

Handreiking cross-border herkenning elektronische handtekeningen

Het beoordelen van elektronische handtekeningen uit
het buitenland

Auteur Projectbureau eHerkenning
Versie 0.9.1
Status Concept
Den Haag, 16-12-2009



Document informatie

Colofon

Auteur	Status
Projectbureau eHerkenning	Concept
Project	Datum
eHerkenning voor Bedrijven	16-12-2009
Organisatie	Classificatie
ICTU eOverheid voor Bedrijven	Openbaar
Titel	Locatie
Handreiking cross-border herkenning elektronische handtekeningen	Den Haag
Versie	
0.9.1	

Historie

Datum	Versie	Wijziging	Status	Verwerkt door
04-10-09	0.1	Eerste conceptversie met hoofdlijnen	Concept	ICTU Project eHerkenning
01-12-09	0.2	Processchema's stappenplan Aanpassingen als gevolg van gepubliceerde beschikking	Concept	ICTU Project eHerkenning
09-12-09	0.9	Reviewcommentaar verwerkt	Concept	ICTU Project eHerkenning
16-12-09	0.9.1	Aangepast aan resultaten praktisch gebruik.	Concept, geschikt voor publicatie.	ICTU Project eHerkenning

Goedkeuring

Datum	Naam	Versie
15-12-09	EZ/DGET	0.9.1

Inhoud

1	Inleiding	5
1.1	Achtergrond	5
1.2	Doel van dit document	6
1.3	Doelgroep van dit document	6
1.4	Scope	6
1.5	Status van dit document	6
1.6	Referenties	7
1.7	Definities	7
1.8	Leeswijzer	8
2	Kader	9
2.1	Verplichte acceptatie van elektronische handtekeningen	9
2.2	Uitgangspunten	10
2.3	Randvoorwaarden	10
3	Elektronische handtekeningen	11
3.1	Introductie elektronische handtekening	11
3.2	Beoordelen van een elektronische handtekening	12
3.3	Positionering handreiking in relatie tot het beoordelen van een elektronische handtekening	12
4	Procesflow op hoofdlijnen	14
4.1	Vorbereidende geautomatiseerde handelingen	14
4.2	Handmatige processtappen	16
4.2.1	Betrouwbaarheid van de CDV	16
4.2.2	Betrouwbaarheid van de handtekening	17
5	Processtappen	18
5.1	Betrouwbaarheid van de CDV	18
5.1.1	Destilleren CDV-dienst waarmee het certificaat is uitgegeven	20
5.1.2	Opzoeken Vertrouwenslijst van de Europese Commissie	22
5.1.3	Opzoeken Vertrouwenslijst van de betreffende EU-lidstaat	22
5.1.4	Opzoeken en verifiëren CDV-dienst	23
5.2	Betrouwbaarheid van de handtekening	24
5.2.1	Introductie	25
5.2.2	Opzoeken gebruik van een SSCD in de Vertrouwenslijst	25
5.2.3	Detailgegevens certificaat openen	25
5.2.4	Bepalen sleutelgebruik en gebruik van een SSCD voor de handtekening	26
5.2.5	Nagaan overeenstemming aanvrager en ondertekenaar	27
5.3	Aanvullende geautomatiseerde ondersteuning vanuit ICT	27
5.4	Wat te doen bij twijfel over de betrouwbaarheid van een elektronische handtekening?	28
6	Interpretatie Vertrouwenslijst (Trusted List)	29

.....

6.1	Introductie	29
6.2	Identificatie en beheerder Vertrouwenslijst	29
6.2.1	TSL type / SLV-type (clause 5.3.3)	30
6.2.2	Scheme operator name / Naam uitvoerder van de regeling (clause 5.3.4)	30
6.3	De regels op basis waarvan partijen op de lijst worden opgenomen	30
6.3.1	Scheme information URI / URI met informatie over de regeling (clause 5.3.7)	30
6.3.2	Status determination approach / Bepaling van de status (clause 5.3.8)	30
6.3.3	Scheme territory / Gebied van de regeling (clause 5.3.10)	31
6.3.4	TSL policy/legal notice / SLV-beleid/juridische informatie (clause 5.3.11)	31
6.4	Beheer van de Vertrouwenslijst	31
6.4.1	Historical information period / Periode van historische informatie (clause 5.3.12)	31
6.4.2	Pointers to other TSL's / Verwijzingen naar andere SLV's (clause 5.3.13)	31
6.4.3	List issue date and time en next update / Publicatiedatum en -uur van de lijst en volgende aanpassing (clause 5.3.14 en 5.3.15)	31
6.5	Overzicht van partijen die gekwalificeerde certificaten uitgeven	32
6.5.1	Introductie	32
6.5.2	Contactgegevens van de VVD	32
6.5.3	Beleid en voorwaarden van de VVD	32
6.5.4	TSP list of services / VVD-dienstenlijst	33

1 Inleiding

Dit hoofdstuk geeft een inleiding bij deze handreiking cross-border herkenning elektronische handtekeningen.

