover relying parties</i>	25
6.4.3	<i>Beperkingen aan de verplichtingen van KPN Telecom</i>	25
6.5	TIJDSTIP VAN CERTIFICAATUITGIFTE	25
6.6	GELDIGHEID EN GELDIGHEIDSDUUR VAN CERTIFICATEN	25
6.7	BEPERKINGEN OP UITGEGEVEN MAAR NOG NIET GEACCEPTEEERDE CERTIFICATEN	25
<b>7.</b>	<b>ACCEPTATIE VAN CERTIFICATEN DOOR GEBRUIKERS</b>	<b>26</b>
7.1	ACCEPTATIE VAN EEN CERTIFICAAT	26
7.1.1	<i>Wijziging van gecertificeerde gegevens na acceptatie</i>	26
7.1.2	<i>Restitutie na acceptatie</i>	26
7.2	GARANTIES GEBRUIKER DOOR ACCEPTATIE CERTIFICAAT	26
7.3	VERPLICHTINGEN GEBRUIKER DOOR ACCEPTATIE CERTIFICAAT	27
7.4	VRIJWARING DOOR DE GEBRUIKER	27
7.5	PUBLICATIE	28
<b>8.</b>	<b>GEBRUIK VAN CERTIFICATEN VOOR DIGITALE HANDTEKENINGEN</b>	<b>29</b>
8.1	DOELSTELLING VERIFICATIE DIGITALE HANDTEKENINGEN	29
8.2	METHODE VAN VERIFICATIE	29
8.2.1	<i>Vaststellen van een certificatieketen voor de digitale handtekening</i>	29
8.2.2	<i>Nagaan van meest geschikte certificatieketen</i>	29
8.2.3	<i>Controleren van geblokkeerde of ingetrokken certificaten in de keten</i>	30
8.2.4	<i>Begrenzen gegevens waaraan digitale handtekeningen worden gekoppeld</i>	30
8.2.5	<i>Aangeven van tijd en datum waarop digitale handtekening is aangemaakt</i>	30
8.2.6	<i>Vaststellen van de garanties zoals die zijn bedoeld door de ondertekenaar</i>	30
8.2.7	<i>Nagaan beperkingen geheime sleutel binnen de certificatieketen</i>	30
8.2.8	<i>Bevestiging van een certificatieketen</i>	30
8.3	GEVOLG VAN VALIDATIE VAN EEN GEBRUIKERSCERTIFICAAT	31
8.4	PROCEDURES BIJ MISLUKTE VERIFICATIE VAN EEN DIGITALE HANDTEKENING	31
8.5	VERTROUWEN IN DIGITALE HANDTEKENINGEN	31
8.6	GELDIGHEID DIGITAAL ONDERTEKENDE BERICHTEN VERSUS GESCHRIFTEN	32
8.7	GELDIGHEID DIGITALE HANDTEKENINGEN VERSUS GEWONE HANDTEKENINGEN	32
8.8	BEVEILIGINGSMAATREGELEN	32
<b>9.</b>	<b>BLOKKERING EN INTREKKING VAN CERTIFICATEN</b>	<b>33</b>
9.1	INTREKKING VAN EEN CERTIFICAAT DOOR KPN TELECOM	33
9.1.1	<i>Directe intrekking van een certificaat door KPN Telecom</i>	33
9.1.2	<i>Kennisgeving en confirmatie bij intrekking</i>	34
9.2	BLOKKERING OF INTREKKING VAN HET CERTIFICAAT VAN KPN TELECOM	34
9.2.1	<i>Blokkering op verzoek van KPN Telecom</i>	35
9.2.2	<i>Beëindiging van blokkering van een certificaat van KPN Telecom</i>	35
9.3	GEVOLGEN VAN BLOKKERING OF INTREKKING	35
9.3.1	<i>Gevolgen voor certificaten</i>	35
9.3.2	<i>Gevolgen voor onderliggende verplichtingen</i>	35
9.4	VEILIGSTELLEN VAN DE GEHEIME SLEUTEL BIJ BLOKKERING OF INTREKKING	36
<b>10.</b>	<b>VERLOPEN VAN CERTIFICATEN</b>	<b>37</b>
10.1	KENNISGEVING VAN VERVALDATUM	37
10.2	GEVOLGEN VAN HET VERLOPEN VAN CERTIFICATEN VOOR ONDERLIGGENDE VERPLICHTINGEN	37
10.3	VERLENGEN EN OPNIEUW AANVRAGEN VAN CERTIFICATEN	37
<b>11.</b>	<b>VERPLICHTINGEN VAN KPN TELECOM EN VERISIGN</b>	<b>38</b>
11.1	BEPERKTE WAARBORGEN EN ANDERE VERPLICHTINGEN	38

11.2	NIET-AANSPRAKELIJKHEIDSCLAUSULES EN BEPERKING VAN VERPLICHTINGEN .....	38
11.3	UITSLUITING VAN BEPAALDE SCHADEVORMEN .....	38
11.4	BEPERKING AANSPRAKELIJKHEID KPN TELECOM EN VERISIGN.....	39
11.4.1.	<i>Beperking aansprakelijkheid KPN Telecom tegenover gebruiker .....</i>	39
11.4.2	<i>Beperking aansprakelijkheid KPN Telecom tegenover gebruiker .....</i>	39
11.4.3	<i>Beperking aansprakelijkheid VeriSign.....</i>	40
11.5	AANSPRAKELIJKHEID VAN DE GEBRUIKER TEN OPZICHTE VAN RELYING PARTIES .....	41
11.6	GEEN FIDUCIAIRE RECHTSVERHOUDING.....	41
11.7	RISICOVOLLE ACTIVITEITEN.....	41
<b>12.</b>	<b>DIVERSE BEPALINGEN.....</b>	<b>42</b>
12.1	STRIJDIGE BEPALINGEN.....	42
12.2	TOEPASSELIJK RECHT.....	42
12.3	GESCHILLENBESLECHTING.....	42
12.4	OPVOLGERS EN RECHTVERKRIJGENDE.....	42
12.5	WIJZIGING VOORWAARDEN .....	42
12.6	VOLLEDIG DOCUMENT .....	43
12.7	UITLEG EN VERTALINGEN .....	43
12.8	GEEN VERKLARING VAN AFSTAND .....	43
12.9	KENNISGEVING .....	43
12.10	KOPPEN EN BIJLAGEN VAN DEZE CPS.....	44
12.11	WIJZIGEN VAN INFORMATIE .....	44
12.12	WIJZIGEN VAN DE CPS .....	44
12.12.1	<i>Algemene wijzigingen.....</i>	44
12.12.2	<i>Materiële wijzigingen.....</i>	44
12.12.3	<i>Wijziging ter voorkoming van inbreuk .....</i>	44
12.12.4	<i>Niet inhoudelijke wijzigingen .....</i>	45
12.12.5	<i>Intrekking certificaat vanwege wijziging CPS.....</i>	45
12.13	INTELLECTUEEL EIGENDOM .....	45
12.14	INBREUK EN ANDER SCHADELIJK MATERIAAL.....	45
12.14.1	<i>Eigen verantwoordelijkheid verstrekte informatie .....</i>	46
12.14.2	<i>Geen onwettige of onrechtmatige informatie .....</i>	46
12.15	TARIEVEN.....	47
12.16	KEUZE VAN CRYPTOGRAFISCHE METHODEN .....	47
12.17	BLIJVENDE GELDIGHEID .....	47
12.18	OVERMACHT .....	47
<b>13.</b>	<b>ACRONIEMEN EN AFKORTINGEN.....</b>	<b>48</b>
<b>14.</b>	<b>DEFINITIES.....</b>	<b>49</b>
	<b>MEDEWERKING AAN DEZE CPS .....</b>	<b>66</b>

# 1. INLEIDING

---

**In dit hoofdstuk wordt de Certification Practice Statement (CPS) geïntroduceerd en wordt ingegaan op de onderliggende TTP infrastructuur. Het hoofdstuk wordt afgesloten met een lijst van acroniemen en afkortingen die in de CPS worden gebruikt.**

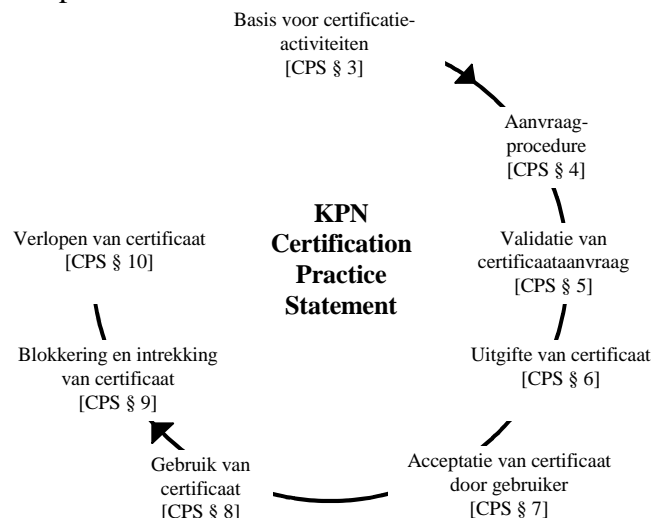
---

## 1.1 Inhoud van de CPS

Deze Certification Practice Statement beschrijft de procedures die worden gevolgd door KPN Telecom en, voorzover toepasselijk, door VeriSign bij het uitgeven en beheren van klasse 3 server certificaten en het onderhouden van een op zulke (en andere) certificaten gebaseerde Public Key Infrastructuur (PKI). De CPS bevat gedetailleerde regelingen voor het certificatieproces van servers, van het gebruik van de repository (zie definities) tot en met de acceptatie van certificaten door gebruikers. Deze CPS is bedoeld om juridisch bindend te zijn voor alle partijen die certificaten maken, gebruiken en valideren binnen de context van de publiek certificatediensten van KPN Telecom en VeriSign. Als zodanig speelt deze CPS een centrale rol bij de uitvoering van de publieke certificatediensten en vormt ze een integraal onderdeel van de gebruikersovereenkomst en de relying party overeenkomst.

## 1.2 Structuur van de CPS

De CPS heeft een integrale benadering ten aanzien van het beschrijven van certificatieprocessen: van het aanvragen van certificaten tot en met het gebruik, het blokkeren en het intrekken ervan. Deze aanpak heeft als voordeel dat gebeurtenissen chronologisch kunnen worden weergegeven, dus van aanmaak tot intrekking, hetgeen de inzichtelijkheid in het proces bevordert. Tevens wordt op die manier geanticipeerd op compatibiliteit met toekomstige Certification Practice Statements in de private en publieke sector.



FIGUUR 1 – LEVENSCYCLUS STRUCTUUR CPS

### 1.3 Publicatie

Deze CPS wordt in de volgende vormen gepubliceerd:

- in elektronische vorm op de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>)
- in elektronische vorm via e-mail ([info@certificaat.kpn.com](mailto:info@certificaat.kpn.com))
- op schrift, verkrijgbaar bij KPN Telecom (Postbus 30150, 2500 GD 's-Gravenhage, o.v.v. CPS)

### 1.4 Verwijzingen naar de CPS

Indien in andere documenten wordt verwezen naar deze CPS, dan dient te worden gesproken over de “KPN CPS voor Klasse 3 Server Certificaten”. Intern, dat wil zeggen in dit document, wordt gesproken over de “CPS”. De CPS wordt regelmatig herzien door KPN Telecom en Verisign; versies van de CPS worden daarom voorzien van een versienummer volgend op “CPS” (bijvoorbeeld “versie 1.0” of “CPS 1.0”).

### 1.5 Beveiliging

Alle in deze CPS genoemde URL's van KPN Telecom en Verisign zijn beveiligd via het SSL protocol (Secure Socket Layer). Door gebruikmaking van dit protocol kan informatie op een veilige manier worden opgevraagd, mits een browser wordt gebruikt die SSL ook daadwerkelijk ondersteunt (zoals Microsoft Internet Explorer 3.x en Netscape Navigator 3.x en hoger).

De op deze pagina's aanwezige informatie is ook beschikbaar zonder gebruikmaking van SSL (dus via een niet beveiligde weg) door in bovenstaande URL's de aanduiding *https* te vervangen door *http*. Het wordt bezoekers van de website echter aangeraden om bij het opvragen van officiële documenten uit de repository van KPN Telecom zoveel mogelijk gebruik te maken van SSL, dus via *https*.

### 1.6 Veronderstelde kennis

In deze CPS wordt er, inhoudelijk gezien, vanuit gegaan dat de lezer enige bekendheid heeft met digitale handtekeningen, certificaten en Public Key Infrastructuren (PKI). Mocht dat niet het geval zijn, dan wordt de lezer geadviseerd om - alvorens een certificaat aan te vragen - zich tenminste globaal van de inhoud van deze onderwerpen op de hoogte te stellen. Opleidings- en trainingsmateriaal is verkrijgbaar via de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>) of door contact op te nemen met de klantenservice ([info@certificaat.kpn.com](mailto:info@certificaat.kpn.com)).

## 2. CERTIFICATIE-INFRASTRUCTUUR

---

**In dit gedeelte wordt ingegaan op de architectuur die ten grondslag ligt aan het systeem van publieke certificatediensten. Tevens wordt aandacht besteed aan certificaatklassen, certificaatextensies, datumstempels en de repository van KPN Telecom.**

---

### 2.1 Infrastructuur op basis van ‘*Trusted Third Parties*’

De certificatediensten van KPN Telecom dienen ter ondersteuning van veilig elektronisch handelsverkeer en van andere algemene beveiligingsdiensten. Om deze diensten mogelijk te maken fungeert KPN Telecom - technisch gefaciliteerd door VeriSign - als een zogenaamde *Trusted Third Party* (betrouwbare derde partij) voor het uitgeven, beheren, blokkeren en intrekken van certificaten conform de in dit document opgenomen processen en procedures.

Een publiek certificatiesysteem zoals dat van KPN Telecom is bedoeld voor personen en/of bedrijven met uiteenlopende eisen en wensen ten aanzien van communicatie en informatiebeveiliging. Om de uniformiteit van de dienstverlening tegenover gebruikers te kunnen garanderen, zijn de organisatorische en technische procedures die worden toegepast ter bescherming van de integriteit van het publieke certificatiesysteem beschreven in deze CPS. Het is de bedoeling dat, door de procedures te beschrijven en aldus transparant te maken, het vertrouwen van de uiteindelijke gebruikers in een juiste werking van de certificatediensten wordt vergroot.

#### 2.1.1 Algemene beschrijving van certificaten en rol KPN Telecom

Binnen de Public Key Infrastructure heeft KPN Telecom als Uitgevende Autoriteit (UA) de functie om de relatie tussen een publieke sleutel en een entiteit (in geval van klasse drie server certificaten: een bedrijf) te confirmeren. Deze confirmatie wordt vormgegeven middels een certificaat – een elektronisch bericht dat is uitgegeven en digitaal ondertekend door KPN Telecom en waarin de genoemde relatie wordt bevestigd. Als zodanig omvat het certificatieproces registratie, naamgeving, authenticatie van de certificaataanvrager, uitgifte van certificaten, blokkering van certificaten, intrekking van certificaten en het opzetten van audits. De naamgeving in het certificaat is voorbehouden aan KPN Telecom en VeriSign, danwel aan een andere partij. Naamgeving van gebruikers vindt plaats volgens een apart registratieproces dat afwijkt van het proces dat wordt toegepast om de geldigheid van certificaten vast te stellen.

Ieder certificaat dat door KPN Telecom wordt uitgegeven, correspondeert met een specifiek beveiligingsniveau; deze verschillen onderling door specifieke vormen van dienstverlening en procedures die zijn afgestemd op verschillende doelgroepen. Voor wat betreft de server certificaten van KPN Telecom bestaat er slechts een niveau: klasse 3. Ter vergelijking: Verisign zelf verkoopt drie niveau's, klasse 1 tot en met 3, waarvan de laatste het hoogste niveau qua beveiliging biedt. Dat niveau is vergelijkbaar met het niveau dat KPN Telecom hanteert.

KPN Telecom heeft, als aan Verisign ondergeschikte autoriteit in de certificatieketen, zelf ook een publieke (en geheime) sleutel en een certificaat. Dat certificaat is ondertekend door Verisign en voor verificatie beschikbaar in de repository (<https://www.kpn-telecom.nl/certificaat>)

Tot het certificatieproces behoort tevens het deactiveren van certificaten en het buiten werking stellen van de bijbehorende geheime sleutels middels een proces waarmee certificaten worden geblokkeerd en ingetrokken. Andere diensten van UA's omvatten het registreren, distribueren, publiceren, opslaan en opvragen van certificaten in overeenstemming met het bedoelde gebruik ervan.

### **2.1.2 Algemene beschrijving uitgifteprocedure en certificaatbeheer**

De uitgifteprocedure van een server certificaat verloopt globaal gezien als volgt. Nadat een certificaataanvraag is binnengekomen, voert KPN Telecom een aantal controles uit om de relatie tussen de publieke sleutel en het bedrijf te kunnen leggen. Wanneer deze controles slagen, wordt een certificaat opgemaakt, gepubliceerd en verstrekt aan de aanvrager. De aanvrager dient vervolgens na te gaan of (de inhoud van) het certificaat correct is en of het certificaat in het algemeen geschikt is voor de doelen die hij ermee nastreeft. Is dat het geval, dan dient hij het certificaat via de daarvoor bestemde procedure te accepteren (waardoor hij certificaathouder wordt, ook wel gebruiker genoemd). Na acceptatie door de aanvrager zal het certificaat gedurende haar looptijd worden beheerd door KPN Telecom, hetgeen naast de verstrekking onder andere ook het blokkeren en intrekken van certificaten inhoudt.

### **2.1.3 Certificatiediensten als beveiligingssysteem**

De publieke certificatie-diensten van KPN Telecom vormen een kader waarbinnen partijen digitale handtekeningen kunnen gebruiken die, door ze via certificaten te verifiëren, de bescherming mogelijk maken van communicatie en elektronisch handelsverkeer via open netwerken. Aldus kunnen certificaten erin voorzien dat inbreuken op de veiligheid van bepaalde netwerk-omgevingen worden tegengegaan danwel verminderd. Desalniettemin is het de gebruiker zelf die, aan de hand van de te verwachten risico's, moet inschatten of de onderhavige certificatie-dienst het beste geschikt is om zijn netwerk-omgeving te beschermen tegen bepaalde inbreuken.

### **2.1.4 Gebruikte standaard voor certificatie-diensten**

Binnen de publieke certificatie-diensten van KPN Telecom wordt gebruik gemaakt van de RSA standaard voor digitale handtekeningen en van de X.509v3 standaard voor certificaten.

## **2.2 Klasse 3 server certificaten**

Klasse 3 server certificaten worden uitgegeven aan particuliere en publieke organisaties en bieden bepaalde garanties omtrent:

- (a) het bestaan van de betrokken organisatie,
- (b) de benaming van de betrokken organisatie, en
- (c) het bezit of rechtmatig gebruik van een specifieke domeinnaam (URL) door de betrokken organisatie

De klasse 3 server certificaten van KPN Telecom zijn met name geschikt voor gebruik in het elektronisch handelsverkeer, zoals bij elektronisch winkelen, Web Electronic Data Interchange (Web EDI) en op lidmaatschappen gebaseerde online diensten.

De validatie van klasse 3 certificaataanvragen (zie hoofdstuk 5) vereist controle door KPN Telecom van bepaalde gegevens (verkregen via de aanvrager danwel uit zakelijke databanken) alsmede het steekproefgewijs bevestigen van informatie bij de aanvragende organisatie. Met name de toepassing van steekproeven resulteert in deze in een grotere mate van zekerheid.

De beschrijving van certificaatklasse 3 vormt geen goedkeuring of aanbeveling door KPN Telecom of VeriSign van een specifieke toepassing of bedoeling van het certificaat en mag ook niet als zodanig worden beschouwd. Gebruikers dienen zelf te bepalen of een klasse 3 server certificaat geschikt is voor het door hen gewenste doel.

### 2.3 Eigenschappen certificaatklassen

Een X.509v3 certificaat is opgebouwd uit de volgende onderdelen:

<b>X.509 v3 CERTIFICAAT</b>
Versie (3)
Serienummer
Handtekening algorithm ID
Naam uitgever
Looptijd
Naam houder certificaat (OU=)
Informatie publieke sleutel houder
Unique identifier uitgever
Unique identifier houder
<b>Standaard extensies</b>
<b>Andere extensies</b>

Figuur 2 – Indeling X.509v3 certificaat

Een certificaat op het niveau van klasse 3 wordt tenminste gekenmerkt door de volgende eigenschappen:

- De identiteit van de certificaathouder staat erin bevestigd;
- Het is ondertekend met de geheime sleutel van de UA;
- De in het certificaat opgenomen publieke sleutel is uniek verbonden met de geheime sleutel van de certificaathouder;
- Er is een operationele infrastructuur die het specifieke niveau garandeert.

#### 2.3.1 Bevestiging van de identiteit van de gebruiker

In iedere certificaatklasse zal de UA (in dit verband: KPN Telecom) bepaalde handelingen verrichten om de identiteit van de certificaataanvrager na te gaan, ook wel de validatieprocedure

genoemd. De informatie die is verstrekt tijdens de aanvraagprocedure wordt dan nagegaan en indien mogelijk bevestigd door de UA. Welke methoden daarbij precies worden toegepast en in welke mate de UA de identiteit van de aanvrager nagaat, is afhankelijk van het beveiligingsniveau dat het certificaat vertegenwoordigt. Voor wat betreft de validatieprocedure die KPN Telecom toepast voor klasse 3 server certificaten wordt verwezen naar hoofdstuk 5 van deze CPS.