1.1 Achtergrond¹

Op 28 december 2009 moet in alle EU-lidstaten de Dienstenrichtlijn zijn ingevoerd. Dankzij de richtlijn kunnen dienstverleners zoals cateraars, installatiebedrijven en horecaondernemers straks eenvoudiger aan de slag in de EU, wat de economische groei in deze sector kan stimuleren. Alle overheden leveren daaraan een bijdrage, waaronder gemeenten, provincies en waterschappen, centrale overheden zoals ministeries, PBO's, uitvoeringsorganisaties en toezichthouders. In het kader van de Dienstenrichtlijn komt er in alle lidstaten een centraal elektronisch loket waar dienstverleners al hun zaken met de overheid elektronisch kunnen regelen: het Dienstenloket. In Nederland wordt dit loket ondergebracht bij www.antwoordvoorbedrijven.nl.

Met het aansluiten op het elektronisch loket kunnen overheidsorganisaties via de berichtenbox elektronische aanvragen van ondernemers verwachten voor bijvoorbeeld vergunningen. Deze aanvragen zullen in sommige gevallen ondertekend zijn met een elektronische handtekening. Ook zal in voorkomend geval een verleende vergunning worden ondertekend namens het bevoegde bestuursorgaan met een elektronische handtekening. Een elektronische handtekening is een belangrijk middel waarmee ondertekenaars van elektronisch uitgewisselde documenten een wilsuiting bekrachtigen en zekerheid geven over de onweerlegbaarheid van het ondertekende document. Het laatste betekent dat u als bevoegde instantie ervan op aan kunt dat het bericht na ondertekening niet meer is gewijzigd.

De Europese Richtlijn elektronische handtekeningen stamt uit 1999 (ref. [1]) en had tot doel het faciliteren van het gebruik van elektronische handtekeningen en het bijdragen aan de juridische erkenning. Tien jaar na de introductie van de richtlijn bleek dat er nog niet zonder meer sprake was van daadwerkelijke grensoverschrijdende erkenning van de elektronische handtekening. Een studie naar dit gegeven, zie ref. [2], heeft dit helder gemaakt, gevolgd door het doen van aanbevelingen om nadere grensoverschrijdende erkenning te realiseren. Dit heeft onder meer geleid tot een beschikking (ref. [3], [4]) met als doel de invoering van een Vertrouwenslijst (VL, of ook wel SLV – Statuslijst Vertrouwensdiensten of Trust-service Status List – TSL- of Trusted List – TL genoemd). Deze lijst is een lijst per lidstaat van de Europese Unie waarop de partijen ("Certificatiedienstverlener – CDV of "Certification Service Providers" – CSP's) zijn opgenomen die in die betreffende lidstaat de middelen (met name certificaten) uitgeven waarmee elektronische handtekeningen gezet kunnen worden. Voor de korte termijn heeft de Europese Unie gekozen voor een verplichte implementatie van een lijst die handmatig geraadpleegd kan worden en optioneel beschikbaar gesteld kan worden voor geautomatiseerde raadpleging (zie ref. [3], [4]). Deze handmatige raadpleging is geen eenvoudige handeling. Evenmin is het volledig beoordelen van de betrouwbaarheid van een elektronische handtekening een eenvoudige handeling. Om die reden is vanuit het project eHerkenning deze handreiking opgesteld.

¹Deels ontleend aan ref. 7



1.2 Doel van dit document

Dit document heeft als doel een handreiking te bieden voor het beoordelen van een ontvangen elektronische handtekening, waarbij deze beoordeling wordt uitgevoerd conform de afspraken die binnen de Europese Unie gemaakt zijn. De handreiking beoogt daarmee de handmatige controle zo hanteerbaar als mogelijk te maken.

Daarbij richt dit document zich op een volledige controle. In de praktijk is het denkbaar dat een deel van het controleproces alsnog door de ICT-afdeling geautomatiseerd wordt in de lokale ICT-infrastructuur. Een aparte paragraaf zal hier nader op in gaan.

1.3 Doelgroep van dit document

De doelgroep van dit document bestaat uit de ambtenaren van de overheidsdienstverleners die aanvragen en andere elektronisch getekende documenten en formulieren ontvangen. De binnen Europa gekozen oplossingsrichting stelt de nodige eisen aan de gebruikers hiervan en daarmee van deze handreiking. De beoogde gebruiker moet zich thuis voelen in ICT-toepassingen en moet in staat zijn om de relatief technische reeks van handelingen uit te voeren.

1.4 Scope

Deze versie van de handreiking richt zich op de beoordeling van elektronische handtekeningen waarbij gebruik wordt gemaakt van de gangbare oplossingen op de werkplek van de persoon die de beoordeling uitvoert, in combinatie met een handmatige controle van de Vertrouwenslijst.

Dit document heeft uitsluitend betrekking op de handtekeningen van het niveau die binnen de Europese Unie zijn vastgesteld in het kader van de Dienstenrichtlijn. Dit betreft de zogenoemde “geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat” en een “gekwalficeerde elektronische handtekening”. Onder dit laatste type handtekening wordt verstaan een “geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat en aangemaakt met een veilig middel”².