### **2.3.2 Ondertekening geheime sleutel UA**

Via de geheime sleutel van KPN Telecom (in dit geval de RSA sleutel van Verisign) worden alle uit te geven certificaten ondertekend. Misbruik van de geheime sleutel zou ertoe kunnen leiden dat partijen die daartoe niet bevoegd zijn, in naam van KPN Telecom klasse 3 server certificaten kunnen ondertekenen en uitgeven. Om een dergelijke vorm van misbruik tegen te gaan, wordt de RSA sleutel van Verisign tegen inbreuk beschermd door gebruikmaking van beveiligde en betrouwbare hardwareproducten.

### **2.3.3 Unieke verbinding publieke en geheime sleutel**

De in het certificaat opgenomen publieke sleutel (die tijdens de aanvraagprocedure aan KPN Telecom wordt aangeboden) is op unieke wijze verbonden met de geheime sleutel van de gebruiker. Gevolg is, dat een met de geheime sleutel gezette handtekening altijd moet corresponderen met de publieke sleutel in het certificaat, wil de handtekening als legitiem kunnen worden beschouwd. De vertrouwelijkheid van de geheime sleutel dient door de certificaathouder derhalve zo goed mogelijk te worden beschermd, om te voorkomen dat anderen zich voor hem gaan uitgeven. De geheime sleutel kan bijvoorbeeld worden beschermd door gebruik te maken van toegangscodes (passwords), encryptiesoftware of hardwaretokens zoals smartcards of PC-cards. Voor meer informatie over de bescherming van de geheime sleutel zie het vraag-antwoord document op de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>).

KPN Telecom noch Verisign genereren de door certificaataanvragers te gebruiken geheime sleutels, aangezien dit gebeurt via de server software op de computer van de aanvrager zelf. Dientengevolge hebben KPN Telecom noch Verisign (een kopie van) deze sleutels in hun bezit; de gebruiker van een certificaat is de enige die over de geheime sleutel kan beschikken.

### **2.3.4 Operationele infrastructuur**

De operationele infrastructuur bestaat uit de organisatorische, personele en andere maatregelen die zijn geïmplementeerd ten behoeve van de specifieke certificaatklasse. Zulke maatregelen kunnen bijvoorbeeld bestaan uit beperkingen aangaande wie certificaten mag verwerven, eisen die gesteld worden aan de opleiding van UA-personeel, richtlijnen voor een scheiding van taken binnen de UA's, documentatierichtlijnen en voorgeschreven procedures en audits. De meeste van deze procedures zijn beschreven in hoofdstuk 3 van de CPS.

## **2.4 Hiërarchie van de Public Key Infrastructure (PKI)**

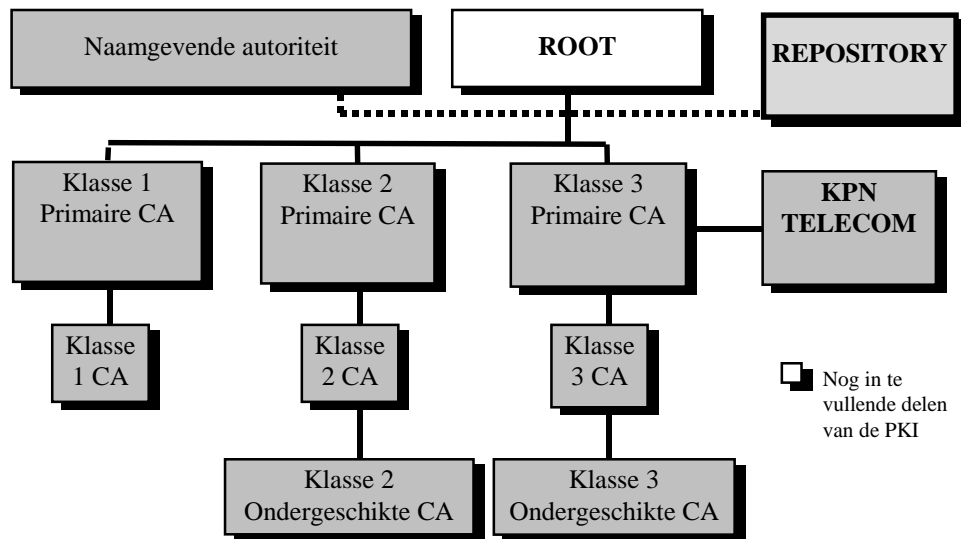
De publieke certificatediensten zijn ondergebracht in een PKI-hiërarchie die uit de volgende uitgevende autoriteiten bestaat:

- de root,

- drie of meer primaire certificatie-autoriteiten (PCA's),
- drie of meer CA's (ten minste één CA onder iedere PCA), en
- andere CA's (waaronder ondergeschikte CA's) die door VeriSign of een geautoriseerde UA zijn geautoriseerd om in overeenstemming met deze CPS publieke certificatediensten te verlenen.

In de PKI-hiërarchie zijn de UA's onderling verbonden; de ene UA functioneert in dienst van de andere. Een UA dient voor het uitgeven van certificaten gebruik te maken van hetzij algemene, hetzij uitgebreide authenticatieprocedures (voor validatie door de UA). Dit is afhankelijk van de klasse van het desbetreffende gebruikerscertificaat, uitgegeven door de laagste UA in de hiërarchie.

Daarnaast mogen UA's bepaalde registratiefuncties delegeren aan een of meerdere LRA's. De PKI omvat tevens de naamgevende autoriteit en de repository van VeriSign. Figuur 4 geeft een overzicht van de structuur van de PKI. (Voor een beter overzicht zijn de LRA's niet in Figuur 2 opgenomen).



FIGUUR 3 – VEREENVOUDIGDE HIËRARCHIE VAN DE PKI-INFRASTRUCTUUR

### 2.4.1 Root

De root – een entiteit die eigendom is van VeriSign en wordt bestuurd door VeriSign – is verantwoordelijk voor het uitgeven van publieke-sleutelcertificaten aan PCA's. De Root dient de *distinguished names* van PCA's te accorderen. Bovendien speelt de Root binnen de publieke certificatediensten een centrale vertrouwensrol. Iedere PCA dient haar eigen publieke sleutel zelf te ondertekenen en deze tijdens de registratie bekend te maken aan de Root. Beide partijen zijn tevens verantwoordelijk voor het op de juiste wijze vervullen van de geldende procedures in overeenstemming met het *Handboek Beveiliging 1996/97* van KPN Telecom.

De initiële RSA-sleutelgrootte van de Root is 2048 bits. Er wordt gebruikgemaakt van betrouwbare hardware (FIPS 140-1 Niveau 3-certificeerbaar) voor het aanmaken, beschermen en

vernietigen van de geheime sleutel van de Root. Het sleutelpaar van de root kan worden vervangen en de vervangende publieke sleutel kan middels de repository openbaar worden gemaakt. Bepaalde delen van de geheime sleutel (de zogenaamde 'secret shares') van de root zijn in bezit van personen die niet in dienst zijn van VeriSign. Doel hiervan is om de betrouwbaarheid en het vertrouwelijke karakter van de root te vergroten. Daarbij worden de procedures gevolgd die zijn neergelegd in deze CPS met betrekking tot het splitsen van geheime delen.

*N.B.: Momenteel is de root is nog niet in gebruik genomen. Reden hiervoor is onder andere het feit dat de sleutelgrootte van 2048 bits nog niet door alle gebruikerssoftware wordt ondersteund. Momenteel fungeert iedere PCA als Root.*

#### **2.4.2 Primaire Certificatie-Autoriteiten (PCA's)**

Binnen de structuur van publieke certificatiediensten gelden CA's als de hoogste actieve certificerende instanties. PCA's zijn verantwoordelijk voor het uitgeven, blokkeren en intrekken van certificaten voor alle CA's. Binnen de PKI-hiërarchie zijn alle PCA's ondergeschikt aan de Root. Iedere PCA is eigendom van en wordt bestuurd door VeriSign.

De initiële sleutelgrootte van iedere PCA is 1024 bits. Er wordt gebruikgemaakt van betrouwbare hardware (FIPS 140-1 Niveau 3-certificeerbaar) voor het aanmaken, beschermen en vernietigen van de geheime sleutel van iedere PCA. De doelstellingen, geboden zekerheden, diensten en verplichtingen van iedere PCA (alsmede de rechten en verantwoordelijkheden van aanvragers, gebruikers en ontvangers van certificaten, relying parties en CA's/ondergeschikte CA's binnen de certificatieketen van de PCA) zijn omschreven in deze CPS.

Cross-certification tussen PCA's van VeriSign en vergelijkbare entiteiten die niet tot de PKI van VeriSign behoren, is toegestaan indien:

- (i) VeriSign bepaalt dat de andere entiteit ten minste een vergelijkbare functie heeft en een vergelijkbare mate van zekerheid en betrouwbaarheid biedt,
- (ii) cross-certification voor VeriSign-gebruikers de waarde van VeriSign-certificaten verhoogt,
- (iii) beide partijen een door VeriSign opgestelde cross-certification-overeenkomst hebben gesloten,
- (iv) VeriSign en de andere entiteit wederzijds certificaten hebben uitgegeven,
- (v) beide partijen voornoemd certificaat hebben geaccepteerd, en
- (vi) partijen het eens zijn over procedures die worden gevolgd met betrekking tot blokkering en intrekking van certificaten.

#### **2.4.3 Certificatie-Autoriteiten (CA's)**

Iedere CA is ondergeschikt aan een PCA en opereert overeenkomstig deze CPS en eventuele beperkingen die specifiek door de PCA aan de CA zijn gesteld (conform deze CPS). Klasse 1-3 CA's mogen gebruikerscertificaten uitgeven, beheren en intrekken. Klasse 2-3 CA's mogen bovendien UA-certificaten uitgeven aan ondergeschikte CA's. Ondergeschikte CA's mogen gebruikerscertificaten uitgeven, beheren en intrekken.

De initiële sleutelgrootte van iedere CA (en ondergeschikte CA) is 1024 bits. Er wordt gebruikgemaakt van betrouwbare hardware (FIPS 140-1 Niveau 3-certificeerbaar) voor het aanmaken, beschermen en vernietigen van de geheime sleutels van Klasse 2-3 CA's. CA's en ondergeschikte CA's zijn doorgaans eigendom van VeriSign en worden ook bestuurd door VeriSign. Indien beide partijen dit wensen, kan VeriSign ook niet-VeriSign-CA's en hieraan ondergeschikte CA's (of niet-VeriSign-CA's die ondergeschikt zijn aan een VeriSign-CA) autoriseren tot het verlenen van diensten binnen het kader van de publieke certificatediensten van VeriSign.

#### **2.4.4 Lokale Registratie-Autoriteiten (LRA's)**

Lokale registratie-autoriteiten (LRA's) zijn entiteiten die certificaataanvragen beoordelen en vervolgens goedkeuren of afwijzen. Daarnaast zijn LRA's in bepaalde gevallen bevoegd om het intrekken of blokkeren van certificaten te bekrachtigen. LRA's mogen een beheerder (BLRA) inzetten om de taken van een LRA uit te voeren. LRA's opereren namens en (binnen het kader van de CPS) uit hoofde van één enkele UA (de Root, PCA of CA die de certificaten daadwerkelijk uitgeeft). Een UA kan meer dan een LRA hebben.

De volgende documenten mogen door een LRA worden geaccepteerd voor het confirmeren van informatie die is verstrekt door de aanvrager van een certificaat:

- (i) notariële akten waarvan redelijkerwijs mag worden verwacht dat ze op de juiste wijze zijn gepasseerd, en
- (ii) algemeen erkende identiteitsbewijzen als paspoorten en rijbewijzen.

Niet-VeriSign-LRA's zijn LRA's die niet gelieerd zijn aan VeriSign, maar bevoegd zijn om de uitgifte en intrekking te accorderen van certificaten bedoeld voor individuele personen die zijn gelieerd aan de desbetreffende LRA. Zo kan een bedrijf een verzoek indienen om een niet-VeriSign-LRA te worden, teneinde certificaten te mogen uitgeven aan haar eigen werknemers en aan andere personen die aan het bedrijf zijn gelieerd. Het bedrijf is niet gerechtigd om certificaten uit te geven aan andere personen.

Certificaten van niet-VeriSign-LRA's mogen alleen worden uitgegeven aan individuele personen waarvan de relatie met de LRA kan worden vastgesteld. Dit dient te geschieden door de BLRA op basis van relevante interne documentatie (zoals personeelsgegevens) en informatie van derden. Alle certificaten die worden uitgegeven na goedkeuring van een certificaataanvraag door een niet-VeriSign-LRA, dienen te zijn voorzien van een *distinguished name* die de relatie van de houder met de LRA uitdrukt. Niet-VeriSign-LRA's dragen de volledige verantwoordelijkheid voor het goedkeuren of afwijzen van certificaataanvragen. VeriSign en UA's wijzen deze verantwoordelijkheid dan ook nadrukkelijk af.

#### **2.4.5 Naamgevende autoriteit**

De naamgevende autoriteit coördineert voor alle UA's van VeriSign het proces met betrekking tot het uitgeven van *distinguished names*. De naamgevende autoriteit mag tevens richtlijnen specificeren ten aanzien van naamgeving van certificaathouders in de repository van VeriSign. Deze richtlijnen kunnen verschillen per certificaatklasse en per UA. Tevens kunnen er

verschillen in de naamgeving bestaan tussen de uitgifte en de heruitgifte/verlenging van certificaten. UA's die geen deel uitmaken van de VeriSign-organisatie dienen ofwel gebruik te maken van de naamgevende autoriteit van VeriSign, ofwel een naamgevende autoriteit in het leven te roepen of te gebruiken waarvan de procedures niet strijdig zijn met die van de naamgevende autoriteit van VeriSign en die geen RDN's door de naamgevende autoriteit van VeriSign laten registreren. Voor de uitgifte van klasse 3 server certificaten maakt KPN Telecom gebruik van de naamgevende autoriteit van Verisign.

#### **2.4.6 Repository**

De repository is een openbare verzameling databases voor het opslaan en opvragen van certificaten en informatie met betrekking tot certificaten. Alle UA's die gelieerd zijn aan Verisign (dus ook KPN Telecom) maken voor de publieke certificatediensten gebruik van de repository van VeriSign. Daarin zijn de certificaten opgeslagen alsmede CRL's en andere informatie over geblokkeerde en ingetrokken certificaten.

In de repository kunnen geen wijzigingen worden aangebracht in certificaten of kennisgevingen over geblokkeerde of ingetrokken certificaten. Voorwaarde is dat de desbetreffende informatie in de juiste vorm door een UA wordt verstrekt. De inhoud van voornoemde bescheiden zal op accurate wijze worden weergegeven.

#### **2.4.7 Openbaarmaking in de repository**

De repository bevat te allen tijde actuele informatie ten aanzien van certificaten, wijzigingen in de CPS, kennisgevingen over geblokkeerde of ingetrokken certificaten en andere informatie in overeenstemming met deze CPS en het toepasselijke recht. De repository van KPN Telecom kan worden geraadpleegd via het WWW (<https://www.kpn-telecom.nl/certificaat>) of op een andere door KPN Telecom of Verisign kenbaar te maken wijze.

Gebruikerscertificaten en gegevens over CRL's kunnen door KPN Telecom zowel middels de repository als anderszins openbaar worden gemaakt. Tenzij KPN Telecom of VeriSign hiervoor toestemming heeft verleend, is het uit hoofde van deze CPS verboden om zich toegang te verschaffen tot enige gegevens in de repository (of andere gegevens van UA's) waarvan de vertrouwelijkheid te kennen is gegeven middels de CPS en/of middels de repository.

### **3. BASIS VOOR CERTIFICATIE-ACTIVITEITEN**

---

**In dit gedeelte worden de basisvereisten beschreven voor de onder deze CPS vallende publieke certificatediensten, alsmede de controles die daartoe worden uitgevoerd. Ingegaan wordt op de eisen die worden gesteld aan de werking van de publieke certificatediensten, het beheer van administratieve gegevens, de audit-procedures en personele zaken. Ten slotte worden de verplichtingen beschreven van KPN Telecom bij beëindiging of staking van haar activiteiten.**

---

#### **3.1 Recht van VeriSign om onderzoek te doen inzake inbreuk**

KPN Telecom en VeriSign zijn gerechtigd om – voorzover de wet dit toestaat - onderzoeken in te stellen indien er sprake is van een vermeende inbreuk op het veiligheidsbeleid. Door het indienen van een certificaataanvraag verklaart de aanvrager zich akkoord met de uitvoering en de omvang van een dergelijk onderzoek. Tevens verklaart de aanvrager te zullen helpen bij het achterhalen van alle feiten, omstandigheden en andere relevante informatie die KPN Telecom en VeriSign relevant en in overeenstemming met de CPS achten, tenzij dergelijk onderzoek strijdig is met geldende wettelijke voorschriften ten aanzien van privacybescherming en gegevensbescherming. Voorbeelden van zaken die het onderzoek kunnen behelzen zijn onder andere vraaggelassen, inzage in relevante boeken, bestanden en procedures en het doen van onderzoeken en inspecties op de desbetreffende locaties. In het geval van gebruikers van certificaten kan het onderzoek onder meer vraaggelassen behelzen alsmede verzoeken tot inzage en beoordeling van documenten.

#### **3.2 Naleving van de CPS**

KPN Telecom en VeriSign zullen zorg dragen voor naleving van deze CPS bij het verzorgen van hun respectievelijke diensten.

#### **3.3 Betrouwbaarheid**

KPN Telecom en VeriSign zullen bij het verzorgen van hun respectievelijke diensten alleen gebruikmaken van betrouwbare systemen.

#### **3.4 Financiële verantwoordelijkheid**

KPN Telecom zal ervoor zorg dragen dat het beschikt over voldoende financiële middelen voor het uitvoeren van de in deze CPS beschreven diensten en taken. Daarbij dient KPN Telecom redelijkerwijs het risico te kunnen dragen van aansprakelijkheid jegens gebruikers en ontvangers van certificaten en andere personen die vertrouwen stellen in de certificaten en de aangebrachte datumstempels. KPN Telecom heeft in verband met die verplichting adequate verzekeringen afgesloten voor het afdekken van gemaakte fouten en omissies.

### **3.5 Gegevens met betrekking tot naleving van de CPS**

KPN Telecom dient, in haar hoedanigheid als UA, op een betrouwbare wijze gegevens bij te houden en op verzoek van VeriSign het volgende te overleggen:

- (i) documentatie waaruit naleving blijkt van de CPS;
- (ii) documentatie ten aanzien van activiteiten en informatie met betrekking tot certificaataanvragen en het aanmaken, uitgeven, gebruiken, blokkeren, intrekken, vervallen en het verlengen of opnieuw aanvragen van certificaten. Deze gegevens dienen tevens te zijn voorzien van alle bewijsstukken die de UA in bezit heeft met betrekking tot:
  - de identiteit van de gebruiker in het certificaat;
  - de identiteit van personen die een verzoek indienen om een certificaat te blokkeren of in te trekken;
  - andere feitelijkheden die zijn opgenomen in het certificaat;
  - datumstempels;
  - bepaalde voorzienbare feitelijkheden met betrekking tot de uitgifte van certificaten.

### **3.6 Datumstempels**

Datumstempels zijn bedoeld om de integriteit van de publieke certificatediensten en de betrouwbaarheid van certificaten van KPN Telecom te vergroten. Daarnaast dragen datumstempels bij aan de onweerlegbaarheid van digitaal door KPN Telecom ondertekende berichten.

Datumstempels vormen een notatiesysteem waarmee (tenminste) de juiste datum en tijd van een bepaalde activiteit (expliciet of impliciet) wordt vastgelegd, alsmede de identiteit van de persoon die verantwoordelijk is voor de notatie. Alle datumstempels zijn gebaseerd op Greenwich Mean Time (GMT) en werken volgens de Universal Time Conventions (UTC). Getallen met de notatie 00-69 duiden op de jaren 2000-2069; getallen met de notatie 70-99 op de jaren 1970-1999.

De volgende gegevens en bestanden worden voorzien van een datumstempel, hetzij direct op de gegevens zelf, hetzij middels een betrouwbare, controleerbare vastlegging:

- certificaten;
- CRL's en andere gegevens met betrekking tot blokkering en intrekking;
- iedere versie van de CPS;
- informatie voor gebruikers;
- andere informatie die middels deze CPS wordt vereist.

### **3.7 Bewaren van gegevens**

Gegevens met betrekking tot Klasse 3-certificaten worden tot tenminste dertig (30) jaar nadat een certificaat is ingetrokken of vervallen door KPN Telecom en Verisign bewaard. Bewaring kan zowel in elektronisch formaat als in de vorm van hard-copy geschieden.

### **3.8 Audits**

KPN Telecom zal gebruikmaken van betrouwbare en controleerbare systemen voor het vastleggen van relevante gebeurtenissen, zoals onder meer:

- aanvragen voor certificaten;
- validatie van aanvragen;
- blokkering en intrekking van certificaten.