Dit document gaat *niet* in op de geautomatiseerde controle van de Vertrouwenslijst.

Het document beschrijft de beoordeling van een ontvangen handtekening. Dit document gaat niet in op het *zetten* van een elektronische handtekening.

Deze handreiking gaat *niet* in op de benodigde technische inrichting en inzet van applicaties om handtekeningen technisch te kunnen interpreteren. Deze inrichting en applicaties zijn randvoorwaarden om de handmatige stappen te kunnen uitvoeren. Dit document gaat uit van een situatie waarbij dergelijke middelen reeds voorhanden zijn.

1.5 Status van dit document

Dit document is versie 0.9 van de handreiking cross-border herkenning elektronische handtekeningen. Dit document biedt daartoe een inzicht in de te nemen stappen voor het

²De gekwalificeerde elektronische handtekening is als term niet gedefinieerd in de Nederlandse Wet elektronische handtekeningen, maar wordt wel gebruikt in de beschikking met betrekking tot de Vertrouwenslijst.

beoordelen van elektronische handtekeningen, en dient enerzijds als basis voor overheidsdienstverleners om de benodigde processen voor het beoordelen van elektronische handtekeningen in te bedden in hun organisatie en anderzijds om in de praktijk beproefd te worden. De voorliggende versie bevat nog niet de verwijzing naar de Vertrouwenslijst van de Europese Commissie. Zowel de plaats van publicatie als de daadwerkelijke vormgeving van deze lijst was ten tijde van het verschijnen van deze versie niet bekend.

De volgende versie van deze handreiking zal de volgende wijzigingen bevatten. Ten eerste zal de handreiking waar nodig aangepast worden aan de hand van beproeving in de praktijk. Ten tweede zal de verwijzing naar de Europese Vertrouwenslijst worden toegevoegd zodra deze beschikbaar is.

1.6 Referenties

- [1] RICHTLIJN 1999/93/EG VAN HET EUROPEES PARLEMENT EN DE RAAD van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, d.d. 19 januari 2000.
- [2] Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications Report, Siemens / TimeLex, A Study for the European Commission (DG Information Society and Media), November 2007.
- [3] Commission Decision 2009/767/EC of 16 October 2009, d.d. 20 October 2009 (followed by a corrigenda published on 14 November 2009), C(2009)7806.
- [4] Beschikking van de Commissie 2009/767/EC van 16 oktober 2009, d.d. 20 oktober 2009 (gevolgd door een rectificatie gepubliceerd op 14 november 2009), C(2009)7806.
- [5] PKIoverheid website <http://www.pkioverheid.nl>.
- [6] Study on the standardisation aspects of eSignature, SEALED / DLA Piper / Across communications, A Study for the European Commission (DG Information Society and Media), final report, d.d. 22 November 2007.
- [7] Rapport BEOORDELING VAN ELEKTRONISCHE HANDTEKENINGEN, Capgemini in opdracht van het Ministerie van EZ, versie 1.0.
- [8] PKIoverheid Handreiking Medewerker, GBO.overheid, augustus 2006.
- [9] Factsheet De elektronische handtekening en de Dienstenrichtlijn, Ministerie van Economische Zaken, 2009.

1.7 Definities

Met de huidige stand der techniek en standaardisatie is het niet te voorkomen dat gebruikers worden geconfronteerd met definities van technische aard. Voor een deel van deze definities wordt verwezen naar de website van PKIoverheid: <http://www.pkioverheid.nl> (ref. [5]). Overige definities zijn opgenomen in de bijlage van dit document.

De voor dit document relevante terminologie die tevens onderdeel uitmaakt van de Beschikking van de Europese Commissie (ref. [3] en [4]), wordt in principe in het Nederlands weergegeven. De gebruikte terminologie in de Vertrouwenslijst zelf wordt zowel in de Nederlandse als Engelse taal weergegeven.

1.8 Leeswijzer

Hoofdstuk 2 beschrijft het kader dat gehanteerd is bij het opstellen van deze handreiking. Dit hoofdstuk is van belang voor iedereen die elektronische handtekeningen beoordeelt omdat het ingaat op de verplichting tot het accepteren van elektronische handtekeningen en op de eisen aan de gebruikersorganisatie die ingevuld moeten zijn voordat beoordeling kan plaatsvinden.

Hoofdstuk 3 positioneert deze handreiking in het proces van het beoordelen van elektronische handtekeningen en introduceert de elektronische handtekening. Het hoofdstuk is primair bedoeld voor eenmalige ter kennisname.

Hoofdstuk 4 toont de procesflow op hoofdlijnen en is bedoeld om een overzicht te geven van het totale proces. Het hoofdstuk is primair bedoeld voor eenmalige ter kennisname.

Hoofdstuk 5 geeft een nadere detaillering van de afzonderlijke processtappen. Dit hoofdstuk is de kern van de handreiking en beschrijft de afzonderlijke stappen en keuzemomenten in de daadwerkelijke beoordeling van een individuele handtekening.