Een openbaar accountant met aantoonbare ervaring op het gebied van computerbeveiliging danwel een bevoegde deskundige op het gebied van computerbeveiliging zal de activiteiten van KPN Telecom tenminste eens per jaar controleren. Tijdens de controles dient te worden nagegaan of deze CPS en eventuele andere geldende overeenkomsten, richtlijnen, procedures en standaards worden nageleefd.

### **3.9 Rampenplannen**

KPN Telecom is verantwoordelijk voor het implementeren, documenteren en regelmatig controleren van relevante rampenplannen en –procedures conform deze CPS en het Handboek Beveiligingsbeleid.

### **3.10 Beschikbaarheid van certificaten KPN Telecom**

KPN Telecom zal zorgen voor het maken van kopieën van haar eigen certificaten (dat wil zeggen de certificaten waarvan KPN Telecom de houder is) alsmede van eventuele intrekkinggegevens (CRL's) welke toegankelijk zijn voor personen die aan de hand daarvan digitale handtekeningen willen verifiëren.

### **3.11 Publicatie door KPN Telecom**

KPN Telecom is verantwoordelijk voor de publicatie van haar certificaat, de CRL en deze CPS.

### **3.12 Vertrouwelijke informatie**

De volgende informatie dient op vertrouwelijke wijze door zowel KPN Telecom als VeriSign te worden behandeld;

- Informatie met betrekking tot certificaataanvragen (uitgezonderd die informatie die conform deze CPS in een certificaat of in de repository wordt geplaatst);
- Gebruikersovereenkomsten;
- Bestanden met betrekking tot transacties (zowel de volledige bestanden als de audit gegevens van transacties);
- Controleerbare vastleggingen door of in het bezit van KPN Telecom of VeriSign (audit logs);
- Audit-rapporten die zijn samengesteld door KPN Telecom of VeriSign danwel hun respectievelijke auditors (zowel intern als extern);
- Rampenplannen;
- Veiligheidsmaatregelen met betrekking tot de werking van hard- en software van KPN Telecom alsmede met betrekking tot het beheer van certificaatdiensten en daartoe aangewezen aanmeldingsprocedures.

Bovenstaande informatie zal, voorzover ze betrekking heeft op de certificaathouder, niet openbaar worden gemaakt zonder expliciete toestemming van zijn kant danwel een wettelijke verplichting tot openbaarmaking. KPN Telecom en VeriSign zullen geen namen van aanvragers

of andere persoonsgegevens openbaar maken, verkopen of mededelen aan andere partijen, tenzij dit wordt toegestaan middels deze CPS en zolang dit binnen de daarvoor geldende wettelijke grenzen gebeurt.

### **3.13 Personeelsbeleid**

KPN Telecom is verantwoordelijk voor het ontwikkelen en onderhouden van een zodanig personeelsbeleid, dat op grond daarvan met redelijke zekerheid kan worden aangenomen dat de medewerkers betrouwbaar en vakbekwaam zijn en dat ze hun taken naar tevredenheid zullen uitvoeren. Het beleid dient in overeenstemming te zijn met deze CPS.

#### **3.13.1 Vertrouwensposities**

Alle werknemers van KPN Telecom of door haar ingeschakelde personen (hierna te noemen “personeel”) die toegang hebben tot of controle uitoefenen over cryptografische bewerkingen welke de uitgifte, het gebruik, het blokkeren of intrekken van certificaten door KPN Telecom wezenlijk kunnen beïnvloeden (met inbegrip van het uitvoeren van gelimiteerde activiteiten in de repository) bevinden zich uit hoofde van deze CPS in een vertrouwenspositie. Voorbeelden van dergelijk personeel zijn:

- Personeel in de back-office;
- Systeembeheerders;
- Bepaalde technische medewerkers;
- Leidinggevenden die tot taak hebben toe te zien op een betrouwbare systeeminfrastructuur.

#### **3.13.2 Onderzoek en naleving**

KPN Telecom zal een vooronderzoek uitvoeren met betrekking tot kandidaten voor vertrouwensposities. Doel hiervan is om na te gaan of de kandidaat in kwestie betrouwbaar is en geschikt is voor de functie. Daarnaast zal KPN Telecom regelmatig onderzoeken uitvoeren ten aanzien van alle personen in vertrouwensposities om na te gaan of deze personen nog steeds betrouwbaar zijn en geschikt om de taken te vervullen in overeenstemming met het personeelsbeleid.

#### **3.13.3 Ontheffing van taken van personen in vertrouwensposities**

Personeel dat niet voldoet aan de eisen die gesteld worden tijdens een vooronderzoek of periodiek onderzoek, mag geen vertrouwenspositie meer innemen. KPN Telecom zal er in dat geval op toezien (of VeriSign, indien er sprake is van personeel van VeriSign) dat zulk personeel wordt ontheven van haar taken.

### **3.14 Accreditaties**

#### **3.14.1 Goedkeuring van software en hardware**

Alle software en hardware die wordt gebruikt in het kader van de publieke certificatediensten is goedgekeurd door VeriSign, een door VeriSign erkende consultant of, indien van toepassing, een andere erkende autoriteit.

### **3.14.2 Personeel in vertrouwensposities**

Het personeel in vertrouwensposities zal worden geaccrediteerd door het opvragen van een bewijs van gedrag bij de justitiële autoriteiten (via gemeentelijke instanties). Deze verplichting geldt niet voor de leden van de Raad van Bestuur van KPN Telecom en van Verisign, behalve wanneer die leden (tevens) operationele bevoegdheden binnen de publieke certificatediensten bekleden.

### **3.15 Genereren van sleutels door KPN Telecom**

KPN Telecom en Verisign zullen hun geheime sleutel(s) op een veilige manier genereren en op adequate wijze beschermen, met gebruikmaking van een betrouwbaar systeem. KPN Telecom en Verisign zullen de nodige voorzorgsmaatregelen nemen teneinde verlies, openbaarmaking, aanpassing of ongeoorloofd gebruik van deze sleutel(s) te voorkomen.

### **3.16 Gedeelde geheimhouding**

KPN Telecom en Verisign maken van een proces van gedeelde geheimhouding (zie definities) via een aantal geautoriseerde houders van geheime delen, om de betrouwbaarheid van hun geheime sleutel(s) te vergroten. Als klasse 3 PCA is de geheime sleutel van KPN Telecom (zijnde de RSA sleutel van Verisign) verdeeld in negen (9) geheime delen. Om het certificaat van KPN Telecom te kunnen ondertekenen, zijn tenminste vijf (5) van de negen geheime delen benodigd. Voor de uitvoering van het rampenplan (zie 3.14.5) bestaan in totaal vier (4) geheime delen, waarvan er tenminste drie (3) benodigd zijn om het plan ten uitvoer te brengen.

#### **3.16.1 Gebruik van beveiligde hardware**

KPN Telecom en Verisign maken gebruik van goedgekeurde, betrouwbare cryptomodules voor alle bewerkingen waarbij een geheime sleutel wordt toegepast. De procedure voor het aanmaken van geheime sleutels zal worden gepubliceerd in de repository van KPN Telecom.

#### **3.16.2 Waarborgen**

Bij de verdeling van de geheime sleutel(s) waarborgen KPN Telecom en Verisign jegens alle betrokken entiteiten dat ze de desbetreffende geheime sleutel(s) op rechtmatige wijze in haar bezit houdt en dat ze de bevoegdheid heeft om deze te verdelen over de hiertoe specifiek geautoriseerde houders, op een wijze conform deze CPS.

#### **3.16.3 Acceptatie van geheime delen door houders van geheime delen**

Alvorens een houder een geheim deel accepteert, dient een meerderheid van de aangewezen houders persoonlijk kennis te hebben genomen van het aanmaken, opnieuw aanmaken en splitsen van geheime delen en het daaropvolgende proces van bewaring.

Iedere houder dient het geheime deel te ontvangen in een fysiek medium, zoals een door VeriSign goedgekeurde hardwaretoken. Nadat de houder het ontvangen geheime deel naar tevredenheid heeft geïnspecteerd, zal hij de acceptatie van het geheime deel bevestigen door het acceptatieformulier te ondertekenen en terug te sturen naar KPN Telecom.

#### **3.16.4 Bescherming van het geheime deel**

De houder van het geheime deel dient gebruik te maken van betrouwbare systemen om het geheime deel tegen inbreuk te beschermen. Tenzij dit expliciet wordt toegestaan middels deze CPS, zal de houder van een geheim deel zich onthouden van:

- het openbaar maken, kopiëren of verstrekken aan derde partijen van het geheime deel, of op enige andere wijze ongeoorloofd gebruikmaken van het geheime deel;
- het openbaar maken (expliciet of impliciet) van het feit dat hij – of enige andere houder – in het bezit is van een geheim deel;
- het opslaan van het geheime deel op een locatie waar het niet door anderen kan worden betrokken ingeval de houder van het geheime deel door omstandigheden zelf niet beschikbaar is voor afgifte.

#### **3.16.5 Beschikbaarheid en vrijgave van geheime delen**

De houder van een geheim deel dient het geheime deel alleen beschikbaar te stellen aan geautoriseerde entiteiten (vermeld in het door de houder ontvangen acceptatieformulier) als het een hiertoe geauthenticeerd bestand heeft ontvangen.

Wanneer er sprake is van een ramp situatie (als zodanig omschreven door de verstrekker van het geheime deel), dient de houder van een geheim deel zich te vervoegen bij een rampencentrum. Hiertoe dient hij zich te houden aan de instructies van de verstrekker van het geheime deel. Alvorens hij afreist naar het rampencentrum en overgaat tot vrijgave van het geheime deel, dient de houder de verklaring van de verstrekker van het geheime deel te authenticeren in overeenstemming met de instructies op het acceptatieformulier (tenzij dit strijdig is met wettelijke bepalingen, zoals in het geval van een strafrechtelijk onderzoek). Deze procedure omvat tevens het gebruik van een toetsingszin (bekendgemaakt door de verstrekker aan de houder van een geheim deel) om uit te sluiten dat de houder afreist naar een onjuiste locatie, waardoor het geheime deel niet zou kunnen worden gebruikt. Op het rampencentrum dient de houder zijn geheime deel persoonlijk vrij te geven.

De houder van een geheim deel mag vertrouwen stellen in alle instructies, documenten, berichten, bestanden, akten en handtekeningen waarvan hij meent dat ze authentiek zijn, vooropgesteld dat dergelijke verklaringen van de verstrekker van een geheim deel worden geauthenticeerd volgens de hierboven omschreven wijze. De verstrekker van het geheime deel zal de houder vooraf voorzien van alle handtekeningen die zullen worden gebruikt om de instructies van de verstrekker te authenticeren.

#### **3.16.6 Registratie van activiteiten**

Verstrekkers en houders van geheime delen dienen alle activiteiten met betrekking tot het proces van gedeelde geheimhouding te registreren. Indien de verstrekker van een geheim deel (of een aangewezen instantie) hiertoe een geauthenticeerd verzoek indient, zal de houder van het geheime deel informatie overleggen met betrekking tot de status van het geheime deel.

### **3.16.7 Verplichtingen van de houder van een geheim deel**

De houder van een geheim deel dient zijn verplichtingen uit hoofde van deze CPS te vervullen en zich in alle opzichten tactvol en verantwoordelijk te gedragen. De houder van een geheim deel dient de verstrekker van het geheime deel onmiddellijk op de hoogte te brengen van verlies, diefstal, ongeoorloofde openbaarmaking of schending van het geheime deel.

De houder van een geheim deel is niet verantwoordelijk voor het niet kunnen nakomen van zijn verplichtingen als hij geen invloed heeft kunnen uitoefenen op de oorzaak hiervan. De houder kan wel aansprakelijk worden gesteld ingeval van oneigenlijke openbaarmaking van een geheim deel, of indien hij de verstrekker niet op de hoogte stelt van oneigenlijk gebruik of inbreuk als gevolg van een fout die hem kan worden toegerekend (waaronder nalatigheid of roekeloos gedrag).

### **3.16.8 Vrijwaring door de verstrekker van een geheim deel**

De verstrekker van een geheim deel zal de houder van een geheim deel vrijwaren jegens alle aanspraken, gedingen, dwangsommen, vonnissen, arbitrage-vergoedingen, uitgaven, kosten (waaronder begrepen die van rechtsbijstand) en andere verplichtingen die niet (deels) worden veroorzaakt door een fout van de houder van het geheime deel (waaronder nalatigheid of roekeloos gedrag).

## **3.17 Beveiliging**

### **3.17.1 Beveiliging van de communicatie**

Communicatie tussen KPN Telecom en de andere partijen binnen de publieke certificatediensten vinden plaats via voorzieningen die eventuele risico's op adequate wijze afdekken. Alle elektronische mededelingen, bevestigingen van ontvangst en andere vormen van communicatie tussen partijen zullen steeds op afdoende wijze worden beveiligd.

### **3.17.2 Beveiliging van de te gebruiken voorzieningen**

KPN Telecom zal gebruikmaken van betrouwbare voorzieningen die minimaal in overeenstemming zijn met de bepalingen in het Handboek Beveiligingsbeleid.

## **3.18 Eisen ten aanzien van medewerkers van Registratie-Autoriteiten**

Bij het leveren van de diensten onder deze CPS vervult KPN Telecom niet alleen de rol van UA, maar ook van RA (Registratie Autoriteit). Personeel van KPN Telecom dat zich bezighoudt met het registratieproces (met name de aanvraagprocedure) of daaraan gerelateerde activiteiten bevinden zich in een vertrouwenspositie. Tabel 1 geeft de eisen voor zulk personeel weer.

	<b>RA-MEDEWERKER KLASSE 3 SERVER CERTIFICAAT</b>
<b>OPLEIDING</b>	Ten minste twee jaar universiteit, afronding van een introductie cursus voor notarissen of vergelijkbare ervaring
<b>TRAINING</b>	Twee weken introductie en ten minste drie maanden in dienst van de RA.
<b>ACCREDITATIES</b>	Bewijs van gedrag, uit te geven door justitie via gemeentelijke autoriteiten. De werknemer dient een goede reputatie te hebben bij zijn of haar RA
<b>INITIEEL ONDERZOEK</b>	Afhankelijk van de eisen die gelden voor een vertrouwenspositie
<b>VOORTGEZET ONDERZOEK</b>	Eens per jaar
<b>BIJHOUDEN VAN GEGEVENS</b>	Ja, conform artikel 3.3 CPS

**Tabel 1 –Eisen die worden gesteld aan RA-medewerkers**

### **3.19 Beëindiging van activiteiten door KPN Telecom**

De volgende verplichtingen zijn bedoeld om nadelige effecten die een eventuele beëindiging van de onder deze CPS vallende certificatie diensten door KPN Telecom zou kunnen hebben voor gebruikers daarvan, zoveel mogelijk te beperken. KPN Telecom zal de genoemde verplichtingen voor, tijdens en na beëindiging van de diensten in acht nemen.

#### **3.19.1 Voorwaarden aan beëindiging**

Alvorens KPN Telecom definitief besluit te stoppen met de onder deze CPS vallende certificatie diensten, dient ze:

- (i) Verisign in te lichten over haar intentie om de activiteiten als UA te beëindigen. Deze kennisgeving dient plaats te vinden tenminste negentig (90) dagen alvorens de UA ophoudt te bestaan. Verisign mag aanvullende verklaringen vereisen, teneinde zeker te stellen dat deze verplichting wordt nageleefd.
- (ii) Alle gebruikers van certificaten die niet zijn geblokkeerd of ingetrokken in te lichten over de intentie om de activiteiten als UA te beëindigen. Deze kennisgeving dient plaats te vinden tenminste negentig (90) dagen alvorens de UA ophoudt te bestaan.
- (iii) Alle certificaten in te trekken die aan het eind van genoemde periode van negentig (90) dagen nog niet zijn geblokkeerd of ingetrokken, ongeacht het feit of de gebruikers al dan niet om intrekking hebben verzocht. Deze intrekking dient vervolgens medegedeeld te worden aan alle betrokken gebruikers, conform paragraaf 9 van de CPS.
- (iv) Redelijke pogingen te doen om ervoor te zorgen dat gebruikers zo weinig mogelijk hinder ondervinden van de beëindiging van certificatie diensten.
- (v) Voorzieningen te treffen voor het bewaren van administratieve gegevens.
- (vi) Een redelijke vergoeding te betalen (niet hoger dan het aankoopbedrag van het certificaat) aan gebruikers voor het intrekken van de certificaten van deze gebruikers voor de vervaldatum.

#### **3.19.2 Heruitgifte van certificaten door een nieuwe UA**

Teneinde te zorgen voor een ongestoorde dienstverlening aan haar aanvragers en gebruikers, zal KPN Telecom wanneer ze haar activiteiten beëindigt een regeling te treffen met een andere UA om heruitgifte mogelijk te maken van uitstaande gebruikerscertificaten. Bij de heruitgifte van

certificaten worden alle rechten en verplichtingen overgedragen op de nieuwe UA (niet te verwarren met een ondergeschikte UA), alsmede – indien dit schriftelijk wordt overeengekomen – alle rechten en verplichtingen met betrekking tot uitstaande certificaten. De CPS blijft onverminderd van kracht, tenzij beide partijen anders overeenkomen.

Partijen kunnen afwijkende bepalingen overeenkomen, mits voornoemde bepalingen alleen gelden voor de contractuele partijen.

## 4. AANVRAAGPROCEDURE CERTIFICAAT

---

**In dit gedeelte wordt de procedure beschreven voor het aanvragen van een certificaat. Hierbij wordt tevens ingegaan op de eisen voor het genereren en beveiligen van een sleutelpaar en een opsomming van de informatie die nodig is voor iedere certificaatklasse**

---

### 4.1 Algemene beschrijving procedures

Een persoon, bedrijf of instelling die een KPN Telecom server certificaat wenst, dient voor iedere certificaataanvraag de volgende procedure te volgen:

- Via de server software een sleutelpaar (geheime en publieke sleutel) genereren en aan KPN Telecom tonen dat dit een functionerend sleutelpaar is;
- De geheime sleutel beschermen tegen inbreuk door derden;
- De publieke sleutel samen met de certificaataanvraag via de website naar KPN Telecom sturen;
- Een distinguished name (zie definities) bepalen;
- De gebruikersovereenkomst op de website van KPN Telecom accepteren.

### 4.2 Genereren en beheren van sleutels

De volgende bepalingen zijn van toepassing op alle personen, bedrijven of instellingen die als onderdeel van bovengenoemde procedure zelf sleutelparen genereren. Opgemerkt moet worden dat voor de aanvraag en uitgifte van een KPN Telecom server certificaat een volledig elektronische procedure wordt gehanteerd; aanmelding is dan ook alleen mogelijk via de website van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>).

#### 4.2.1 Verplichtingen ten aanzien van sleutelparen

Tenzij anders bepaald in deze CPS, dient iedere certificaataanvrager zijn of haar eigen sleutelpaar te genereren via de server software. Bij de generatie dient de aanvrager gebruik te maken van een betrouwbaar systeem en de noodzakelijke voorzorgsmaatregelen te nemen om inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik van met name de geheime sleutel te voorkomen. Voor meer informatie daaromtrent zie het vraag-antwoord document met betrekking tot bescherming van geheime sleutels (<https://www.kpn-telecom.nl/certificaat>)

Iedere gebruiker van een certificaat verklaart dat hij alleen - en niet KPN Telecom of Verisign - verantwoordelijk is voor de bescherming van zijn geheime sleutel(s) tegen inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik. Tijdens het aanmaken en installeren ervan dient de gebruiker de geheime sleutel dan ook te beveiligen met een – zelf te kiezen – toegangscode (password). Wanneer de server software verschillende niveau's van beveiliging van de geheime sleutel mogelijk maakt, dient de gebruiker tenminste dat niveau te kiezen dat van een toegangscode gebruik maakt.

Iedere gebruiker is gehouden om de publieke certificatediensten van KPN Telecom en Verisign als zodanig niet te verstoren, te verhinderen, te beschadigen of er reverse engineering op toe te

passen, tenzij expliciet toegestaan in deze CPS of door voorafgaande schriftelijke toestemming van KPN Telecom danwel VeriSign. Elke handeling die ingaat tegen dit gebod kan een grond voor intrekking van certificaten van betrokkene opleveren.

#### 4.2.2 Overdracht van verantwoordelijkheid geheime sleutel(s)

Wanneer de verantwoordelijkheid voor een geheime sleutel wordt overgedragen, ontslaat dat degene die overdraagt niet van zijn of haar verplichtingen en aansprakelijkheden met betrekking tot het op veilige en betrouwbare wijze gebruiken, beheren, in bewaring houden of wijze vernietigen van de geheime sleutel op een wijze conform deze CPS. Overdracht van de verantwoordelijkheid voor een geheime sleutel kan voorts alleen plaatsvinden wanneer de nieuw verantwoordelijke te dien aanzien dezelfde verplichtingen en aansprakelijkheden in acht neemt als zijn voorganger en zich conformeert aan de bepalingen van deze CPS.

#### 4.3 Informatie en communicatie met betrekking tot certificaataanvragen

Om een certificaataanvraag in behandeling te kunnen nemen, is de informatie nodig zoals beschreven in onderstaande tabel (Tabel 2). Let wel: niet alle informatie zal uiteindelijk in het certificaat worden opgenomen. De informatie die wel in het certificaat terecht komt, is in onderstaande tabel aangeduid met een asterisk (\*). Alle informatie die niet in het certificaat is opgenomen, zal door KPN Telecom en Verisign vertrouwelijk worden behandeld.

CERTIFICAAT	VEREISTE INFORMATIE VOOR AANVRAAG
<b>SERVER CERTIFICAAT KLASSE 3</b>	<ul style="list-style-type: none"> <li>• Domeinnaam*</li> <li>• Organisatie*</li> <li>• Organisatorische eenheid (indien van toepassing)*</li> <li>• Contactpersonen voor technische aangelegenheden en facturering</li> <li>• Woonplaats, provincie, land*</li> <li>• Postcode</li> <li>• Telefoon, fax, E-mail</li> <li>• Nummer Kamer van Koophandel en/of Dunn &amp; Bradstreet</li> <li>• Toetsingszin</li> </ul>

**TABEL 2 – VEREISTE INFORMATIE MET BETREKKING TOT CERTIFICAATAANVRAAG**

## 5. VALIDATIE VAN CERTIFICAATAANVRAGEN

---

**In dit gedeelte worden de eisen genoemd voor validatie van certificaataanvragen door de betreffende UA of door een daartoe bevoegde lokale registratie-autoriteit. Ook worden de procedures toegelicht voor aanvragen die niet kunnen worden gevalideerd.**

---

### 5.1 Doelstelling validatie

Na ontvangst van een certificaataanvraag zal KPN Telecom een aantal validaties uitvoeren om de aangemelde gegevens op hun echtheid te controleren. Via de validatieprocedure tracht KPN Telecom te bevestigen dat:

- (a) de certificaataanvrager het bedrijf of de instelling is die in de aanvraag wordt genoemd;
- (b) de certificaataanvrager een bestaand bedrijf of instelling is;
- (c) de certificaataanvrager de houder danwel rechtmatig gebruiker is van de opgegeven InterNIC domeinnaam;
- (d) de certificaataanvrager de rechtmatige houder is van de geheime sleutel welke correspondeert met de publieke sleutel die in het certificaat moet worden vermeld (deze verplichting kan worden vervuld door middel van een verklaring hieromtrent van de certificaataanvrager);
- (e) de informatie die in het certificaat moet worden opgenomen correct is, met uitzondering van die gegevens die niet worden gevalideerd (in dit geval de organisatorische eenheid);
- (f) eventuele vertegenwoordigers die namens een zakelijke entiteit een aanvraag indienen hiertoe gerechtigd zijn.

### 5.2 Eenmalig karakter validatie

Zodra een certificaat is uitgegeven, vervalt de plicht van KPN Telecom om de juistheid van de informatie in een certificaat te (blijven) bewaken en onderzoeken. Het uitgegeven certificaat is een jaar geldig en vormt gedurende die tijd een momentopname van de omstandigheden tijdens de aanvraag en de daarop volgende validatieprocedure. Slechts wanneer KPN Telecom gedurende de looptijd door de gebruiker van een certificaat danwel een derde partij op de hoogte wordt gesteld van omissies in of verandering van de gecertificeerde gegevens, zal de inhoud van een certificaat door haar opnieuw worden beoordeeld.

### 5.3 Eisen validatie

Voor de validatie van klasse 3 server certificaten gelden de volgende eisen:

- Bevestiging door derden van bestaan en benaming zakelijke entiteit
- Bevestiging van InterNIC domeinnaam

KPN Telecom behoudt zich het recht voor deze validatieprocedures aan te passen ter verbetering van het validatieproces. Aangepaste validatieprocedures worden, zodra ze worden vrijgegeven, opgenomen in een nieuwe versie van de CPS en geplaatst in de KPN Telecom repository.

### **5.3.1 Bevestiging door derden van bestaan en benaming zakelijke entiteiten**

KPN Telecom zal de bij de aanvraag ingediende gegevens nagaan bij de Kamer van Koophandel en/of bij Dunn & Bradstreet. Eventueel zal via een (meestal telefonische) steekproef getracht worden om bepaalde informatie bevestigd te krijgen, bijvoorbeeld de positie van een vertegenwoordiger binnen de organisatie. Mocht de daaruit voortvloeiende informatie onvoldoende basis voor bevestiging vormen, dan kan KPN Telecom een nader onderzoek starten, terwijl de certificaataanvrager in dat geval eveneens om aanvullende informatie en bewijzen kan worden verzocht.

### **5.3.2 Bevestiging InterNIC domeinnaam**

KPN Telecom zal via InterNIC nagaan of de opgegeven domeinnaam (a) daadwerkelijk bestaat en (b) toebehoort aan de aanvragende entiteit. Voor meer informatie over InterNIC procedures en garanties wordt verwezen naar hun website (<http://ds.internic.net/ds/admin.html>).

## **5.4 Goedkeuring van aanvragen**

Nadat alle vereiste onderdelen van de validatieprocedure zijn uitgevoerd, zal de aanvraag worden goedgekeurd door KPN Telecom. Deze goedkeuring leidt tot de (elektronische) uitgifte van een klasse 3 server certificaat op een wijze conform deze CPS.

## **5.5 Afwijzing van een certificaataanvraag**

Wanneer validatieprocedure niet met succes kan worden afgerond, dan zal KPN Telecom de certificaataanvraag afwijzen. De certificaataanvrager wordt dan terstond op de hoogte worden gebracht van de mislukte validatie, onder vermelding van de reden van de mislukking.

## 6. UITGIFTE VAN CERTIFICATEN

---

**In dit gedeelte wordt ingegaan op de eisen die gelden voor de uitgifte van certificaten. Tevens worden de specifieke verplichtingen genoemd die door de uitgevende autoriteiten worden aangegaan bij de uitgifte van certificaten**

---

### 6.1 Algemene procedure

Nadat een certificaataanvraag is gevalideerd en goedgekeurd geeft KPN Telecom een klasse 3 server certificaat uit. De uitgifte van een normaal certificaat is een bewijs van definitieve en volledige goedkeuring van de certificaataanvraag door KPN Telecom.

### 6.2 Toestemming van de gebruiker voor uitgifte

KPN Telecom zal geen certificaten uitgeven zonder toestemming van de aanvrager. Toestemming voor uitgifte wordt voorondersteld aanwezig te zijn op basis van de ingediende aanvraag, ondanks het feit dat acceptatie van het certificaat door de aanvrager dan nog niet heeft plaatsgevonden.

### 6.3 Weigering tot uitgifte van een certificaat

KPN Telecom kan naar eigen goeddunken weigeren een certificaat uit te geven aan eenieder, zonder dat dit leidt tot enige vorm van aansprakelijkheid of verantwoordelijkheid voor enige schade of onkosten die het gevolg zijn van een dergelijke weigering.

### 6.4 Verplichtingen van KPN Telecom bij uitgifte

#### 6.4.1 Verplichtingen van KPN Telecom tegenover de gebruiker

Tenzij anders bepaald in deze CPS, of tenzij KPN Telecom en de gebruiker van het certificaat anders overeenkomen in een rechtsgeldig document, verzekert KPN Telecom de in het certificaat genoemde gebruiker ervan dat:

- (a) de door de aanvrager verstrekte gegevens op correcte wijze in het certificaat zijn opgenomen;
- (b) er bij de invoering van gegevens die door KPN Telecom van de certificaataanvrager zijn ontvangen geen fouten zijn optreden die het gevolg zijn van het niet in acht nemen van voldoende zorgvuldigheid door KPN Telecom bij het aanmaken van het certificaat;
- (c) het certificaat voldoet aan alle materiële eisen van deze CPS.

Tenzij anders bepaald in deze CPS, of tenzij KPN Telecom en de gebruiker van het certificaat anders overeenkomen in een rechtsgeldig document, verbindt KPN Telecom zich jegens de gebruiker om zich in voldoende mate in te spannen om conform de voorwaarden in deze CPS:

- (a) terstond certificaten te blokkeren of in te trekken;
- (b) gebruikers op de hoogte te brengen van haar bekende feiten die een materiële invloed hebben op de geldigheid en betrouwbaarheid van het aan de betrokken gebruiker uitgegeven certificaat.

De hierboven genoemde verplichtingen en beloften worden uitsluitend aangegaan ten behoeve van de gebruiker en komen niet ten goede aan of zijn afdwingbaar door enige andere partij. KPN Telecom zal ervoor zorg dragen dat haar handelwijze in overeenstemming is met deze CPS en met de toepasselijke wetten.

#### **6.4.2 Verplichtingen van KPN Telecom tegenover relying parties**

Door uitgifte van een certificaat verplicht KPN Telecom zich ten opzichte van allen die redelijkerwijs kunnen vertrouwen op een digitale handtekening die verifieerbaar is met behulp van de publieke sleutel in het certificaat dat:

- (i) het certificaat is uitgegeven aan de gebruiker en dat deze het certificaat heeft geaccepteerd conform deze CPS;
- (ii) alle informatie die zich bevindt in of waarnaar wordt verwezen in het certificaat op het moment van validatie correct was of redelijkerwijs leek te zijn;
- (iii) KPN Telecom heeft voldaan aan de eisen van deze CPS bij de uitgifte van het certificaat.

#### **6.4.3 Beperkingen aan de verplichtingen van KPN Telecom**

Voornoemde verplichtingen gelden onder de voorwaarden in de gebruikersovereenkomst, de overeenkomst voor relying parties en deze CPS.

#### **6.5 Tijdstip van certificaatuitgifte**

KPN Telecom zal zich in voldoende mate inspannen om informatie uit certificaataanvragen zo spoedig mogelijk te bevestigen en om, zodra alle relevante informatie door KPN Telecom is ontvangen, de uitgifte van klasse 3 server certificaten te realiseren binnen 1-3 werkdagen. Of KPN Telecom en VeriSign binnen deze indicatie kunnen blijven is afhankelijk van de tijdige verstrekking door de aanvrager van volledige en accurate informatie. Daarnaast is het van belang dat door de aanvrager adequaat wordt gereageerd op alle administratieve verzoeken van KPN Telecom en VeriSign.

#### **6.6 Geldigheid en geldigheidsduur van certificaten**

De geldigheidsduur voor KPN Telecom klasse 3 server certificaten is een (1) jaar, behoudens eerdere beëindiging van de looptijd ten gevolge van blokkering of intrekking. Alle certificaten worden als geldig beschouwd zodra uitgifte door KPN Telecom en acceptatie door de gebruiker heeft plaatsgevonden, te rekenen vanaf de dag en het tijdstip van uitgifte, tenzij een latere dag en tijdstip wordt aangegeven in het certificaat (nooit langer dan zestig dagen). De geldigheidsduur begint steeds op de in het certificaat aangegevendatum en tijdstip, zelfs als het certificaat nog niet is geaccepteerd.

#### **6.7 Beperkingen op uitgegeven maar nog niet geaccepteerde certificaten**

Voordat het certificaat door hem geaccepteerd is, mag de gebruiker geen digitale handtekeningen aanmaken met behulp van een geheime sleutel die overeenkomt met de in het certificaat vermelde publieke sleutel (of anderszins gebruikmaken van een dergelijke geheime sleutel).

## **7. ACCEPTATIE VAN CERTIFICATEN DOOR GEBRUIKERS**

---

**In dit gedeelte wordt ingegaan op de eisen voor acceptatie van certificaten door gebruikers. Tevens worden de waarborgen door gebruikers bij acceptatie, de verplichtingen van de gebruikers om hun geheime sleutels te beschermen en de procedures voor publicatie van certificaten nader verklaard.**

---

### **7.1 Acceptatie van een certificaat**

Een gebruik wordt geacht een certificaat te hebben geaccepteerd na uitgifte van het certificaat door KPN Telecom. De tijdstempel in het certificaat is bepalend voor het moment van uitgifte en acceptatie.

KPN Telecom zal, na uitgifte, het certificaat per E-mail aan de gebruiker doen toekomen. Na ontvangst van het certificaat dient de gebruiker na te gaan of er eventuele onnauwkeurigheden of onvolkomenheden in het certificaat aanwezig zijn. Is dat het geval, dan dient hij zo spoedig mogelijk contact op te nemen met KPN Telecom.

#### **7.1.1 Wijziging van gecertificeerde gegevens na acceptatie**

Vanaf het moment van acceptatie van een klasse 3 server certificaat heeft de gebruiker een termijn van vijftien (15) dagen om KPN Telecom te verzoeken om de gecertificeerde gegevens te wijzigen, in zoverre deze gegevens onjuist of onvolledig zijn. KPN Telecom zal het certificaat dan intrekken, waar nodig de nieuw verschaft gegevens valideren en (kosteloos) een nieuw klasse 3 server certificaat aan de gebruiker verstrekken. De mogelijkheid tot wijziging raakt met de uitgifte van het nieuwe certificaat uitgeput, hoewel de gebruiker ervan nog wel aanspraak kan maken op de restitutie-termijn van paragraaf 7.1.2. van deze CPS.

#### **7.1.2 Restitutie na acceptatie**

Vanaf het moment van acceptatie van een klasse 3 server certificaat heeft de gebruiker een termijn van vijftien (15) dagen om het gebruik van de dienst te beëindigen en KPN Telecom om restitutie te verzoeken. Wordt een dergelijk verzoek gedaan, dan dient de gebruiker de procedure voor kennisgeving uit deze CPS te volgen (zie 12.9) en zich tegenover KPN Telecom te authenticeren via zijn toetsingszin. Vervolgens zal KPN Telecom het bewuste certificaat zo spoedig mogelijk intrekken en binnen een redelijke termijn tot restitutie overgaan.

### **7.2 Garanties gebruiker door acceptatie certificaat**

Door acceptatie van een door KPN Telecom uitgegeven certificaat verklaart de gebruiker tegenover KPN Telecom en tegenover allen die redelijkerwijs vertrouwen op de informatie in het certificaat, dat ten tijde van de acceptatie en gedurende de volledige geldigheidsduur van het certificaat, tenzij anders kenbaar gemaakt door de gebruiker:

- (i) Iedere digitale handtekening vervaardigd met behulp van de geheime sleutel die correspondeert met de publieke sleutel in het certificaat, de digitale handtekening van de

- gebruiker is en dat het certificaat is geaccepteerd en geldig is (niet verlopen, geblokkeerd of ingetrokken) op het moment dat de digitale handtekening werd gezet;
- (ii) Geen enkele onbevoegde persoon toegang heeft gehad tot de geheime sleutel van de gebruiker;
  - (iii) Alle gegevens die de gebruiker aan KPN Telecom heeft verstrekt ten behoeve van de onder deze CPS vallende diensten juist en volledig zijn;
  - (iv) Alle in het certificaat verwerkte gegevens juist en volledig zijn, tenzij de gebruiker KPN Telecom op een wijze conform deze CPS op de hoogte heeft gesteld van het feit dat deze gegevens niet juist of volledig zijn;
  - (v) Het certificaat uitsluitend gebruikt zal worden voor wettelijke doeleinden die verenigbaar zijn met deze CPS;
  - (vi) De gebruiker een eindgebruiker is en geen UA, en dat hij de geheime sleutel die correspondeert met de publieke sleutel in het certificaat niet zal gebruiken voor de ondertekening van een certificaat, een andere vorm van gecertificeerde publieke sleutel, een CRL, als UA of anderszins, tenzij uitdrukkelijk schriftelijk overeengekomen tussen de gebruiker en KPN Telecom.

### **7.3 Verplichtingen gebruiker door acceptatie certificaat**

Door acceptatie van een certificaat verklaart de gebruiker tegenover KPN Telecom:

- (i) Dat hij akkoord gaat met de voorwaarden in deze CPS;
- (ii) Dat hij zijn geheime sleutel goed zal beheren en afdoende voorzorgsmaatregelen zal nemen om verlies, openbaarmaking, wijziging of onbevoegd gebruik te voorkomen.

### **7.4 Vrijwaring door de gebruiker**

Door acceptatie van een certificaat verklaart de gebruiker dat hij KPN Telecom, VeriSign en hun vertegenwoordigers en contractanten zal vrijwaren van enige schade als gevolg van handelingen of verzuimen van gebruiker die leiden tot aansprakelijkheid, schade of benadeling, alsmede eventuele gerechtelijke procedures en daaruit voortvloeiende kosten (met inbegrip van redelijke kosten voor rechtsbijstand) voor KPN Telecom, VeriSign en hun vertegenwoordigers en contractanten, veroorzaakt door het gebruik of de publicatie van een certificaat en voortkomend uit:

- (i) Het al dan niet bewust verstrekken van onjuiste of onvolledige gegevens door of namens de gebruiker aan KPN Telecom;
- (ii) Verzuim door de gebruiker om een relevant materieel feit binnen een redelijke termijn aan KPN Telecom te melden op een wijze conform deze CPS, al dan niet bewust bedoeld om KPN Telecom, VeriSign of enig ander persoon die het certificaat ontvangt of erop vertrouwt te misleiden; of
- (iii) Verzuim van de gebruiker om de geheime sleutel te beschermen, gebruik te maken van een betrouwbaar systeem of anderszins noodzakelijke voorzorgsmaatregelen te nemen om inbreuk, verlies, openbaarmaking, wijziging of onbevoegd gebruik van de geheime sleutel van de gebruiker te voorkomen.

Wanneer een certificaat wordt uitgegeven op verzoek van een vertegenwoordiger van de gebruiker, dienen zowel deze vertegenwoordiger als de gebruiker zelf gezamenlijk en elk

afzonderlijk KPN Telecom, VeriSign en hun vertegenwoordigers en contractanten te vrijwaren in overeenstemming met deze bepaling. De gebruiker heeft een voortdurende plicht om de certificaatuitgever op de hoogte te houden van eventuele verkeerde voorstellingen van zaken en verzuimen door een vertegenwoordiger.

## **7.5 Publicatie**

Nadat de gebruiker het certificaat heeft geaccepteerd, zal KPN Telecom een kopie van het certificaat publiceren in de repository en in één of meer andere repository's, zoals bepaald door KPN Telecom en VeriSign. Gebruikers mogen hun certificaten publiceren in andere repository's.

## **8. GEBRUIK VAN CERTIFICATEN VOOR DIGITALE HANDTEKENINGEN**

---

**In dit gedeelte wordt ingegaan op de rechten en plichten van de partijen (zie definitie) met betrekking tot het gebruik van digitale handtekeningen en digitaal ondertekende berichten die corresponderen met door KPN Telecom uitgegeven certificaten.**

---

### **8.1 Doelstelling verificatie digitale handtekeningen**

Verificatie van een digitale handtekening wordt verricht om te bepalen dat:

- (i) de digitale handtekening is aangemaakt met behulp van de geheime sleutel die correspondeert met de publieke sleutel die is vermeld in het certificaat van de ondertekenaar, en
- (ii) het bijbehorende bericht geen wijzigingen heeft ondergaan nadat de digitale handtekening is aangemaakt.

### **8.2 Methode van verificatie**

Verificatie van digitale handtekeningen gekoppeld aan certificaten van KPN Telecom dient te worden verricht op een manier die strookt met deze CPS, en wel als volgt:

- Vaststellen van een certificatieketen voor de digitale handtekening
- Nagaan van meest geschikte certificatieketen
- Controleren van geblokkeerde of ingetrokken certificaten in de keten
- Begrenzen van gegevens waaraan digitale handtekeningen worden gekoppeld
- Aangeven tijd en datum waarop digitale handtekening is aangemaakt
- Vaststellen van de garanties zoals die zijn bedoeld door de ondertekenaar
- Nagaan beperkingen geheime sleutel binnen de certificatieketen
- Bevestiging van een certificatieketen

#### **8.2.1 Vaststellen van een certificatieketen voor de digitale handtekening**

Een digitale handtekening dient te worden geverifieerd om een succesvolle bevestiging te verkrijgen van een certificatieketen.

#### **8.2.2 Nagaan van meest geschikte certificatieketen**

Het is mogelijk om meer dan één geldige certificatieketen te hebben die kan worden herleid vanaf een bepaald certificaat tot aan een root (zoals via cross-certification). Indien er meer dan één certificatieketen kan worden herleid, heeft degene die de digitale handtekening verifieert verschillende keuzemogelijkheden voor de selectie van een certificatieketen en de validatie ervan. Het is bijvoorbeeld mogelijk dat een PCA met een hoge betrouwbaarheidsgraad wordt gecertificeerd door een PCA met een lagere betrouwbaarheidsgraad. In dat geval kan degene die de digitale handtekening verifieert er de voorkeur aan geven de certificatieketen te gebruiken die eindigt in de PCA met de hoge betrouwbaarheidsgraad boven de keten die eindigt in de PCA met

de lagere betrouwbaarheidsgraad. Tevens kan hij er voor kiezen om de certificatieketen te gebruiken die eindigt in de root.

### **8.2.3 Controleren van geblokkeerde of ingetrokken certificaten in de keten**

De ontvanger dient vast te stellen of er certificaten zijn in de keten van de ondertekenaar tot aan de root die zijn geblokkeerd of ingetrokken; een blokkering of intrekking heeft immers tot gevolg dat de geldigheid van bepaalde digitale handtekeningen in de keten voortijdig wordt beëindigd. Of dat het geval is, kan op twee verschillende manieren worden vastgesteld. Ten eerste kan de repository van KPN Telecom worden geraadpleegd, om zo de meest actuele status van de certificaten in de keten te verkrijgen. Daarnaast is het ook mogelijk dat de certificatieketen is voorzien van een of meer CRL's. Deze CRL 's kunnen dan worden gebruikt om de intrekkingstatus van certificaten in de keten vast te stellen.