Hoofdstuk 6 gaat in op de betekenis van de verschillende velden in de Vertrouwenslijst, een centrale component in het beoordelen van elektronische handtekeningen. Dit hoofdstuk dient daarmee als naslag voor verdere achtergrondinformatie.

In de appendix zijn definities opgenomen.

2 Kader

Er zijn vele verschillende wijzen van implementatie van de validatie van elektronische handtekeningen. Dit hoofdstuk gaat in op de verplichte acceptatie van een elektronische handtekening en geeft een opsomming van de relevante uitgangspunten en randvoorwaarden op basis waarvan deze handreiking is opgesteld.

2.1 Verplichte acceptatie van elektronische handtekeningen

Een geldige elektronische handtekening die is ontvangen in het kader van de Dienstenrichtlijn, kan niet geweigerd worden wanneer het gaat om een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat of een gekwalificeerde elektronische handtekening, zie ook ref. [3] en [4]. Wanneer uw proces helemaal niet om een handtekening vraagt, kunt u een binnengekomen elektronische handtekening negeren. In de gevallen dat zekerheid over de wil en identiteit van de aanvrager naar uw oordeel niet nodig is, hoeft u de handtekening ook niet op echtheid te controleren.

Wanneer u echter op basis van een risicoanalyse heeft vastgesteld dat u voor een bepaalde transactie een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat nodig heeft, bent u ook verplicht om geavanceerde elektronische handtekeningen uit andere lidstaten te accepteren en om handtekeningen van een hoger betrouwbaarheidsniveau – de gekwalificeerde elektronische handtekening – te accepteren. Wanneer een overheidsdienstverlener ondertekening vraagt door middel van bijvoorbeeld een geavanceerde elektronische handtekening zonder gekwalificeerd certificaat, dan moet deze overheidsdienstverlener ook de geavanceerde handtekening met gekwalificeerd certificaat of de gekwalificeerde handtekening accepteren. Door toepassing van het principe dat handtekeningen van een hoger niveau ook gebruikt kunnen worden voor processen waar een lager niveau volstaat, wordt voorkomen dat ondernemers voor ieder proces een verschillende handtekening moeten aanschaffen.

Een elektronische handtekening mag wel geweigerd worden als uit de beoordeling blijkt dat deze niet geldig of betrouwbaar is. Een elektronische handtekening die niet geldig is, mag dus geweigerd worden. Een elektronische handtekening die niet voldoet aan de eisen uit de beschikking (ref. [3] en [4]) mag ook geweigerd worden. In het geval dat u een onbetrouwbare elektronische handtekening ontvangt, kunt u de afzender hiervan in kennis stellen. De wijze waarop de beoordeling van de elektronische handtekening plaatsvindt, is onderwerp van deze handreiking.



2.2 Uitgangspunten

Deze paragraaf beschrijft de punten op basis waarvan de handreiking is vormgegeven.

1. Deze handreiking gaat uit van het beoordelen van geavanceerde elektronische handtekeningen gebaseerd op een gekwalificeerd certificaat en van gekwalificeerde elektronische handtekeningen, conform de eisen zoals gedefinieerd in ref. [1]³.
2. Deze lijst van de Europese Commissie is tevens in XML-formaat en getekend met een elektronische handtekening.
3. Er zijn enkele lidstaten zijn die hun Vertrouwenslijst beschikbaar stellen in XML- en mogelijk ASN.1-formaat, al dan niet elektronisch getekend en/of via een beveiligde web-verbinding (TLS/SSL). Een dergelijke lijst is geautomatiseerd raadpleegbaar en valt om die reden buiten de scope van dit document. In dat geval dient de te gebruiken applicatie in staat te zijn om volgens de daartoe geldende standaarden de Vertrouwenslijst elektronisch te raadplegen.

2.3 Randvoorwaarden

Deze paragraaf bevat een opsomming van maatregelen die reeds genomen moeten zijn om de handreiking te kunnen gebruiken. Deze (veelal technische inrichting die gereed moet zijn om met handtekeningen te kunnen omgaan) zijn randvoorwaardelijk voor het gebruik van de handreiking.

1. Deze handreiking is gebaseerd op een situatie waarbij de benodigde technische inrichting en inzet van oplossingen om handtekeningen technisch te kunnen interpreteren, aanwezig zijn. Dit betekent dat er ICT-middelen zijn ingezet die het gebruik van elektronische handtekeningen mogelijk maken.
2. De Europese Commissie stelt een Vertrouwenslijst beschikbaar, bestaande uit een verwijzing naar alle Vertrouwenslijsten van de lidstaten van de Europese Unie.
3. Alle lidstaten stellen een Vertrouwenslijst beschikbaar in PDF-formaat. In voorkomende gevallen is de lijst getekend, in andere gevallen is deze beschikbaar via een beveiligde web-verbinding (TLS/SSL).
4. De machine waar de handtekening wordt gecontroleerd is voorzien van een applicatie die de volgende functionaliteit ondersteunt:
 1. Handtekeningformaten XAdES -BES en -EPES, CAdES -BES en -EPES en PAdES Basic variant (part II van de specificatie).
 2. Padvalidatie bij een certificaathierarchie zodat bij de verificatie van een certificaat ook de certificaten uit de eventuele bovenliggende PKI-hierarchie op geldigheid worden gecontroleerd.

³In de richtlijn elektronische handtekeningen wordt overigens de geavanceerde elektronische handtekening gedefinieerd, evenals het gekwalificeerd certificaat. De term gekwalificeerde elektronische handtekening wordt niet als zodanig gedefinieerd, maar wordt genoemd wordt een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat én is aangemaakt met een veilig middel (VMAH, Veilig Middel voor het Aanmaken van Handtekeningen of SSCD, Secure Signature Creation Device).

3 Elektronische handtekeningen

Met de invoering van de elektronische dienstenrichtlijn en de stand der techniek wordt de kans steeds groter dat u als ambtenaar bij een overheidsdienstverlener een elektronisch ondertekend document of formulier ontvangt. Dit hoofdstuk geeft een korte introductie van elektronische handtekeningen, relevant voor deze handreiking. De tekstpassages zijn ontleend aan ref. [7]. De volgende hoofdstukken gaan in op de daadwerkelijk uit te voeren processtappen om een elektronische handtekening te beoordelen.

3.1 Introductie elektronische handtekening

De elektronische handtekening is, zoals de naam al doet vermoeden, de elektronische variant op de handgeschreven handtekening die al honderden jaren wordt gebruikt. Hoewel de elektronische handtekening er heel anders uitziet dan een handgeschreven versie, is het doel hetzelfde. Technisch gezien is een elektronische handtekening een bestand dat een afzender van een bericht of document kan meesturen. Een handtekening heeft tot doel om de identiteit van de ondertekenaar te bevestigen, en om vast te leggen dat deze de inhoud van het document onderschrijft. In het geval van een handgeschreven handtekening kan de handtekening worden gecontroleerd aan de hand van een betrouwbare bron. Een betrouwbare bron is bijvoorbeeld een paspoort of een handtekeningenregister .

Het is belangrijk om de samenhang maar ook de verschillen tussen herkenning en de handtekening goed in het oog te houden. Herkenning is in essentie het proces dat erop gericht is zekerheid te verschaffen over de identiteit van iemand. Een handtekening verschaft een ontvangende partij een rechtens bruikbare bevestiging van een verklaring of wilsuiking van een persoon. Een handtekening kan gebruikt worden voor herkenning, mits de ontvangende partij met de gewenste mate van betrouwbaarheid het verband kan leggen tussen de handtekening en de daarbij behorende identiteit van de persoon die de handtekening heeft gezet. Indien voldaan wordt aan de daartoe relevante eisen (zie ref. [1]) is sprake van een geavanceerde elektronische handtekening.

Elektronische handtekeningen zijn bedoeld als digitale bron van vertrouwen. Daarvoor is het noodzakelijk dat de ontvanger van een elektronisch ondertekend document voldoende zekerheid heeft over wie de handtekening heeft gezet. De partij die garant staat voor de koppeling van een handtekening aan een persoon en onder toezicht staat van de overheid, wordt doorgaans aangeduid met de term certificatedienstverlener, kortweg CDV (of ook wel Certification Service Provider – CSP). Een handtekening met hoge betrouwbaarheid is gebaseerd op een publiekesleutelinfrastructuur, kortweg PKI (Public-Key Infrastructure). In deze handreiking wordt te allen tijde een handtekening op basis van PKI bedoeld. U vindt achtergrondinformatie over PKI op de website van PKIoverheid, ref. [5]).

Voor het vastleggen van de koppeling tussen personen en openbare sleutels binnen een PKI wordt gebruik gemaakt van digitale certificaten. Een digitaal certificaat is een door een CDV digitaal ondertekend elektronisch bestandje dat informatie bevat over een elektronische handtekening en over de persoon die die handtekening kan zetten (de houder van het certificaat).

.....

Certificaten die volgens strikte, hoogwaardige eisen zijn uitgegeven, worden gekwalificeerde certificaten genoemd. Deze term is gedefinieerd in ref. [1]. Uitsluitend handtekeningen die zijn aangemaakt op basis van een gekwalificeerd certificaat zijn onderwerp van deze handreiking. Er is sprake van een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat. Aanvullend kan er gebruik gemaakt zijn van een zogenaamd veilig middel (in technische termen ook wel Secure Signature Creation Device, SSCD, genoemd). Een veilig middel in de praktijk kan een smartcard of een betrouwbaar hardware 'token' zijn. In een dergelijk geval wordt gesproken van een gekwalificeerde elektronische handtekening.