### **8.2.4 Begrenzen gegevens waaraan digitale handtekeningen worden gekoppeld**

Met het oog op verificatie van een digitale handtekening is het nodig precies te weten welke gegevens worden ondertekend. Wordt een standaard voor publieke sleutel cryptografie gebruikt (Public Key Cryptography Standaard), dan bevat die een getekend berichtenformaat specifiek ter aanduiding van de ondertekende gegevens.

### **8.2.5 Aangeven van tijd en datum waarop digitale handtekening is aangemaakt**

Om ondersteuning voor onweerlegbaarheid (non-repudiation) te bieden, moeten de gegevens waaraan een digitale handtekening wordt gekoppeld voorzien zijn van een tijdstempel of een referentie naar zo'n stempel bevatten. De tijdstempel dient het moment vast te leggen waarop de digitale handtekening is toegevoegd aan een bericht.

### **8.2.6 Vaststellen van de garanties zoals die zijn bedoeld door de ondertekenaar**

Er kunnen verschillende technische middelen worden gebruikt om te bepalen voor welk doel (of met welke betekenis) de digitale handtekening door de ondertekenaar is bedoeld. In formele protocollen (zoals EDI) worden digitale handtekeningen geclassificeerd als specifieke beveiligingsdiensten die dusdanig goed zijn gedefinieerd en omschreven, dat hun betekenis zo duidelijk mogelijk is. Degene die het certificaat verifieert dient tevens te bepalen of het een normaal of voorlopig certificaat betreft.

### **8.2.7 Nagaan beperkingen geheime sleutel binnen de certificatieketen**

KPN Telecom kan het aantal doeleinden waarvoor een geheime sleutel wordt gebruikt beperken. Deze beperkingen worden aangegeven in of bij het certificaat en waarschuwen ontvangers voor omstandigheden waarin het niet verstandig is te vertrouwen op het certificaat. Personen die een certificaat ontvangen en vervolgens op hun waarde moeten schatten, dienen de inhoud van dat certificaat te onderzoeken op dergelijke waarschuwingen en beperkingen om er zeker van te zijn dat de gehele certificatieketen het gebruik van de betrokken geheime sleutel autoriseert.

### **8.2.8 Bevestiging van een certificatieketen**

Bevestiging van een certificatieketen (zie definitie) is het proces waarbij eerst een certificatieketen en vervolgens een gebruikerscertificaat worden geverifieerd. Iedere UA wordt

gecertificeerd door een bovengeschatte UA (met uitzondering van de VR of andere root, die een zelf-ondertekende publieke sleutel heeft) en erft aldus het vertrouwen dat is geassocieerd met de bovengeschatte UA. Iedere UA wordt tenminste even betrouwbaar geacht als de bovengeschatte UA.

### **8.3 Gevolg van validatie van een gebruikerscertificaat**

Een digitale handtekening is bindend ten opzichte van de maker ervan indien:

- (i) de handtekening is aangemaakt tijdens de geldigheidsduur van een geldig certificaat,
- (ii) een dergelijke digitale handtekening correct kan worden geverifieerd door confirmatie van de certificatieketen,
- (iii) de relying party geen kennis heeft van of op de hoogte gesteld is van een inbreuk op de eisen van deze CPS door de ondertekenaar, en
- (iv) de relying party heeft voldaan aan alle eisen van deze CPS.

Het gebruik van certificaten is geen bewijs van bevoegdheid van enig gebruiker om te handelen namens een ander persoon of om een bepaalde handeling te verrichten. Personen die digitaal ondertekende berichten verifiëren zijn zelf verantwoordelijk voor een weloverwogen en verstandig oordeel over het vertrouwen dat ze kunnen stellen in de certificaten en digitale handtekeningen van KPN Telecom en VeriSign. Een certificaat kan niet gelijk worden gesteld aan de toekenning van enige rechten of gunsten door KPN Telecom, tenzij specifiek zo bepaald in deze CPS.

### **8.4 Procedures bij mislukte verificatie van een digitale handtekening**

Iemand die vertrouwen stelt in een niet-verifieerbare of niet-geverifieerde digitale handtekening is zelf verantwoordelijk voor alle daaraan verbonden risico's en is niet gerechtigd aan te nemen dat de digitale handtekening kan worden beschouwd als de handtekening van de gebruiker. In gevallen waarin verificatie van een certificaat door omstandigheden (bijvoorbeeld een technisch probleem) niet mogelijk blijkt, doet de ontvanger er dan ook goed aan geen enkel vertrouwen in het certificaat te stellen totdat verificatie wel mogelijk is.

### **8.5 Vertrouwen in digitale handtekeningen**

Iemand die een bericht ontvangt dat is ondertekend met een digitale handtekening van de gebruiker, kan erop vertrouwen dat deze digitale handtekening bindend is ten opzichte van de gebruiker wanneer:

- (i) de digitale handtekening is gemaakt tijdens de geldigheidsduur van een geldig certificaat en kan worden geverifieerd door middel van een gevalideerde certificatieketen, en
- (ii) dit vertrouwen onder de gegeven omstandigheden redelijk is.

Mochten de omstandigheden aanvullende garanties noodzakelijk maken, dan moet de relying party in deze garanties voorzien om te garanderen dat het vertrouwen redelijk is. De definitieve beslissing met betrekking tot het al dan niet vertrouwen op een geverifieerde digitale handtekening ligt uitsluitend bij degene die de verificatie uitvoert.

## **8.6 Geldigheid digitaal ondertekende berichten versus geschriften**

KPN Telecom, VeriSign, gebruikers van klasse 3 server certificaten alsmede relying parties verklaren voor wat betreft de onder deze CPS vallende diensten het volgende. Een digitaal ondertekend bericht, welke is geverifieerd via een publieke sleutel uit een geldig certificaat, heeft voor hen dezelfde geldigheid, effectiviteit en afdwingbaarheid bezit als een op papier geschreven en ondertekend bericht.

## **8.7 Geldigheid digitale handtekeningen versus gewone handtekeningen**

KPN Telecom, VeriSign, gebruikers van klasse 3 server certificaten alsmede relying parties verklaren voor wat betreft de onder deze CPS vallende diensten het volgende. Waar een wettelijke regel of toepasselijke praktijk een handtekening vereist of bepaalde gevolgen verbindt aan de afwezigheid van zo'n handtekening, wordt aan deze regel voldaan wanneer een bericht wordt ondertekend door een digitale handtekening, mits de handtekening kan worden geverifieerd met behulp van de publieke sleutel in een geldig certificaat.

## **8.8 Beveiligingsmaatregelen**

Personen die gebruikmaken van of vertrouwen op een door KPN Telecom uitgegeven certificaat in samenhang met een digitaal ondertekend bericht, dienen afdoende maatregelen te nemen om het bericht te authenticeren en om, indien dat vereist is, de vertrouwelijkheid van de gegevens te waarborgen.

## 9. BLOKKERING EN INTREKKING VAN CERTIFICATEN

---

**In dit gedeelte wordt ingegaan op de omstandigheden waaronder een certificaat kan (of moet) worden geblokkeerd of ingetrokken. Tevens worden de procedures toelicht voor blokkering, intrekking en herstel van certificaten.**

---

### 9.1 Intrekking van een certificaat door KPN Telecom

Een klasse 3 server certificaat zal door KPN Telecom worden ingetrokken wanneer:

- de geheime sleutel van de certificaathouder verloren is gegaan, is gestolen, gewijzigd, zonder toestemming openbaar gemaakt, of op enige andere wijze aan inbreuk heeft blootgestaan;
- de certificaathouder inbreuk heeft gepleegd op een verplichting in de gebruikersovereenkomst of in deze CPS;
- de uitvoering van verplichtingen door KPN Telecom of VeriSign op grond van de gebruikersovereenkomst of deze CPS is vertraagd of verhinderd door een van de volgende oorzaken: overmacht, een natuurramp, een computerstoring of een storing in de communicatie, door wijzigingen in statuten, regels of andere wetgeving, door een overheidsbesluit, zoals (maar niet beperkt tot) besluiten van instellingen die verantwoordelijk zijn voor exportcontrole of door een andere oorzaak die redelijkerwijs buiten de schuld van KPN Telecom of VeriSign valt en als gevolg waarvan de informatie van een andere partij in materiële zin is of zou kunnen worden bedreigd of in gevaar gebracht;
- indien de gebruiker (of een geautoriseerd vertegenwoordiger) KPN Telecom om blokkering of intrekking heeft verzocht.

In tegenstelling tot het certificaat van KPN Telecom (zie 9.2) is het momenteel nog niet mogelijk om klasse 3 server certificaten behalve in te trekken ook te blokkeren. Zodra die mogelijkheid wel bestaat, zal KPN Telecom hiervan melding maken op haar website en zal deze CPS dienaangaande worden aangepast.

#### 9.1.1. Directe intrekking van een certificaat door KPN Telecom

Onder de volgende omstandigheden zal KPN Telecom een klasse 3 server certificaat direct danwel zo spoedig mogelijk intrekken:

- (i) Wanneer de gebruiker van het certificaat een verzoek tot intrekking indient en KPN Telecom afdoende heeft vastgesteld dat degene die het verzoek doet ook inderdaad de gebruiker van dat certificaat is, of
- (ii) Wanneer KPN Telecom vaststelt dat het certificaat niet is uitgegeven conform de in deze CPS voorgeschreven procedures en nader onderzoek dit heeft bevestigd.

Intrekking van het certificaat van een gebruiker door KPN Telecom als bedoeld onder (i) kan geschieden onder de volgende voorwaarden:

- De gebruiker moet KPN Telecom uitdrukkelijk om de blokkering hebben verzocht;

- Het verzoek om intrekking moet zijn gedaan in de vorm van een elektronisch bericht, een faxbericht of een telefonisch bericht afkomstig van de gebruiker van het certificaat of van diens vertegenwoordiger;
- De afzender van het verzoek (de gebruiker van het certificaat of diens vertegenwoordiger) moet worden geauthenticeerd door middel van een toetsingszin danwel door een opsomming van bepaalde vooraf ingediende inschrijvingsinformatie.

### **9.1.2 Kennisgeving en confirmatie bij intrekking**

Na intrekking van een certificaat van een gebruiker zal KPN Telecom een kennisgeving van de intrekking publiceren in de repository. KPN Telecom zal daarbij de volgende gegevens publiceren:

- Een lijst van ingetrokken (en geblokkeerde) certificaten, beschikbaar via een beveiligd kanaal;
- Een Certificate Revocation List (CRL) die zowel ingetrokken als geblokkeerde certificaten bevat. KPN Telecom zal tenminste éénmaal per dag een nieuwe CRL publiceren voor klasse 3 server certificaten. Ook na noodgevallen dient een nieuwe CRL te worden gepubliceerd, zoals bepaald door KPN Telecom;
- Een samengestelde CRL die wordt uitgegeven door VeriSign en die is gegenereerd met behulp van CRL's welke in de repository zijn gedeponeerd door bij VeriSign betrokken UA's (waaronder KPN Telecom).

KPN Telecom zal daarnaast aan eenieder die hierom verzoekt expliciet bevestigen dat een certificaat al dan niet is ingetrokken.

## **9.2 Blokkering of intrekking van het certificaat van KPN Telecom**

VeriSign zal op eigen initiatief het certificaat van KPN Telecom blokkeren of intrekken, met of zonder toestemming, indien één van de volgende situaties optreedt:

- een feit dat in het certificaat wordt beschreven is onjuist of wordt door VeriSign op redelijke gronden onjuist geacht;
- een voorwaarde voor uitgifte van een certificaat is niet vervuld en van deze voorwaarde is ook niet afgezien;
- de geheime sleutel of het betrouwbaar systeem van KPN Telecom is in gevaar gebracht op een manier die direct invloed heeft op de betrouwbaarheid van het certificaat;
- KPN Telecom heeft als certificaathouder inbreuk gepleegd op een verplichting volgens deze CPS.

VeriSign zal KPN Telecom zo spoedig mogelijk van de blokkering of intrekking op de hoogte brengen, onder vermelding van de reden(en) die daarvoor aanleiding zijn geweest.

### **9.2.1 Blokkering op verzoek van KPN Telecom**

VeriSign zal het certificaat van KPN Telecom blokkeren op verzoek van een daartoe bevoegde vertegenwoordiger van KPN Telecom conform de volgende voorwaarden:

- KPN Telecom moet VeriSign uitdrukkelijk om de blokkering hebben verzocht;
- Het verzoek om blokkering moet zijn gedaan in de vorm van een elektronisch bericht, een faxbericht of een telefonisch bericht afkomstig van KPN Telecom of van diens vertegenwoordiger;
- De afzender van het verzoek (KPN Telecom of diens vertegenwoordiger) moet worden geauthenticeerd door middel van een toetsingszin danwel door een opsomming van bepaalde vooraf ingediende inschrijvingsinformatie.

Indien VeriSign het certificaat van KPN Telecom blokkeert conform bovenstaande procedure kan ze niet aansprakelijk worden gesteld voor de ongeoorloofde blokkering van dat certificaat, mits ze in goed vertrouwen handelt en zich baseert op voldoende geautoriseerde instructies.

### **9.2.2 Beëindiging van blokkering van een certificaat van KPN Telecom**

VeriSign zal de blokkering van het certificaat van KPN Telecom beëindigen (en aldus het certificaat herstellen) indien:

- (i) KPN Telecom hierom verzoekt en zijn identiteit jegens VeriSign afdoende bevestigt,
- (ii) VeriSign bepaalt dat het verzoek om blokkering is gedaan zonder autorisatie van KPN Telecom, of
- (iii) VeriSign bepaalt dat de redenen voor blokkering ongegrond waren.

## **9.3 Gevolgen van blokkering of intrekking**

### **9.3.1 Gevolgen voor certificaten**

Tijdens de blokkering, of op permanente basis na intrekking van een gebruikerscertificaat, moet de geldigheidsduur van het betreffende certificaat als onmiddellijk beëindigd worden beschouwd. In het geval van het aan KPN Telecom uitgegeven certificaat, betekent de beëindiging van de geldigheidsduur van het betreffende certificaat tevens dat de bevoegdheid van KPN Telecom om klasse 3 server certificaten uit te geven, wordt ingetrokken. Dit heeft echter geen invloed op de geldigheid van certificaten die door KPN Telecom zijn uitgegeven *tijdens* de geldigheidsduur van haar certificaat, dat wil zeggen voor de blokkering of intrekking.

### **9.3.2 Gevolgen voor onderliggende verplichtingen**

Blokkering of intrekking van een certificaat heeft geen invloed op de contractuele verplichtingen die de gebruiker van dat certificaat is aangegaan met KPN Telecom en VeriSign, tenzij als zodanig contractueel bepaald.

#### **9.4 Veiligstellen van de geheime sleutel bij blokkering of intrekking**

Geheime sleutels die corresponderen met publieke sleutels welke zijn opgenomen in een geblokkeerd of ingetrokken certificaat, moeten door de gebruiker van dat certificaat op een betrouwbare manier worden veiliggesteld gedurende de volledige periode van blokkering. Bij intrekking van het certificaat moet dit gebeuren gedurende de toepasselijke bewaartermijn, tenzij de geheime sleutel wordt vernietigd.

## **10. VERLOPEN VAN CERTIFICATEN**

---

**In dit gedeelte wordt ingegaan op de plichten die de partijen hebben ten aanzien van het verlopen van certificaten.**

---

### **10.1 Kennisgeving van vervaldatum**

KPN Telecom zal gebruikers via e-mail in kennis te stellen van een ophanden zijnde vervaldatum van hun certificaten. Een dergelijke kennisgeving is uitsluitend bedoeld om de gebruiker tijdig van dienst te zijn bij het verlengen van de certificaten met een naderende vervaldatum.

### **10.2 Gevolgen van het verlopen van certificaten voor onderliggende verplichtingen**

Het verlopen van de geldigheid van een certificaat heeft geen invloed op hieraan verbonden contractuele verplichtingen die zijn aangegaan uit hoofde van de gebruikersovereenkomst of de CPS.

### **10.3 Verlengen en opnieuw aanvragen van certificaten**

Certificaten dienen te worden verlengd via dezelfde procedure als de oorspronkelijke aanvraag, met als enige uitzondering dat de gebruiker van het te verlengen certificaat alleen die informatie hoeft in te dienen die gedurende de looptijd is vernieuwd of gewijzigd.

De eisen voor het verlengen en opnieuw aanvragen van certificaten kunnen eenzijdig worden gewijzigd door KPN Telecom. De meest recente eisen voor het verlengen en opnieuw aanvragen van certificaten (indien gewijzigd ten opzichte van deze CPS) kunnen worden opgevraagd in de repository van KPN Telecom (<https://www.kpn-telecom.nl/certificaat>).

## 11. VERPLICHTINGEN VAN KPN TELECOM EN VERISIGN

---

**Dit gedeelte beschrijft de waarborgen en beloften van KPN Telecom en VeriSign, de niet-aansprakelijkheidsclausules en de beperkingen van genoemde verplichtingen.**

---

### 11.1 Beperkte waarborgen en andere verplichtingen

KPN Telecom (en VeriSign, voor zover toepasselijk) garanderen tegenover de gebruikers van de certificatedienst dat hetgeen in deze CPS staat beschreven door haar als zodanig zal worden opgezet, aangeboden en uitgevoerd. Noch KPN Telecom noch VeriSign geeft enige andere waarborgen en hebben geen verdere verplichtingen uit hoofde van de CPS.

### 11.2 Niet-aansprakelijkheidsclausules en beperking van verplichtingen

Tenzij uitdrukkelijk bepaald in het voorgaande, wijzen KPN Telecom en VeriSign alle waarborgen en verplichtingen van welke aard dan ook af, met inbegrip van alle waarborgen met betrekking tot verhandelbaarheid, geschiktheid voor een bepaald doel en nauwkeurigheid van de verstrekte informatie, en wijzen zij bovendien iedere aansprakelijkheid af voor verzuim en gebrek aan voldoende zorgvuldigheid.

Tenzij uitdrukkelijk vermeld in deze CPS verklaren KPN Telecom en VeriSign:

- geen garanties te geven voor de nauwkeurigheid, authenticiteit, betrouwbaarheid, volledigheid, gangbaarheid, verhandelbaarheid of geschiktheid van enige informatie die aanwezig is in certificaten of anderszins is gecompileerd, gepubliceerd of verspreid door of namens KPN Telecom en VeriSign;
- geen aansprakelijkheid te aanvaarden voor verplichtingen die voortkomen uit informatie die aanwezig is in certificaten, op voorwaarde dat de inhoud van deze certificaten wezenlijk conform deze CPS is;
- geen garantie van onweerlegbaarheid (non-repudiation) te verstrekken voor enig certificaat of daarmee verbonden bericht, aangezien de eventuele weerlegbaarheid van berichten uitsluitend wordt bepaald door wet en door het toepasselijke mechanisme voor het beslechten van geschillen;
- geen garantie te geven voor welke software dan ook.

### 11.3 Uitsluiting van bepaalde schadevormen

In geen geval kunnen KPN Telecom of VeriSign aansprakelijk worden gesteld voor enige indirecte, speciale, incidentele of gevolgschade of voor schade als gevolg van enige vermindering van winst, verlies van gegevens of enige andere indirecte schade, gevolgschade of punitieve schade die het gevolg is van of betrekking heeft op:

- levering of het gebruik van het certificaat
- licentieverlening
- het al dan niet functioneren van certificaten of digitale handtekeningen

- enige andere transactie of dienst beschreven in deze CPS, zelfs indien KPN Telecom en/of VeriSign in kennis zijn gesteld van de mogelijkheid van dergelijke schadevormen.

## **11.4 Beperking aansprakelijkheid KPN Telecom en VeriSign**

### **11.4.1 Beperking aansprakelijkheid KPN Telecom tegenover gebruiker**

Met inachtneming van 11.3 is KPN jegens Gebruiker slechts aansprakelijk voor de schade die Gebruiker lijdt door een toerekenbare tekortkoming van KPN in de nakoming van haar verplichtingen op grond van deze overeenkomst, voorzover het betreft:

- Directe schade, waaronder wordt verstaan kosten van de vervanging van het Certificaat;
- Schade aan zaken van Gebruiker;
- Schade door dood of lichamelijk letsel.

De eventuele vergoedingsplicht van KPN is gebonden aan het hieronder genoemde maximum per Certificaat, welk maximum zowel geldt voor Gebruiker als voor derden die op het Certificaat vertrouwen (“relying parties”)

In geen geval zal de vergoedingsplicht van KPN op grond van deze bepaling een bedrag van maximaal 200.000 (tweehonderdduizend) gulden per certificaat te boven gaan. Indien ten gevolge van een schadeveroorzakend feit als hierboven bedoeld meer dan één vordering ontstaat en de gezamenlijke vorderingen het maximumbedrag van 200.000 (tweehonderdduizend) gulden te boven gaan, worden de vorderingen naar evenredigheid voldaan.

KPN kan zich niet beroepen op een uit dit artikel voortvloeiende uitsluiting of beperking van aansprakelijkheid, indien deze schade voortvloeit uit opzet of grove schuld aan de zijde van KPN.

Eventuele schade op grond van deze bepaling dient zo spoedig mogelijk en in ieder geval binnen tien (10) weken na intrekking van het bewuste certificaat op schriftelijke wijze aan KPN te worden gemeld

Gebruiker vrijwaart KPN tegen aanspraken op vergoeding van schade doordat Gebruiker zijn uit deze overeenkomst voortvloeiende verplichtingen niet nakomt.

### **11.4.2 Beperking aansprakelijkheid KPN Telecom tegenover gebruiker**

KPN is jegens de relying party slechts aansprakelijk voor de schade die de relying party lijdt door toerekenbare tekortkomingen van KPN in de nakoming van haar verplichtingen op grond van de CPS, voorzover het betreft:

- Directe schade, waaronder moet worden verstaan de prijs die is betaald voor de transactie, bij het sluiten waarvan op het certificaat is vertrouwd;
- Schade aan zaken van de relying party;
- Schade door dood of lichamelijk letsel.

De eventuele vergoedingsplicht van KPN is gebonden aan het hierna genoemde maximum per certificaat, welk maximum zowel geldt voor de relying party, andere relying parties als voor de houder van het certificaat.

In geen geval zal de vergoedingsplicht van KPN op grond van dit artikel een bedrag van maximaal 200.000 (tweehonderdduizend) gulden per certificaat te boven gaan. Indien ten gevolge van een schadeveroorzakend feit als hierboven bedoeld meer dan één vordering ontstaat en de gezamenlijke vorderingen het maximumbedrag van 200.000 (tweehonderdduizend) gulden te boven gaan, worden de vorderingen naar evenredigheid voldaan.

KPN kan zich niet beroepen op een uit dit artikel voortvloeiende uitsluiting of beperking van aansprakelijkheid, indien deze schade voortvloeit uit opzet of grove schuld aan de zijde van KPN.

Eventuele schade op grond van dit artikel dient zo spoedig mogelijk en in ieder geval binnen tien (10) weken na intrekking van het bewuste certificaat op schriftelijke wijze aan KPN te worden gemeld.

#### **11.4.3 Beperking aansprakelijkheid VeriSign**

In geen geval zal de totale aansprakelijkheid van VeriSign ten opzichte van alle partijen (waaronder begrepen maar niet beperkt tot gebruikers, aanvragers, ontvangers of relying parties) uitgaan boven de van toepassing zijnde aansprakelijkheidslimiet per klasse 3 server certificaat, zijnde een bedrag van 100.000 (honderdduizend) US dollars voor het totaal van alle digitale handtekeningen en/of transacties die betrekking hebben op dat certificaat.

Bovenstaande limitering van de aansprakelijkheid van VeriSign voor klasse 3 server certificaten heeft betrekking op verlies en schade van elke aard, waaronder begrepen maar niet beperkt tot (i) directe schade, (ii) indirecte schade, (iii) compenserende schade, (iv) speciale schade, (v) gevolgschade, (vi) karakteristieke schade, of (vii) incidentele schade geleden door enig persoon, waaronder begrepen maar niet beperkt tot gebruikers, aanvragers, ontvangers of relying parties, en welke schade is veroorzaakt als gevolg van vertrouwen op of gebruik van een certificaat uitgegeven, beheerd, gebruikt, geblokkeerd of ingetrokken door KPN Telecom. Deze aansprakelijkheidsbeperking is eveneens van toepassing op de aansprakelijkheid volgens contract, onrechtmatige daad en enige andere vordering.

De aansprakelijkheidslimiet is voor elk certificaat gelijk, ongeacht het aantal digitale handtekeningen, transacties of vorderingen met betrekking tot een dergelijk certificaat. Wanneer de genoemde limiet wordt overschreden, dient de aansprakelijkheid vooralsnog te worden toebedeeld aan de eerst binnengekomen vorderingen. De hieraan ten grondslag liggende geschillen moeten als eerste definitief worden beslecht, tenzij anderszins is bepaald door een terzake bevoegde rechtbank. In geen geval kan VeriSign worden verplicht meer te betalen dan het bedrag van de totale aansprakelijkheidslimiet voor elk certificaat, ongeacht de methode van toebedeling van dit bedrag onder de eisers.

### **11.5 Aansprakelijkheid van de gebruiker ten opzichte van relying parties**

Onverminderd de overige verplichtingen zoals vermeld in deze CPS, zijn gebruikers aansprakelijk voor iedere onjuiste voorstelling van zaken gedaan in certificaten tegenover derde partijen die, na verificatie van een of meer digitale handtekeningen met behulp van het certificaat, redelijkerwijs mochten vertrouwen op de hierin opgenomen verklaringen.

### **11.6 Geen fiduciaire rechtsverhouding**

KPN Telecom en VeriSign zijn geen tussenpersonen, vertrouwenspersonen, gevolmachtigden of anderszins vertegenwoordigers van de gebruikers van klasse 3 server certificaten of van partijen die daarop vertrouwen. De relatie tussen KPN Telecom (of VeriSign) en gebruikers van certificaten alsmede de relatie tussen KPN Telecom (of VeriSign) en relying parties is er niet een van tussenpersoon en opdrachtgever. Noch gebruikers, noch relying parties hebben enige autoriteit om KPN Telecom (of VeriSign) contractueel of anderszins te binden aan enige verplichting. KPN Telecom en VeriSign mogen en zullen geen verklaringen doen die het tegendeel suggereren, hetzij expliciet, impliciet, ogenschijnlijk of anderszins.

### **11.7 Risicovolle activiteiten**

De publieke certificatediensten van KPN Telecom en VeriSign zijn niet ontworpen of bedoeld voor, danwel bruikbaar als controlemiddel in risicovolle omstandigheden of in omstandigheden die een feilloze prestatie vereisen, zoals de bediening van een nucleaire installatie, de navigatie van luchtvaartuigen of communicatiesystemen, luchtverkeerscontrolesystemen of wapenbeheersingsystemen, waar een storing direct zou kunnen leiden tot dodelijke verwondingen of tot ernstige milieuschade.

## 12. DIVERSE BEPALINGEN

---

**In dit gedeelte worden de algemene voorwaarden van de server certificatiedienst van KPN Telecom en VeriSign behandeld die niet in de andere gedeeltes zijn besproken.**

---

### 12.1 Strijdige bepalingen

In het geval van strijdigheid tussen de gebruikersovereenkomst en de CPS en/of andere regels of richtlijnen is de gebruiker gebonden aan de bepalingen van de overeenkomst.

### 12.2 Toepasselijk recht

De afdwingbaarheid, samenstelling, uitleg en geldigheid van de gebruikersovereenkomst en deze CPS wordt beheerst door het Nederlandse recht.

### 12.3 Geschillenbeslechting

Alvorens toevlucht wordt gezocht tot een juridische procedure (waaronder begrepen procesvoering, kort geding of arbitrage) voor het beslechten van geschillen die betrekking hebben op (aspecten van) de gebruikersovereenkomst, de CPS, een door KPN Telecom uitgegeven certificaat danwel aanverwante zaken (met uitzondering van een geschil tussen KPN Telecom en VeriSign), dienen de betrokken partijen te trachten het geschil onderling te beslechten. Mochten ze daar niet in slagen, dan wordt het geschil voorgelegd aan de daartoe bevoegde rechter te 's-Gravenhage, tenzij de betrokken partijen zich akkoord verklaren met arbitrage ter beslechting van het geschil. Wanneer partijen daarvoor kiezen, wordt de procedure bepaald door de Nederlandse wetgeving op dat gebied.

### 12.4 Opvolgers en rechtverkrijgenden

Zowel de gebruikersovereenkomst als de CPS komen ten goede aan en zijn bindend voor de opvolgers, executeurs, erfgenamen, vertegenwoordigers, beheerders en rechtverkrijgenden, zij het expliciet, impliciet of schijnbaar, van de partijen. De rechten en verplichtingen in de gebruikersovereenkomst en de CPS kunnen door de partijen worden toegewezen op grond van een wettelijke bepaling (zoals ten gevolge van een fusie of overdracht van een meerderheidsbelang in aandelen met stemrecht) of anderszins, op voorwaarde dat een dergelijke toewijzing niet leidt tot een vernieuwing van andere schulden of verplichtingen van de toewijzende partij aan andere partijen op het tijdstip van de toewijzing. Worden door KPN Telecom danwel VeriSign rechten en/of verplichtingen overgedragen, dan dient dit te worden gedaan met inachtneming van paragraaf 3.16 door de overdragende en de ontvangende partij.

### 12.5 Wijziging voorwaarden

Geen van de voorwaarden of bepalingen van de gebruikersovereenkomst of de CPS die direct van invloed zijn op de rechten en verplichtingen van KPN Telecom of VeriSign mogen mondeling worden geamendeerd, opgegeven, aangevuld, gewijzigd of beëindigd, behalve door een

geauthenticeerd bericht of document van de betrokken partij danwel wanneer daar in de gebruikersovereenkomst of de CPS uitdrukkelijk in is voorzien.

## **12.6 Volledig document**

Indien enige bepaling van deze CPS of de toepassing ervan om welke reden en in welke mate dan ook ongeldig of niet-afdwingbaar wordt geacht, zal het resterende deel van deze CPS (en de toepassing van de ongeldige of niet-afdwingbare bepaling op andere personen of omstandigheden) zodanig worden uitgelegd dat de intentie van de partijen zo goed mogelijk in de praktijk wordt gebracht. Er wordt expliciet overeengekomen dat iedere bepaling van deze CPS met betrekking tot een beperking van de aansprakelijkheid, een niet-aansprakelijkheidsclausule of een beperkte aansprakelijkheid ten aanzien van garanties of andere verplichtingen, danwel een uitsluiting van de verplichting tot schadevergoedingen, apart kan worden beschouwd en onafhankelijk is van alle overige bepalingen en als zodanig afdwingbaar is.

## **12.7 Uitleg en vertalingen**

Tenzij anders bepaald, dient deze CPS te worden uitgelegd conform hetgeen commercieel aanvaardbaar wordt geacht onder de gegeven omstandigheden. Bij de uitleg van deze CPS moet rekening worden gehouden met de internationale draagwijdte en toepassing ervan, met de voordelen die zijn verbonden aan een uniforme toepassing en met het in acht nemen van de goede trouw.

## **12.8 Geen verklaring van afstand**

Verzuim van welk persoon dan ook om een bepaling van de gebruikersovereenkomst of de CPS af te dwingen, kan niet worden uitgelegd als een verklaring van afstand met betrekking tot de toekomstige afdwingbaarheid van de genoemde bepaling of van enige andere bepaling.

## **12.9 Kennisgeving**

Indien conform de gebruikersovereenkomst of de CPS een verplichting bestaat om mededelingen of verzoeken te doen, dan zal dit op een van de volgende manieren plaatsvinden:

- met behulp van digitaal ondertekende elektronische berichten
- langs schriftelijke weg.

Alle elektronische communicatie zal van kracht worden zodra de afzender een authentieke digitaal ondertekende bevestiging van ontvangst krijgt van de partij aan wie het bericht is verzonden, welke bevestiging dient te zijn ontvangen binnen vijf (5) werkdagen. Is het gebruik van elektronische berichtgeving niet mogelijk, dan dient een schriftelijke mededeling van ontvangst te worden gedaan.

Alle schriftelijke communicatie dient te worden afgeleverd door een koeriersdienst die de aflevering schriftelijk bevestigt, danwel via aangetekende post met bewijs van ontvangst, voorgefrankeerd en als volgt geadresseerd:

Aan KPN Telecom: KPN Telecom  
t.a.v. certificaat diensten  
Postbus 30150  
2500 GD 's-Gravenhage

Aan VeriSign: VeriSign, Inc.  
1350 Charleston Road  
Mountain View, CA 94043  
USA  
T.a.v. Certification Services

## **12.10 Koppen en bijlagen van deze CPS**

De koppen, subkoppen en overige bijschriften in deze CPS zijn uitsluitend bestemd als hulpmiddel en referentie en mogen niet worden gebruikt bij de uitleg, samenstelling of het afdwingen van de bepalingen van deze CPS.

## **12.11 Wijzigen van informatie**

Iedere gebruiker kan bepaalde informatie over zichzelf die aanwezig is in de bestanden van de UA en die niet in het certificaat is opgenomen, wijzigen binnen een termijn van dertig (30) dagen conform paragraaf 12.9 van deze CPS. Zulk een wijziging van informatie is van kracht na een periode van dertig (30) dagen.

## **12.12 Wijzigen van de CPS**

### **12.12.1 Algemene wijzigingen**

Indien noodzakelijk zal KPN Telecom in deze CPS wijzigingen aanbrengen, maar ze kan daaraan geen terugwerkende kracht ontnemen. KPN Telecom zal een gewijzigde versie van de CPS opnemen in de repository, met inachtneming van de in 12.12.2 genoemde bepalingen. Zulke wijzigingen komen vanaf de opname in de repository in de plaats van strijdige en specifiek aangewezen bepalingen in de desbetreffende versie van de CPS.

### **12.12.2 Materiële wijzigingen**

Inhoudelijke wijzigingen van de CPS worden van kracht vijftien (15) dagen nadat KPN Telecom de wijziging heeft gepubliceerd in de repository conform bovenstaande procedure, tenzij KPN Telecom vóór het einde van de periode van vijftien (15) dagen een aankondiging van intrekking van de wijziging in de repository plaatst.

### **12.12.3 Wijziging ter voorkoming van inbreuk**

Indien KPN Telecom een inhoudelijke wijziging publiceert die noodzakelijk is om compromittering van (een gedeelte van) de certificatediensten te voorkomen, dan geldt het moment van publicatie als tijdstip waarop de wijziging van de CPS van kracht wordt.

#### **12.12.4 Niet inhoudelijke wijzigingen**

Een wijziging op de CPS die niet inhoudelijk van aard is (bijvoorbeeld het herstellen van een typefout) wordt onmiddellijk van kracht na publicatie in de repository conform bovenstaande procedure. Of een wijziging aangeduid kan worden als inhoudelijk of niet-inhoudelijk is ter beoordeling aan KPN Telecom.

#### **12.12.5 Intrekking certificaat vanwege wijziging CPS**

Indien de gebruiker niet binnen vijftien (15) dagen na publicatie van een inhoudelijke wijziging van de CPS tot intrekking van zijn certificaat overgaat, wordt hij geacht met deze wijziging in te stemmen. Voor meer informatie hieromtrent zie de repository van KPN Telecom.

#### **12.13 Intellectueel eigendom**

Tenzij anderszins overeengekomen tussen partijen worden de volgende bestanden en gegevens met betrekking tot de onder deze CPS vallende certificatiendiensten beschouwd als eigendom van de hieronder aangegeven partijen:

- Certificaten zijn eigendom van KPN Telecom;
- De Certification Practice Statement (CPS) is eigendom van KPN Telecom en VeriSign, Inc;
- Distinguished names zijn eigendom van de daarmee verbonden personen (eventueel hun werkgever of opdrachtgever) of bedrijven;
- Geheime sleutels zijn eigendom van de gebruiker(s) van het certificaat;
- Publieke sleutels van de VeriSign Root, met inbegrip van alle publieke sleutels van KPN Telecom, zijn eigendom van VeriSign, Inc. VeriSign verleent aan de relying parties een licentie voor het gebruik van voornoemde sleutels uitsluitend in combinatie met betrouwbare hardware of software waarin de publieke sleutel van de root is gedistribueerd op gezag van VeriSign;
- Geheime delen van de sleutel van VeriSign zijn eigendom van VeriSign.

Certificaten die zijn uitgegeven door KPN Telecom (als UA in de certificatieketen van VeriSign) bevatten een mededeling met betrekking tot het auteursrecht (“Auteursrecht (c)1997 VeriSign, Inc., alle rechten voorbehouden” of “(c)97” in samenhang met VeriSign). Bij deze wordt door VeriSign toestemming verleend voor de reproductie en distributie van certificaten op een niet-exclusieve en royalty-vrije basis, op voorwaarde dat deze reproductie en/of distributie volledig is. Tevens geldt als restrictie dat certificaten niet zonder uitdrukkelijke schriftelijke toestemming van VeriSign mogen worden gepubliceerd in een publiek toegankelijke repository of directory, hetgeen met name bedoeld is om de privacy van gebruikers te beschermen tegen hernieuwde publicatie van hun certificaat zonder voorafgaande toestemming. Vragen met betrekking tot de auteursrechtelijke mededeling kunnen worden gezonden naar VeriSign op het adres dat is vermeld in artikel 12.9 van de CPS of naar het volgende e-mailadres: [practices@VeriSign.com](mailto:practices@VeriSign.com).

#### **12.14 Inbreuk en ander schadelijk materiaal**

Iedere gebruiker van een certificaat garandeert dat de indiening van de aanvraag bij KPN Telecom, de daarbij verschaft informatie en het gebruik van een bepaald domein of distinguished name geen belemmering vormen voor of inbreuk maken op:

- rechten van derde partijen onder welke jurisdictie dan ook;
- woord- of beeldmerken;
- handelsnamen, of
- enig ander intellectueel eigendomsrecht.

Verder garandeert iedere gebruiker van een certificaat dat hij niet de intentie heeft het domein en de distinguished name te gebruiken voor onwettige doeleinden, waaronder begrepen maar niet beperkt tot het volgende:

- onrechtmatig nastreven van toekomstige zakelijke voordelen;
- oneerlijke concurrentie;
- beschadiging van de reputatie van een ander;
- verwarring of misleiding van personen, hetzij natuurlijke personen, hetzij rechtspersonen, of
- plegen van enig strafbaar feit.

Iedere gebruiker van een certificaat zal KPN Telecom en Verisign vrijwaren en schadeloos stellen voor elk verlies en/of schade resulterend uit het hiervoor genoemde onrechtmatig handelen.

#### **12.14.1 Eigen verantwoordelijkheid verstrekte informatie**

Voor informatie die de gebruiker ter certificatie aanbiedt aan KPN Telecom en die niet in de validatieprocedure wordt nagegaan, zijn KPN Telecom en VeriSign niet verantwoordelijk. Verder zijn gebruikers van certificaten zelf verantwoordelijk voor de rechtsgeldigheid van de informatie die ze verstrekken voor gebruik in die certificaten conform de CPS in iedere jurisdictie waarin deze inhoud kan worden gebruikt of bekeken. Omdat de wetten met betrekking tot de transmissie en beschikbaarheid van informatie voortdurend veranderen en zeer verschillend zijn, worden de verantwoordelijkheden van gebruikers van certificaten niet uitsluitend bepaald door de bestaande wetten op het tijdstip van uitgifte door KPN Telecom van een certificaat aan een certificaataanvrager, maar ook door wetten die pas na dat tijdstip van kracht worden gedurende de looptijd van het certificaat. Gebruikers van certificaten dienen zich ervan bewust te zijn dat er een groot aantal wetten bestaat met betrekking tot de transmissie van gegevens, met name gegevens die versleuteld zijn of waarbij encryptiealgoritmen een rol spelen. Bovendien kunnen deze wetten van staat tot staat en van land tot land sterk verschillen. Daarnaast is het in het algemeen niet mogelijk om de distributie van content via het Internet of bepaalde andere netwerken te beperken op basis van de plaats waar de gebruiker zich bevindt, zodat gebruikers van certificaten kunnen worden gedwongen de wetten na te leven van iedere jurisdictie waarin de inhoud kan worden bekeken of gebruikt.

#### **12.14.2 Geen onwettige of onrechtmatige informatie**

Gebruikers van certificaten zullen aan KPN Telecom, VeriSign of de repository van KPN Telecom geen materiaal voorleggen dat:

- (i) lasterlijk, smadelijk, obscene, pornografisch, beledigend, onverdraagzaam, haatdragend of discriminerend ten aanzien van ras is;
- (ii) aanzet tot illegale activiteiten of waarin illegale activiteiten worden besproken met de bedoeling deze te bedrijven;

(iii) anderszins in strijd is met de wet.

### **12.15 Tarieven**

KPN Telecom kan gebruikers kosten in rekening brengen voor het gebruik van haar diensten. Een actueel overzicht van de tarieven kan worden opgevraagd bij de repository (<https://www.kpn-telecom.nl/certificaat>). Voor wat betreft klasse 3 server certificaten gaat het dan om de betaling van een eenmalig bedrag aan het begin van de looptijd van het certificaat.

### **12.16 Keuze van cryptografische methoden**

Ieder persoon erkent dat hij zelf - en niet KPN Telecom of VeriSign - alleen verantwoordelijk is voor een onafhankelijk oordeel met betrekking tot de keuze van beveiligingssoftware en - hardware alsmede voor de algoritmen voor encryptie en digitale handtekeningen, waaronder begrepen de hierbij behorende parameters, procedures en technieken.

### **12.17 Blijvende geldigheid**

De verplichtingen en beperkingen in deze CPS met betrekking tot audits, vertrouwelijke informatie, verplichtingen van KPN Telecom en VeriSign alsmede de diverse bepalingen uit dit hoofdstuk zullen ook na een eventuele beëindiging van deze CPS van kracht blijven.

### **12.18 Overmacht**

KPN Telecom en VeriSign zijn niet verantwoordelijk voor vertragingen, niet-nakomingen op garanties of niet-geleverde prestaties uit hoofde van de gebruikersovereenkomst of de CPS indien dit het gevolg is van gebeurtenissen buiten de invloedssfeer van KPN Telecom of VeriSign, zoals een natuurramp, oorlogshandeling, epidemie, stroomstoring, brand, aardbeving of andere ramp.