3.2 Beoordelen van een elektronische handtekening

Voor het benodigde vertrouwen in een elektronische handtekening staan drie componenten in samenhang garant:

1. Vertrouwen in de certificatie dienstverlener (CDV): de uitgever van de middelen om een elektronische handtekening te plaatsen.
Als de ontvangende partij weet dat zij de CDV kan vertrouwen, dan kan zij ervan uitgaan dat die de identiteit van de houder van het certificaat op voldoende betrouwbare wijze heeft vastgesteld en vastgelegd.
2. Vertrouwen in de geldigheid van het certificaat.
Een geldig certificaat levert de ontvangende partij het volgende op:
 - informatie over welke CDV het certificaat heeft uitgegeven;
 - een bevestiging dat die CDV een identiteit heeft vastgelegd behorend bij de handtekening, en dat de gegevens op het certificaat daarmee overeenstemmen;
 - Vertrouwen in de geldigheid van de handtekening.
3. Een geldige elektronische handtekening levert de ontvangende partij het volgende op:
 - een bewijs (ook voor derde partijen) dat de handtekening gezet is door de houder van het certificaat;
 - een bevestiging dat de elektronisch getekende informatie na ondertekening niet is gewijzigd.

3.3 Positionering handreiking in relatie tot het beoordelen van een elektronische handtekening

Deze handreiking gaat met name in op de eerste component zoals genoemd in de voorgaande paragraaf: het beoordelen van de betrouwbaarheid van een CDV. Daarnaast gaat deze handreiking in op het verkrijgen van de daartoe benodigde informatie. Dit betreft stappen die horen bij de tweede component: het vertrouwen in de geldigheid van het certificaat. De derde component, de geldigheid van een elektronische handtekening, is een technische controle die in principe geautomatiseerd wordt uitgevoerd door een applicatie die certificaten ondersteunt.

De eerste component, het vertrouwen in de CDV, wordt bepaald aan de hand van de beoordeling van een zogenaamde Vertrouwenslijst. Dit is een lijst van CDV's (in de lijst benoemd onder het bredere begrip Trust Service Provider, TSP) die per lidstaat wordt bijgehouden. Op de lijst worden

gedetailleerde gegevens van CDV's opgenomen die, volgens de wetgeving in de betreffende lidstaat, betrouwbaar zijn. Deze CDV's geven middelen uit waarmee elektronische handtekeningen gezet kunnen worden conform het binnen de EU afgesproken niveau (geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat of een gekwalificeerde elektronische handtekening). Deze handreiking gaat in op de wijze waarop de Vertrouwenslijst geraadpleegd kan worden en hoe de informatie in een Vertrouwenslijst geïnterpreteerd dient te worden. Daarmee wordt zekerheid gekregen over de betrouwbaarheid van de CDV, een belangrijke pijler voor de vereiste overkoepelende betrouwbaarheid.

Om op de juiste wijze een Vertrouwenslijst te raadplegen, is informatie uit een certificaat nodig. Deze informatie wordt verkregen aan de hand van de tweede component uit de voorgaande paragraaf, het beoordelen van het vertrouwen in een certificaat. Dit betreft het verkrijgen van informatie over de CDV die het certificaat heeft uitgegeven. Daarnaast betreft dit informatie over het gebruik en de kwaliteit van het certificaat. Deze elementen worden eveneens in dit document beschreven.

4 Procesflow op hoofdlijnen

Dit hoofdstuk gaat globaal in op het proces om handtekeningen te beoordelen. Voorafgaand aan de handmatige processtappen zal een applicatie een aantal voorbereidende geautomatiseerde handelingen uitvoeren. Dit deel is beschreven in paragraaf 4.1, onder meer gebaseerd op ref. [8]. Paragraaf 4.2 beschrijft op hoofdlijnen de handmatige processtappen die nodig zijn om de beoordeling van de relevante aspecten uit paragraaf 3.2 uit te voeren. Indien gewenst is nadere achtergrondinformatie voor specifieke doelgroepen te vinden in de verschillende handreikingen van PKI-overheid, zie ref. [5].

4.1 Voorbereidende geautomatiseerde handelingen

Deze paragraaf beschrijft op hoofdlijnen de stappen die een daartoe geschikte applicatie geautomatiseerd zal uitvoeren. Deze geautomatiseerde acties gaan vooraf aan de handmatige procesflow. Een applicatie is geschikt om onderstaande handelingen uit te voeren indien deze in staat is om elektronische handtekeningen te herkennen conform de aangeboden formaten van de handtekening (zie ook paragraaf 2.3).