\*\*\*

### 13. ACRONIEMEN EN AFKORTINGEN

CA	Certificatie-Autoriteit
CPS	Certification Practice Statement
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol met SSL
UA	Uitgevende Autoriteit
LRA	Lokale Registratie-Autoriteit
PCA	Primaire Certificatie-Autoriteit
PCD	Publieke CertificatieDiensten
PIN	Persoonlijk IdentificatieNummer
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest, Shamir & Adelman
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
WWW	World Wide Web

## 14. DEFINITIES

### A-B

#### **AANVRAGER VAN EEN CERTIFICAAT**

Een persoon of geautoriseerde instantie die verzoekt om de uitgifte van een publieke-sleutelcertificaat door een UA.

#### **ACCEPTEREN (VAN EEN CERTIFICAAT)**

Het instemmen met een certificaat door de aanvrager ervan, waarbij de aanvrager bekend is met of kennis heeft genomen van de inhoud van het certificaat conform de CPS.

#### **ACCREDITATIE**

Een formele verklaring van een onafhankelijke instantie dat een informatiesysteem of een medewerker, aannemer of organisatie gemachtigd is om bepaalde taken te vervullen en om te werken conform specifieke voorgeschreven veiligheidsrichtlijnen.

#### **ALIAS**

Een pseudoniem.

#### **ARCHIVEREN**

Het voor een bepaalde tijdsduur opslaan van records en bijbehorende informatie uit oogpunt van beveiliging, het maken van back-ups of het verrichten van controle.

#### **AUDIT**

Een procedure die wordt gebruikt om na te gaan of er controleprocedures worden toegepast en of deze geschikt zijn voor het betreffende doel. Hieronder wordt tevens verstaan het registreren en analyseren van activiteiten om indringing in en misbruik van informatiesystemen vast te stellen. Onvolkomenheden die tijdens een audit worden vastgesteld, worden gerapporteerd aan de daarvoor verantwoordelijken.

#### **AUTHENTICATIE**

Een proces dat wordt toegepast om iemands identiteit te bevestigen of om de integriteit van bepaalde informatie vast te stellen. Bij authenticatie van berichten dient de bron van een bericht te worden bepaald en te worden vastgesteld dat het bericht niet is aangepast of tijdens de verzending is vervangen.

#### **AUTORISATIE**

Het toekennen van rechten, waaronder begrepen de toegang tot bepaalde specifieke informatie of bronnen.

**BEHEER VAN EEN CERTIFICAAT**

Het beheer van een certificaat behelst (maar beperkt zich niet tot) het opslaan, verspreiden, publiceren, intrekken en blokkeren van certificaten. Een UA vervult de taken die behoren bij het beheer van certificaten in de hoedanigheid van registratie-autoriteit van gebruikerscertificaten. Een UA maakt uitgegeven en geaccepteerde certificaten geldig door publicatie.

**BEHEERDER VAN EEN LOKALE REGISTRATIE-AUTORITEIT (BLRA)**

De werknemer van een LRA die verantwoordelijk is voor het uitvoeren van de werkzaamheden van een LRA.

**BERICHT**

Informatie die op digitale wijze is weergegeven. Onderliggend begrip van bestand (zie definitie).

**BESCHIKBAARHEID**

De mate waarin informatie of processen redelijkerwijs op verzoek toegankelijk en bruikbaar zijn voor een geautoriseerde partij, waardoor de geautoriseerde toegang tot bronnen mogelijk is en aan tijd gebonden activiteiten tijdig kunnen worden uitgevoerd.

**BESTAND**

Informatie die is vastgelegd op een tastbaar medium (een document) of opgeslagen in elektronische of andere vorm en die zichtbaar kan worden gemaakt.

**BETROUWBAAR SYSTEEM**

Hardware, software en procedures die behoorlijk beveiligd zijn tegen indringing en misbruik, behoorlijk beschikbaar zijn en correct werken, redelijkerwijs geschikt zijn om de taken te vervullen waarvoor ze gemaakt zijn en voldoen aan het van toepassing zijnde beveiligingsbeleid.

**BEVEILIGING**

Het beschermd worden of zijn tegen niet-geautoriseerde toegang of ongecontroleerde verliezen of gevolgen. Volledige beveiliging blijkt in de praktijk onmogelijk om te realiseren; de kwaliteit van ieder beveiligingssysteem is relatief. Binnen het kader van een statusgeoriënteerd beveiligingssysteem is beveiliging een specifieke "status", die tijdens verschillende omstandigheden bewaard dient te blijven.

**HANDBOEK BEVEILIGINGSBELEID**

Document met daarin de eisen en gewenste procedures met betrekking tot de beschermingsmaatregelen die moeten worden getroffen door een betrouwbaar systeem in het kader van de publieke certificatediensten.

**BEVEILIGINGSDIENSTEN**

Diensten die worden gerealiseerd middels beveiligingsvoorzieningen waaronder toegangscontrole, vertrouwelijkheid van gegevens en integriteit van gegevens.

**BEVESTIGEN / BEVESTIGING**

Vermelden of door gedrag te kennen geven dat gegevens correct zijn of dat informatie juist is.

**BLOKKEREN VAN EEN CERTIFICAAT**

Het opschorten van de werking van een geldig certificaat.

**BOVENGESCHIKTE UA**

In de hiërarchie van UA's binnen de PKI van VeriSign is iedere UA ofwel de VR, een PCA, een CA of een "ondergeschikte CA". De bovengeschikte UA van een ondergeschikte CA is ofwel een andere ondergeschikte CA of een CA; de bovengeschikte van een CA is een PCA; de bovengeschikte van een PCA's is ofwel de Root of de PCA zelf. De Root is haar eigen bovengeschikte UA.

**BRON VAN HERKOMST**

De persoon door wie (of namens wie) een gegevensbericht kennelijk is gemaakt, opgeslagen of verzonden. Niet de persoon die als intermediair is opgetreden.

# C

**CERTIFICAAT (PUBLIEKE-SLEUTELCERTIFICAAT)**

Een bericht (zie definitie) waarin ten minste de naam of de identiteit van de UA wordt vermeld, alsmede de gebruiker, de publieke sleutel van de gebruiker, de geldigheidsduur van het certificaat en het serienummer van het certificaat. Het bericht dient digitaal door de UA te zijn ondertekend.

**CERTIFICAATAANVRAAG**

Een verzoek van de aanvrager van een certificaat (of een geautoriseerde instantie), gericht aan een UA, tot uitgifte van een certificaat.

**CERTIFICAAT-EXTENSIE**

Een veld op een certificaat waarin aanvullende informatie kan zijn opgenomen over de publieke sleutel die wordt gecertificeerd, de gecertificeerde gebruiker, de uitgever van het certificaat en/of het certificatieproces. Standaardextensies zijn gedefinieerd in Amendement 1 van ISO/IEC 9594-8:1995 (X.509).

**CERTIFICAAT-HIËRARCHIE**

Afhankelijk van hun rol hebben alle UA's hun plaats in de "boomstructuur" van ondergeschikte UA's. Een UA geeft certificaten uit en beheert deze voor gebruikers en/of voor één of meerdere UA's op een lager niveau. Let op: een UA in een vertrouwelijke hiërarchie dient zich te houden aan uniforme richtlijnen met betrekking tot namen, het maximale aantal niveaus, etc., teneinde de integriteit van het domein te waarborgen en door het gebruik van betrouwbare operationele processen te zorgen voor controleerbaarheid en beheersbaarheid.

**CERTIFICATE REVOCATION LIST (CRL)**

Een periodiek (of, indien noodzakelijk, vaker) uitgegeven overzicht, digitaal ondertekend door een UA, van certificaten die vóór de vervaldatum zijn geblokkeerd of ingetrokken. Doorgaans vermeldt een CRL de naam van de autoriteit die de CRL heeft uitgegeven, de datum van uitgifte, de geplande datum van de volgende CRL, de serienummers van de geblokkeerde of ingetrokken certificaten en de data en redenen van blokkering of intrekking.

**CERTIFICATIE / CERTIFICEREN**

Het uitgeven van een certificaat door een UA.

**CERTIFICATIE-AUTORITEIT (CA)**

Een persoon of instantie die bevoegd is om certificaten uit te geven. Binnen de publieke certificatediensten van VeriSign is een CA ondergeschikt aan een PCA.

**CERTIFICATIEKETEN**

Een geordende lijst van certificaten met een gebruikerscertificaat en UA-certificaten.

**CERTIFICATION PRACTICE STATEMENT (CPS)**

Een beschrijving van de processen en procedures die worden gevolgd bij het uitgeven, beheren, blokkeren en intrekken van certificaten om de daarmee verbonden dienstverlening transparant te maken voor gebruikers en relying parties.

**CONNECTIE**

Een bevestiging door een UA (of diens LRA) van de verhouding tussen een met name genoemde entiteit en diens publieke sleutel.

**CONTROLES**

Maatregelen die worden genomen om de integriteit en kwaliteit van een proces te waarborgen.

**CORRESPONDEREN**

Tot hetzelfde sleutelpaar behoren.

**CROSS CERTIFICATION**

De omstandigheid dat een PCA en/of een CA van een bepaald certificatedomein een certificaat uitdeeft aan een PCA en/of CA van een ander certificatedomein en vice versa, om aldus elkaars certificaten te erkennen.

**CRYPTOGRAFIE**

- (i) Een wiskundig proces dat wordt toegepast om de vertrouwelijkheid en authenticatie van gegevens te waarborgen door deze gegevens te vervangen door een versleutelde versie, die alleen kan worden ontcijferd door iemand die in het bezit is van het juiste cryptografische algoritme en de sleutel.
- (ii) Een discipline die de principes, middelen en methoden beschrijft voor het omzetten van gegevens teneinde de inhoud van deze gegevens te verbergen, te voorkomen dat de gegevens

onopgemerkt worden gewijzigd en/of te voorkomen dat de gegevens op ongeoorloofde wijze worden gebruikt.

#### **CRYPTOGRAFIE MET PUBLIEKE SLEUTELS**

Een vorm van cryptografie waarbij gebruik wordt gemaakt van een sleutelpaar bestaande uit wiskundig gerelateerde cryptografische sleutels. De publieke sleutel kan worden verstrekt aan iedereen die er gebruik van wenst te maken en wordt gebruikt om informatie te versleutelen of om een digitale handtekening te verifiëren. De geheime sleutel wordt geheim gehouden door de houder en wordt gebruikt om informatie te ontcijferen of om een digitale handtekening te genereren.

#### **CRYPTOGRAFISCH ALGORITME**

Een duidelijk gespecificeerd wiskundig proces voor berekeningen, een verzameling regels die een voorgeschreven resultaat produceren.

#### **CRYPTOMODULE**

Een betrouwbare implementatie van een cryptosysteem waarmee op een veilige wijze gegevens kunnen worden versleuteld (encryptie) en ontcijferd (decryptie).

## **D**

#### **DATABASE/DATABANK**

Een systematische verzameling gegevens die middels een geautomatiseerd management-informatiesysteem wordt gemaakt, opgeslagen en bewerkt.

#### **DATUMSTEMPEL**

Vermelding van (ten minste) de juiste datum en tijd van een activiteit, alsmede de identiteit van de persoon die verantwoordelijk is voor de verzending of ontvangst van de datumstempel.

#### **DIENSTEN WAARBIJ DE INTEGRITEIT VAN DE INHOUD WORDT GECONTROLEERD**

Diensten die certificaten verlenen aan uitgevers van software die hun publicaties van een digitale handtekening willen voorzien, teneinde hun klanten (gebruikers) in staat te stellen de software te valideren.

#### **DIGITALE HANDTEKENING**

Transformatie van een bericht met behulp van een asymmetrisch cryptosysteem, op zodanige wijze dat een persoon die in het bezit is van het oorspronkelijke bericht en de publieke sleutel van de ondertekenaar nauwkeurig kan bepalen of de transformatie heeft plaatsgevonden met behulp van de geheime sleutel die correspondeert met de publieke sleutel van de ondertekenaar en of het bericht na transformatie nog veranderingen heeft ondergaan.

#### **DISTINGUISHED NAME**

Een verzameling gegevens die een bestaande entiteit identificeert, zoals een persoon in het kader

van computertoepassingen. (bijv. landnaam=NL, organisatie naam=KPN, eigen naam=Kees Janssen).

#### **DOCUMENT**

Informatie, vastgelegd op een tastbaar medium, zoals papier. In dit verband dus geen informatie die is vastgelegd in een computer.

## **E-F**

#### **ELEKTRONISCHE POST ('E-MAIL')**

Berichten die in digitale vorm worden verzonden, ontvangen of doorgezonden middels een geautomatiseerd communicatiesysteem.

#### **ENCRYPTIE (VERSLEUTELING)**

Proces waarbij informatie in een onbegrijpelijke vorm wordt vervormd (cijfertekst), op zodanige wijze dat de oorspronkelijke gegevens ofwel niet kunnen worden hersteld (simplex encryptie), ofwel alleen kunnen worden hersteld door middel van een omgekeerd ontcijferingsproces (duplex encryptie).

#### **EXTENSIES**

Velden voor extra informatie in X.509 v3-certificaten.

#### **FILE TRANSFER PROTOCOL (FTP)**

Protocol voor bestandsoverdracht via het Internet.

## **G-H**

#### **GARANTIES**

Verklaringen die bedoeld zijn om een algemene, oprechte intentie over te brengen met betrekking tot het vermogen van een UA om een specifieke dienst te kunnen leveren en te kunnen onderhouden.

#### **GEAUTHENTICEERD BESTAND**

Een ondertekend document, voorzien van de juiste bevestigingen van authenticatie of een bericht met een digitale handtekening, geverifieerd middels een geldig Klasse 3-certificaat door een relying party. Bij een kennisgeving van blokkering of intrekking dient de digitale handtekening te zijn vervaardigd met behulp van de geheime sleutel die correspondeert met de publieke sleutel in het certificaat voor de desbetreffende certificaatklasse.

#### **GEBRUIKER**

De houder van een certificaat die bevoegd en in staat is tot het gebruik van de geheime sleutel die correspondeert met de publieke sleutel zoals genoemd in het certificaat.

**GEBRUIKERSOVEREENKOMST**

Overeenkomst die wordt gesloten door een gebruiker en een UA voor de levering van bepaalde publieke certificatediensten conform deze CPS.

**GEHEIM DEEL**

Deel van een cryptografisch geheim dat is verdeeld over een aantal fysieke hardwaretokens.

**GEHEIME SLEUTEL**

Een wiskundige sleutel (die door de eigenaar geheim wordt gehouden) die wordt gebruikt om digitale handtekeningen te vervaardigen, en - afhankelijk van het algoritme - kan worden gebruikt voor de ontcijfering van berichten of bestanden die zijn versleuteld (uit veiligheidsoverwegingen) met de desbetreffende publieke sleutel.

**GELDIG CERTIFICAAT**

Een door een UA uitgegeven certificaat, geaccepteerd door de gebruiker, dat op de huidige dag en tijd danwel, afhankelijk van de context, op een andere, aangegeven dag en tijd, valt binnen de geldigheidsduur.

**GELDIGHEIDSDUUR**

De periode die aanvangt op de datum en tijd waarop het certificaat wordt uitgegeven (of op een latere datum en tijd indien vermeld op het certificaat) en eindigt op de datum en tijd waarop de geldigheid van het certificaat vervalst, danwel op een eerdere datum, indien de geldigheid van het certificaat wordt geblokkeerd of ingetrokken.

**GEMEENSCHAPPELIJKE SLEUTEL**

Bij bepaalde cryptografische apparatuur wordt beveiliging toegepast door middel van een proces van gedeelde geheimhouding. Daarbij dient het laatste deel fysiek aan de hardware bevestigd te blijven om deze te beveiligen. Het laatste deel is dan de “gemeenschappelijke sleutel”. Het wordt niet als geheim gezien, omdat het niet voortdurend in bezit is van één enkele persoon.

**GENEREREN VAN EEN SLEUTEL**

Betrouwbaar proces voor het maken van een sleutelpaar van een geheime sleutel en een publieke sleutel. De publieke sleutel wordt verstrekt aan een UA wanneer het certificaat wordt aangevraagd.

**GENEREREN VAN EEN SLEUTELPAAR**

Een betrouwbaar proces voor het maken van een geheime sleutel tijdens de certificaataanvraag. De publieke sleutel die correspondeert met deze geheime sleutel wordt tijdens de certificaataanvraag verstrekt aan de relevante UA. Hierbij dient te worden aangetoond dat de aanvrager in staat is de geheime sleutel te gebruiken.

**HANDTEKENING**

Een methode die wordt gebruikt door de maker van een document om zichzelf te identificeren.

De methode kan worden geaccepteerd door de ontvangende partij of gebruikelijk zijn onder de omstandigheden.

#### **HASH (HASH-FUNCTIE)**

Een algoritme dat een reeks bits omzet of vertaalt in een andere (doorgaans kleinere) reeks, op zodanige wijze dat:

1. een bericht steeds hetzelfde resultaat oplevert als het algoritme wordt uitgevoerd met het desbetreffende bericht als input;
2. Het rekenkundig onmogelijk is om een bericht te herleiden of samen te stellen op basis van de uitkomst van het algoritme.
3. Het rekenkundig onmogelijk is om twee verschillende berichten te vinden die dezelfde hash-uitvoer hebben indien hetzelfde algoritme wordt toegepast.

#### **HIËRARCHIE VAN EEN PUBLIC KEY INFRASTRUCTURE (PKI)**

Een reeks UA's wiens functies geregeld zijn volgens het principe van overdracht van bevoegdheid; de UA's verhouden zich tot elkaar als ondergeschikte en bovengeschikte UA.

#### **HOUDER (VAN EEN CERTIFICAAT)**

De eigenaar van een geheime sleutel die correspondeert met een publieke sleutel. Het begrip "houder" kan betrekking hebben op zowel het systeem of apparaat dat is voorzien van de geheime sleutel als op de individuele persoon (indien van toepassing) die het systeem of apparaat bedient. Een houder krijgt een eenduidige naam toegewezen, die is gekoppeld aan de publieke sleutel vermeld op het certificaat van de desbetreffende houder.

#### **HOUDER VAN EEN GEHEIM DEEL**

Geautoriseerde houder van een hardwaretoken met een geheim deel.

## **I**

#### **IDENTIFICATIE / IDENTICEREN**

Het vaststellen van de identiteit van een persoon. Bij cryptografie met publieke sleutels vindt identificatie plaats door middel van certificaten.

#### **IDENTITEIT**

Een uniek stukje informatie, dat een bepaalde entiteit binnen een domein markeert of aanduidt. Deze informatie is alleen uniek binnen een bepaald domein.

#### **INBREUK**

Een (vermeende) schending van het veiligheidsbeleid, waardoor ongeoorloofde openbaarmaking van of verlies van controle over vertrouwelijke informatie kan hebben plaatsgevonden. (

#### **INTEGRITEIT VAN GEGEVENS**

Toestand waarin gegevens niet zijn gewijzigd of op een ongeoorloofde wijze zijn vernietigd.

#### **INTREKKEN VAN EEN CERTIFICAAT**

Het proces waarbij de geldigheid van een certificaat vanaf een bepaald moment permanent wordt beëindigd.

## **J-L**

#### **KENNISGEVEN**

Mededeling doen van specifieke informatie aan een andere persoon, op de wijze die wordt vereist door deze CPS en door het toepasselijke recht.

#### **KENNISGEVING**

Het resultaat van een kennisgeving in overeenstemming met deze CPS.

#### **KLASSE 3-CERTIFICAAT**

Een certificaat met een bepaald vertrouwelijkheidsniveau (klasse 3).

#### **LOKALE REGISTRATIE-AUTORITEIT (LRA)**

Een entiteit die door een UA is gemachtigd om personen te assisteren bij de aanvraag van certificaten, is gemachtigd tot het intrekken van certificaten, en - indien daartoe geautoriseerd - het blokkeren van certificaten, of beide, alsmede het goedkeuren van voornoemde aanvragen. Een LRA is geen bemiddelaar voor de aanvrager van een certificaat. Een LRA is alleen gerechtigd om de bevoegdheid tot het goedkeuren van certificaatapplicaties over te dragen aan geautoriseerde beheerders van de LRA.

## **M-N**

#### **NAAM**

Een reeks identificerende kenmerken die een bepaalde entiteit beschrijven.

#### **NAAMGEVENDE AUTORITEIT**

Een lichaam dat namen toekent, hiertoe procedures volgt, en het beheer voert over de registratie en toekenning van distinguished names aan bepaalde voorwerpen.

#### **NAAMGEVENDE AUTORITEIT VAN VERISIGN**

Registratie-autoriteit van VeriSign die richtlijnen en controleprocedures opstelt en zeggenschap heeft met betrekking tot de uitgifte van relative distinguished names voor alle UA's (echter niet voor gebruikers).

#### **NAAMGEVING**

Het toekennen van beschrijvende, identificerende kenmerken aan bepaalde voorwerpen door een

autoriteit die hiertoe specifieke procedures volgt en specifieke administratieve systemen bijhoudt met betrekking tot dit registratieproces.

#### **NIET-GEVERIFIEERDE INFORMATIE VAN GEBRUIKERS**

Informatie die door de aanvrager van een certificaat is verstrekt aan een UA en is opgenomen in een certificaat, die niet door de UA is geconfirmeerd en waarvoor de UA geen assurances afgeeft, behalve dat de informatie is verstrekt door de aanvrager van het certificaat. Tenzij anders aangegeven, worden titels, professionele graden, accreditaties en Registration Field Information beschouwd als niet geverifieerde informatie van gebruikers.

## **O-P**

#### **ONDERGESCHIKTE UA**

In de hiërarchie van UA's binnen de PKI van VeriSign is iedere UA ofwel de VR, een PCA, een CA of een "ondergeschikte CA". De ondergeschikte UA van de Root is een PCA; de ondergeschikte UA van een PCA is een CA; de ondergeschikte UA van een CA is een ondergeschikte CA. Indien van toepassing: de ondergeschikte UA van een ondergeschikte CA is weer een andere ondergeschikte CA.

#### **ONDERTEKENAAR**

Een persoon die een digitale handtekening aanmaakt voor een bericht of een handtekening onder een document plaatst.

#### **ONDERTEKENEN**

Het zetten van een digitale handtekening onder een bericht, danwel het plaatsen van een handtekening op een document.

#### **ONDERWERPAANDUIDING**

De eenduidige waarde in het veld voor onderwerpaanduidingen van een certificaat dat is gekoppeld aan de publieke sleutel.

#### **ON-LINE**

Communicatie waarmee een directe verbinding met de publieke certificatiediensten van VeriSign tot stand wordt gebracht.

#### **ONTVANGER (van een digitale handtekening)**

Persoon die een digitale handtekening ontvangt en in een positie is om deze te vertrouwen (onafhankelijk van het feit of dit al dan niet gebeurt).

#### **ONWEERLEGBAARHEID**

Leverd bewijs met betrekking tot de verzending of ontvangst van gegevens teneinde de verzender te beschermen indien de geadresseerde valselijk ontkent dat hij de gegevens heeft ontvangen of

om de geadresseerde te beschermen indien de verzender valselijk ontkent dat hij de gegevens heeft verzonden.

#### **ORGANISATIE**

Een instantie waaraan een gebruiker is gelieerd. Een organisatie kan ook een gebruiker zijn.

#### **PARTIJEN**

Entiteiten waarvan de rechten en verplichtingen door deze CPS worden geregeld. Dit kunnen ook aanvragers van certificaten, UA's, gebruikers en relying parties zijn.

#### **PC-KAART**

Een hardware-token conform de normen van de Personal Computer Memory Card International Association (PCMCIA) waarmee de functionaliteit van computers kan worden uitgebreid, zoals de mogelijkheid tot gegevensbeveiliging.

#### **PERSOON**

Een mens of een organisatie (of een inrichting onder controle van een mens of een organisatie) die in staat is een bericht te ondertekenen of te verifiëren, hetzij rechtsgeldig, hetzij feitelijk (een synoniem van entiteit)

#### **PERSOONLIJK VERSCHIJNEN**

Het aanwezig zijn (fysiek, niet virtueel of middels een beeldverbinding) bij een LRA of een andere, aangewezen instantie, teneinde bewijs te leveren van iemands identiteit, is in bepaalde omstandigheden een vereiste voor het uitgeven van een certificaat.

#### **PRIMAIRE CERTIFICATIE-AUTORITEIT (PCA)**

Persoon die praktijkrichtlijnen opstelt voor alle certificatie-autoriteiten en users die binnen haar domein vallen.

#### **PUBLIC KEY INFRASTRUCTURE (PKI)**

De architectuur, organisatie, technieken, praktijken en procedures die als geheel de implementatie en werking ondersteunen van een op cryptografisch systeem met publieke sleutels voor de uitgifte van certificaten. De PKI bestaat uit systemen die samenwerken voor een goede werking van de publieke certificatediensten en eventueel daaraan gerelateerde diensten.

#### **PUBLICEREN / PUBLICATIE**

Het opslaan van informatie in de repository van VeriSign en indien gewenst in een of meerdere andere repository's teneinde deze informatie openbaar te maken op een wijze die overeenkomt met deze CPS en het toepasselijke recht.

#### **PUBLIEKE CERTIFICATIEDIENSTEN**

Het certificatiesysteem van VeriSign en iedere door VeriSign geautoriseerde UA die in deze CPS wordt beschreven.

**PUBLIEKE SLEUTEL**

Wiskundige sleutel die algemeen beschikbaar kan worden gemaakt. De sleutel wordt gebruikt voor het verifiëren van handtekeningen die zijn gemaakt met de corresponderende geheime sleutel. Publieke sleutels kunnen – afhankelijk van het algoritme – worden gebruikt om berichten of bestanden te versleutelen; deze kunnen vervolgens worden ontcijferd met de corresponderende geheime sleutel.

# R

**REGISTRATIE-AUTORITEIT (RA)**

Een entiteit die bevoegd is om andere entiteiten te registreren en relatieve waarden toe te kennen waarmee ze zich onderscheiden van andere entiteiten: een distinguished name, een hash of een certificaat. Door middel van een registratiesysteem wordt ervoor gezorgd dat iedere geregistreerde waarde binnen een domein uniek blijft.

**REGISTRATIEVELD-INFORMATIE**

Gegevens als het adres, de leeftijd en het geslacht van de gebruiker.

**RELYING PARTY**

Een ontvanger die vertrouwen stelt in een certificaat en een digitale handtekening.

**REPOSITORY**

Een database met certificaten en andere relevante informatie die on-line toegankelijk is.

**ROOT**

De UA die het eerste certificaat in een certificatieketen uitgeeft. Om een certificatieketen te kunnen valideren, dient de publieke sleutel van de root vooraf bekend te zijn bij de gebruiker van een certificaat. De betrouwbaarheid van de publieke sleutel van de root komt niet door een certificaat tot stand, maar door een ander systeem (zoals beveiligde fysieke distributie).

**RSA**

Een cryptografisch systeem middels publieke sleutels, ontwikkeld door Rivest, Shamir & Adelman.

# S

**S/MIME**

Specificatie voor beveiliging van e-mail waarbij gebruik wordt gemaakt van een cryptografische berichtensyntax in een Internet MIME-omgeving.

**SCHRIFT**

Informatie in een record die toegankelijk is en op een later tijdstip voor referentiedoeleinden kan worden gebruikt.

**SERIENUMMER VAN EEN CERTIFICAAT**

Een waarde waarmee eenduidig kan worden vastgesteld dat een certificaat door een UA is gemaakt.

**SERVER**

Een computersysteem dat aanvragen van client-systemen behandelt.

**SLEUTELPAAR**

Een geheime sleutel en de daarmee corresponderende publieke sleutel. Met de publieke sleutel kan een digitale handtekening worden geverifieerd die met de corresponderende geheime sleutel is aangemaakt. Bovendien kunnen onderdelen van sleutelparen – afhankelijk van het soort algoritme dat wordt gebruikt – worden gebruikt om informatie uit veiligheidsoverwegingen te versleutelen en te ontsleutelen. In dit geval kan met een geheime sleutel alleen informatie worden ontcijferd die met de corresponderende publieke sleutel is versleuteld.

**SMART CARD**

Een hardwaretoken die is voorzien van een of meerdere geïntegreerde circuits (IC's), waarmee cryptografische bewerkingen kunnen worden uitgevoerd en die is voorzien van een ingebouwde, fraudebestendige beveiliging.

**SPLITSSEN VAN GEHEIME DELEN**

Het verdelen van de geheime delen van een geheime sleutel over een aantal houders.

# T

**TOEGANG**

Een specifieke vorm van interactie tussen een aanvraag en communicatie- of informatiebronnen, resulterend in een informatiestroom, het uitoefenen van controle of het in gang zetten van een proces.

**TOETSINGSZIN**

Een verzameling cijfers en/of letters, gekozen door de aanvrager van een certificaat en kenbaar gemaakt aan de UA bij de certificaataanvraag, die door de UA wordt gebruikt voor de authenticatie van de gebruiker voor verschillende doeleinden (zoals vereist in de CPS). Een toetsingszin kan ook worden gebruikt door de houder van een geheim deel voor de authenticatie jegens de verstrekker van een geheim deel.

**TOKEN**

Een hardwarecomponent voor beveiligingsdoeleinden, met de geheime sleutel(s) van een

gebruiker, het publieke-sleutelcertificaat, en - indien gewenst – een geheime vermelding van andere certificaten, waaronder alle certificaten in de certificatieketen van een gebruiker.

#### **TRANSACTIE**

De overdracht van zakelijke informatie middels de computer, bestaande uit specifieke processen om communicatie over wereldwijde netwerken mogelijk te maken.

#### **TRUSTED ROOT**

Een trusted root is een publieke sleutel die is verbonden aan een UA, hetgeen is geconfirmeerd door een gebruiker of systeembeheerder. Software en systemen voor authenticatie op basis van publieke cryptografie en certificaten gaan ervan uit dat de waarde van deze sleutel op correcte wijze verkregen is. Dit wordt bevestigd door het feit dat er altijd toegang wordt verkregen tot de sleutel vanuit een betrouwbare systeem-repository, waarin alleen geïdentificeerde en betrouwbare beheerders bevoegd zijn om wijzigingen door te voeren.

#### **TRUSTED THIRD PARTY (TTP)**

Een onafhankelijke en objectieve derde partij, die een bijdrage levert aan een optimale beveiliging en betrouwbaarheid van een geautomatiseerde overdracht van informatie. De aanwezigheid van een trusted third party impliceert niet het bestaan van een ‘trustor-trustee’-relatie of een andere vertrouwensrelatie.

#### **TYPE (CERTIFICAAT)**

De bepalende eigenschappen van een certificaat waarmee het gebruik ervan wordt beperkt tot de categorie toepassingen die slechts voor dat type zijn voorbehouden.

## **U-V**

#### **UA-CERTIFICAAT**

Een certificaat dat is uitgegeven door een bovengeschiede UA aan een ondergeschiede UA.

#### **UITGEVENDE AUTORITEIT (UA)**

Binnen de publieke certificatediensten van VeriSign de VR, PCA of CA (of ondergeschiede CA) die een certificaat uitgeeft, blokkeert of intrekt. UA's identificeren zich door de unieke naam die ze vermelden op alle certificaten en CRL's die ze uitgeven. Indien hiertoe vooraf toestemming van VeriSign is verkregen, mag een UA de verantwoordelijkheid voor het beoordelen en toekennen/afwijzen van certificaataanvragen overdragen aan één of meerdere LRA's die geen eigendom zijn van of worden bestuurd door de UA, conform CPS § 2.1.3. Indien voornoemde overdracht van bevoegdheden heeft plaatsgevonden en vervolgens in deze CPS het begrip “UA” wordt gebruikt, dan zullen alle verplichtingen, borgstellingen, waarborgen en niet-aansprakelijkheidsclausules tevens van toepassing zijn op voornoemde LRA's.

#### **UITGEVER VAN EEN GEHEIM DEEL**

Persoon aangewezen door een UA voor het maken en splitsen van geheime delen.

**UITGIFTE VAN EEN CERTIFICAAT**

De acties die worden uitgevoerd door een UA om een certificaat te maken en om de aanvrager van het certificaat (die gebruiker wenst te worden) op de hoogte te stellen van de inhoud van het certificaat.

**UNIFORM RESOURCE LOCATOR (URL)**

Een gestandaardiseerde methode voor het identificeren en lokaliseren van bepaalde records en andere bronnen op het World Wide Web.

**VALIDATIE (VAN EEN CERTIFICAATAANVRAAG)**

Het proces dat wordt uitgevoerd door een UA (of diens LRA) nadat een aanvraag is ingediend tot uitgifte van een certificaat. Dit is een vereiste voordat een aanvraag wordt goedgekeurd en een certificaat wordt uitgegeven.

**VERIFIEREN (VAN EEN CERTIFICAAT)**

Het proces dat wordt uitgevoerd door een ontvanger of relying party om na te gaan of een gebruikerscertificaat geldig is op het moment dat een bepaalde digitale handtekening wordt geplaatst.

**VERIFIEREN (VAN EEN CERTIFICATIEKETEN)**

Het proces dat voor ieder certificaat in een keten wordt uitgevoerd door de ontvanger of relying party om de publieke sleutel te authenticeren (voor ieder certificaat) en om te confirmeren dat ieder certificaat geldig is, is uitgegeven binnen de geldigheidsduur van het bijbehorende UA-certificaat en dat alle betrokken partijen (UA's, gebruikers, ontvangers en relying parties) hun taken met betrekking tot alle certificaten binnen de keten hebben vervuld conform deze CPS.

**VERIFIEREN (VAN EEN DIGITALE HANDTEKENING)**

Het met betrekking tot een bepaalde digitale handtekening, bericht of publieke sleutel nauwgezet nagaan of: (i) de digitale handtekening is gemaakt tijdens de geldigheidsduur van een geldig certificaat met behulp van de geheime sleutel die correspondeert met de publieke sleutel die is vermeld in het certificaat en (ii) het bijbehorende bericht geen wijzigingen heeft ondergaan nadat de digitale handtekening is gemaakt.

**VEILIG KANAAL**

Een middels cryptografie verbeterd communicatiepad dat berichten beschermt tegen mogelijke bedreigingen inzake de veiligheid ervan.

**VERISIGN-ROOT**

Een UA die PCA's registreert door de zelf ondertekende publieke sleutel van iedere PCA te registreren.

**VERLENGING**

Het verwerven van een nieuw certificaat (zelfde klasse, zelfde type) voor hetzelfde doel nadat het bestaande certificaat vervallen is.

**VERTROUWELIJKHEID**

Het feit dat gevoelige informatie geheim wordt gehouden en alleen aan daartoe bevoegde partijen bekend wordt gemaakt.

**VERTROUWEN OP (een CERTIFICAAT en een DIGITALE HANDTEKENING)**

Het accepteren van een digitale handtekening en het zich gedragen op een wijze die nadelige gevolgen zou kunnen hebben in geval van ongeldigheid van de handtekening.

**VERTROUWEN**

De aanname dat een entiteit zich in grote lijnen op een vooraf verwachte manier zal gedragen. Vertrouwen kan ook alleen betrekking hebben op een bepaalde taak. De belangrijkste rol van dit begrip binnen het kader van authenticatie is het beschrijven van de verhouding tussen een authenticatie-entiteit en een UA. Een authenticatie-entiteit dient er vertrouwen in te hebben dat de UA louter geldige en betrouwbare certificaten maakt. De gebruikers van deze certificaten zijn weer afhankelijk van het vertrouwen dat de authenticatie-entiteit in een UA stelt.

**VERTROUWENSPERSOON**

Persoon die zich bevindt in een vertrouwenspositie en bevoegd is om de bijbehorende taken binnen het kader van deze CPS te vervullen.

**VERTROUWENSPOSITIE**

Plaats binnen een UA met toegang tot of controle over cryptografische bewerkingen die direct invloed kunnen hebben op de uitgifte, het gebruik, de blokkering of intrekking van certificaten. Hiertoe behoren ook activiteiten die de toegang tot een repository kunnen beperken.

**VERVALDATUM VAN EEN CERTIFICAAT**

De datum en tijd, vermeld op het certificaat, waarop de geldigheidsduur van het certificaat eindigt indien geen sprake is van eerdere blokkering of intrekking.

**VOORLOPIG CERTIFICAAT**

Een Klasse 2-certificaat gedurende de eerste 21 dagen van de geldigheidsduur, uitgegeven na het succesvol afronden van alle vereiste validatieprocedures die binnen de UA gelden met betrekking tot een aanvraag van een Klasse 2-certificaat. De voorlopige status geeft aan dat de validatie van de certificaataanvraag aangaande de identiteit van de gebruiker nog dient te worden afgerond middels een "mail-back"-procedure naar het opgegeven postadres.

# W-Z

**WACHTWOORD (PIN-CODE)**

Vertrouwelijke informatie, meestal een reeks tekens, waarmee toegang kan worden verkregen tot bepaalde computerfuncties.

**WERKNEMER MET EEN GOEDE REPUTATIE**

Een werknemer die niet in zijn of haar proefperiode zit, is ontslagen of op non-actief is gesteld, en jegens wie zijn of haar werkgever geen disciplinaire maatregelen heeft getroffen.

**WORLD WIDE WEB (WWW)**

Een op hypertext gebaseerd, wijdverbreid informatiesysteem, waarmee gebruikers hypertext-documenten kunnen maken, bewerken of doorbladeren. Een medium om grafische documenten te maken en op te vragen; een verzameling onderling verbonden documenten op Internet.

**X.509**

De standaard van de ITU-T (International Telecommunications Union-T) voor certificaten. X.509 v3 heeft betrekking op certificaten die extensies (kunnen) bevatten.

**ZELF ONDERTEKENDE PUBLIEKE SLEUTEL**

Een gegevensstructuur die op dezelfde wijze is samengesteld als een certificaat, maar wordt ondertekend door de houder. Een zelf ondertekende publieke sleutel kan niet, zoals een certificaat, worden gebruikt om een publieke sleutel op een betrouwbare manier te authenticeren ten behoeve van andere partijen. Een zelf ondertekende publieke sleutel van een PCA die digitaal is ondertekend door de Root kan worden beschouwd als een certificaat.

\*\*\*

## MEDEWERKING AAN DEZE CPS

KPN Telecom en VeriSign zijn de volgende mensen erkentelijk voor alle suggesties, aanbevelingen en andere hulp bij het tot stand komen van de Certification Practice Statement van VeriSign, waarop deze CPS is gebaseerd.

### Juridische Zaken

Professor Dr. Mads Bryde Andersen	Universiteit van Kopenhagen, Denemarken
Harold S. Burman, Esq.	U.S. State Department
Robert Daniels, Esq.	U.S. Social Security Administration
Professor Jos Dumortier	Universiteit van Leuven, België
Deborah Fuerer, Esq.	United States Fidelity and Guaranty Company
Eugene E. Hines, Esq.	American Society of Notaries
Janette M. Hoover, Esq.	Tomlinson Zisko Morosoli & Maser LLP
Toshio Kosone, Esq.	Kosone & Associates, Japan
Charles R. Merrill, Esq.	McCarter & English
Ray Nimmer, Esq.	Weil, Gotshal & Manges
Arthur F. Purcell, B.E., J.D.	U.S. Patent and Trademark Office
Ira Rubenstein, Esq.	Microsoft Corporation
John D. Ryan, Esq.	America Online, Inc.
Ruven Schwartz, Esq.	West Publishing Company
John F. Simanski Jr., Esq.	United States Fidelity and Guaranty Company
Michiru Takahashi, Esq.	Showa Law Office, Japan
Timothy Tomlinson, Esq.	Tomlinson Zisko Morosoli & Maser LLP
Shinya Watanabe, Esq.	Showa Law Office, Japan

### Technologie

Frank Chen	Netscape Communications Corporation
Allan Cooper	Microsoft Corporation
Steve Crocker	CyberCash, Inc.
Steve Dussé	RSA Data Security, Inc.
Taher Elgamal, Ph.D.	Netscape Communications Corporation
James M. Galvin, Ph.D.	CommerceNet
Peter Landrock, Ph.D.	Cryptomathic, Denemarken
Ron Rivest, Ph.D.	Massachusetts Institute of Technology
Jeff Schiller	Massachusetts Institute of Technology
Allan Shiffman	Terisa Systems
David I. Solo	BBN, Inc.

### Management & Consultancy

Dwight Arthur	National Securities Clearing Corporation
Kaye Caldwell	Software Industry Coalition
Bruce Crabtree	Conanicut Communications
F. Jo Goodson	Goldman, Sachs & Co.
Mark Greene, Ph.D.	IBM Corporation
F. Lynn McNulty	RSA Data Security, Inc.
Michel Peereman	Belgische Federatie van Kamers van Koophandel

Guy Richard

La Poste, Frankrijk

### **Audits en zakelijke controles**

Eric T. Ashdown

KPMG Peat Marwick

Cris R. Castro, CISP

Ernst & Young (voorheen KPMG Peat Marwick)

Kevin M. Coleman

KPMG Peat Marwick

Steven A. Dougherty

KPMG Peat Marwick

Martin Ferris

U.S. Department of the Treasury

Dwight Olsen

Data Securities International

Gary W. Riske

KPMG Peat Marwick

Professor Horton Sorkin, Ph.D.

Howard University

Stephen Spaulding

KPMG Peat Marwick

Geoffrey W. Turner

Ernst & Young (voorheen KPMG Peat Marwick)

Daarnaast worden de Information Security Committee, de Electronic Commerce and Information Technology Division, de Section of Science and Technology van de American Bar Association, afdeling Digital Signature Guidelines, bedankt voor alle initiatieven bij het tot stand komen van specifieke procedures.

Ten slotte: de specificatie door MasterCard/Visa van het Secure Electronic Transaction (SET)-protocol is erkend als bron van ontwerpprocedures (zoals hiërarchie) - deze CPS streeft overeenstemming met dit protocol na.

### **OPMERKINGEN EN AANBEVELINGEN**

Opmerkingen en aanbevelingen voor toekomstige versies van deze CPS worden door ons bijzonder op prijs gesteld. Ze kunnen per E-mail worden verstuurd naar [info@certificaat.kpn.com](mailto:info@certificaat.kpn.com) of naar [practices@VeriSign.com](mailto:practices@VeriSign.com).