De geautomatiseerde acties zijn:

1. Een getekend formulier of document wordt door de applicatie ontvangen. Dit kan bijvoorbeeld een Microsoft Office document, een Open Office document, een PDF-document, maar ook een XML-formulier met elektronische handtekening zijn. De applicatie waarin het betreffende document is getekend, kan in de vorm van een service worden aangeboden door ontvangende partij (bijvoorbeeld uw organisatie) of een applicatie zijn aan de zijde van de indiener van het getekende document.
2. De applicatie controleert of de handtekening technisch geldig is aan de hand van:
 1. een controle of het document gewijzigd is na ondertekening: indien het document is gewijzigd, zal de applicatie dit opmerken en presenteren in de vorm van een melding op het scherm;
 2. een controle of het certificaat dat gebruikt is voor de handtekening op dat moment in de tijd geldig is (een certificaat heeft namelijk een beperkte geldigheidsduur van typisch 3 tot 5 jaar). Indien een certificaat is verlopen, mag de handtekening niet worden vertrouwd;
 3. een controle via het internet of het certificaat niet is ingetrokken: intrekkingen kunnen plaatsvinden als iemand geen recht meer heeft op de middelen om een handtekening te zetten of als de ondertekenaar zijn middel niet meer in het bezit heeft (bijvoorbeeld wegens diefstal of verlies). Uitgevers houden een "zwarte" lijst bij van certificaten die niet meer geldig zijn. Deze wordt via het internet automatisch geraadpleegd. Als een certificaat zich op een dergelijke lijst bevindt, mag de handtekening niet worden vertrouwd;
 4. een controle of het certificaat van de uitgevende CDV (en eventuele tussenliggende certificaten) geldig is (binnen de geldigheidsperiode en niet ingetrokken). De uitgevende CDV dient bekend te zijn in uw lokale ICT-infrastructuur om foutmeldingen te voorkomen. De applicatie kan zo worden ingesteld dat het certificaten die zijn uitgegeven door bepaalde instanties automatisch vertrouwt. Het volgende hoofdstuk

gaat nader in op de handmatige controle van de betrouwbaarheid van een CDV (door de gebruiker of door de ICT-beheerder van de lijst met vertrouwde certificaten).

Na de controle door een applicatie kan een venster worden opgevraagd door te klikken op de door de applicatiebouwer of -leverancier gekozen presentatie van de elektronische handtekening (bijvoorbeeld een icoontje dat eruit ziet als een zegel of een aanklikbare weergave van een handgeschreven handtekening). Als de ondertekening niet geldig is of als het bericht na ondertekening is gewijzigd, wordt dit duidelijk aangegeven voordat de inhoud van het document kan worden bekeken.

De bovenstaande stappen zijn (deels) ook beschikbaar via verschillende diensten op het internet. Voorbeelden van deze diensten zijn:

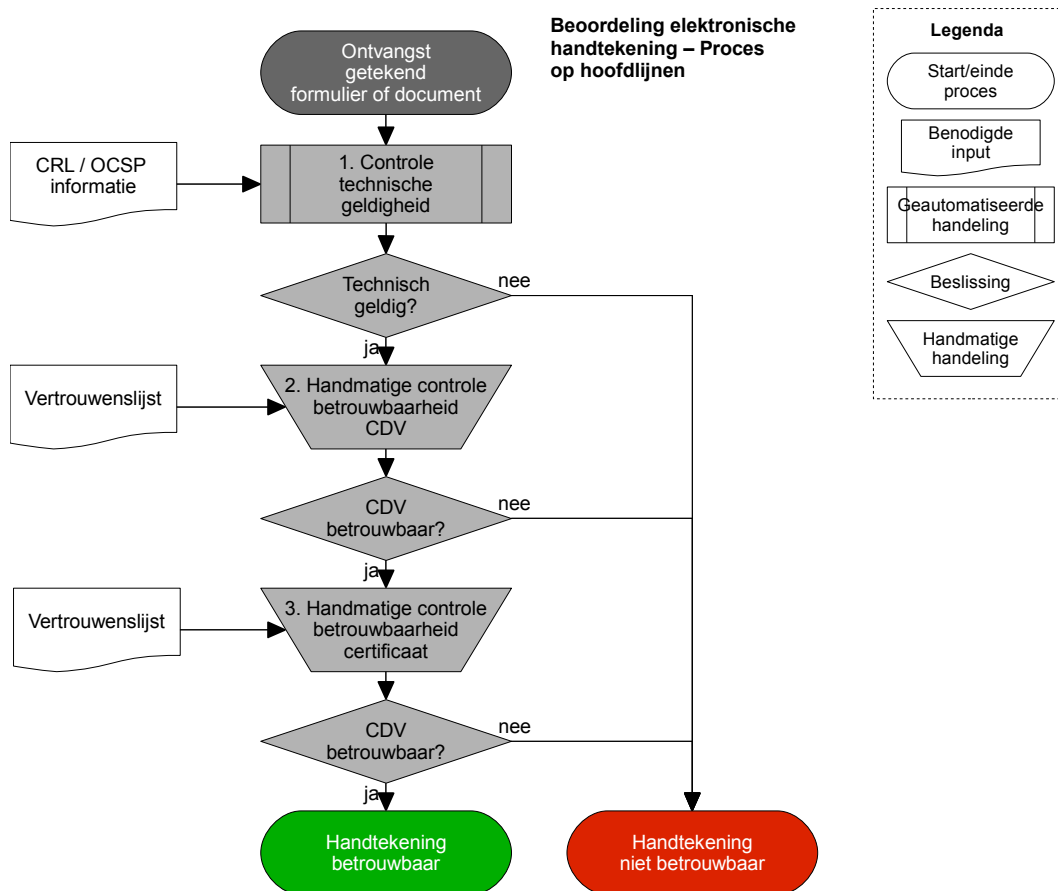
- <http://www.diginotar.nl/klantenservice/certificaten/valideren.aspx>
- <http://www.de-electronische-signatuur.nl/cms/nl/handtekening-controleren.html>
- <http://www.pinkroccadecsp.nl/website/421/Certificaat/Geldigheid%20certificaten%20controleren.html>
- <http://www.quovadisglobal.nl/Repository/DownloadRootsAndCRL.aspx>

Met de hiervoor genoemde handelingen is de technische geldigheid van de handtekening en het daartoe gebruikte certificaat vastgesteld. Vervolgens dienen de volgende, vooralsnog handmatig uit te voeren, handelingen uitgevoerd te worden:

1. controle van de betrouwbaarheid van de CDV;
2. controle van de betrouwbaarheid van het certificaat.

Dit proces op hoofdlijnen is weergegeven in Afbeelding 1. De processtappen 2 en 3 worden uitgewerkt in separate afbeeldingen in hoofdstuk 5.

In alle gevallen geldt dat als u twijfelt over de betrouwbaarheid van de gebruikte elektronische handtekening of technische problemen ondervindt met de beoordeling van elektronische handtekeningen, raadpleeg dan de leidinggevende of de beveiligingsmanager. De voorliggende handreiking is tevens voor hen bedoeld. Daarnaast zijn er specifieke op deze doelgroepen gerichte handreikingen beschikbaar op de website van PKIoverheid, zie ref. [5]. Zij kunnen waar nodig de ICT-afdeling inschakelen.



Afbeelding 1: Hoofdproces Beoordelen betrouwbaarheid elektronische handtekening

4.2 Handmatige processtappen

Deze paragraaf geeft de hoofdlijnen van de uit te voeren stappen voor de twee handmatige controles.

4.2.1 Betrouwbaarheid van de CDV

De betrouwbaarheid van de CDV wordt als volgt vastgesteld (nader gedetailleerd en grafisch weergegeven in hoofdstuk 5):

1. uit het certificaat destilleren van de CDV-dienst waarmee het certificaat is uitgegeven;
2. op het internet de Vertrouwenslijst van de Europese Commissie opzoeken;
3. in de Vertrouwenslijst de verwijzing naar de Vertrouwenslijst van de EU-lidstaat opzoeken waar de uitgevende CDV is gevestigd;
4. in de Vertrouwenslijst van de lidstaat de betreffende CDV-dienst opzoeken en nagaan of deze dienst op de lijst aanwezig is en een actieve status heeft.

Indien deze acties leiden tot een positief resultaat mag geconcludeerd worden dat de handtekening is gezet met een betrouwbaar middel dat door een betrouwbare CDV is uitgegeven.

4.2.2 Betrouwbaarheid van de handtekening

Met de controles uit de voorgaande subparagraaf is duidelijk geworden dat de handtekening tenminste de status geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat of de status gekwalificeerd elektronisch certificaat heeft. De juridische waarde is daarmee hoog, conform ref. [1] en voldoet aan de in de betreffende lidstaat vigerende wetgeving.

Indien additioneel het gebruik van een veilig middel vereist was voor het proces waarin de handtekening is toegepast, is nog een aanvullende controle nodig om het betrouwbaarheidsniveau van de handtekening vast te kunnen stellen. Dit betreft het vaststellen of bij het plaatsen van de handtekening gebruik is gemaakt van een veilig middel (SSCD), aangezien dit het onderscheid is tussen de geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat en de gekwalificeerde elektronische handtekening. Daartoe dienen de volgende acties uitgevoerd te worden (zie hoofdstuk 5 voor een nadere uitwerking van de te nemen stappen):

1. zoek in de Vertrouwenslijst op of bij de betreffende CDV-dienst is aangegeven dat er sprake is van een certificaat op basis van een veilig middel (SSCD);
2. indien in de Vertrouwenslijst niet is aangegeven of het certificaat is gebaseerd op een veilig middel (SSCD) is opgenomen, zijn de volgende stappen nodig:
 1. open de detailgegevens van het gebruikte certificaat;
 2. zoek aan de hand van de gegevens in het certificaat op of het certificaat is uitgegeven op basis van een veilig middel (SSCD);
3. ga na of de naam van de certificaathouder in het certificaat overeenkomt met de naam van de aanvrager in het document of formulier. Daarbij dient rekening gehouden te worden met het gegeven dat, afhankelijk van de notatie in het document of formulier, afwijkingen mogelijk zijn zonder dat sprake mag zijn van het afwijzen van een certificaat. In een certificaat zijn namelijk varianten mogelijk ten aanzien van het hanteren van voorletters, voornamen of een combinatie van beide. Tevens kan in certificaten gekozen zijn voor de geslachtsnaam, zonder of in combinatie met de naam van de partner.


5 Processtappen

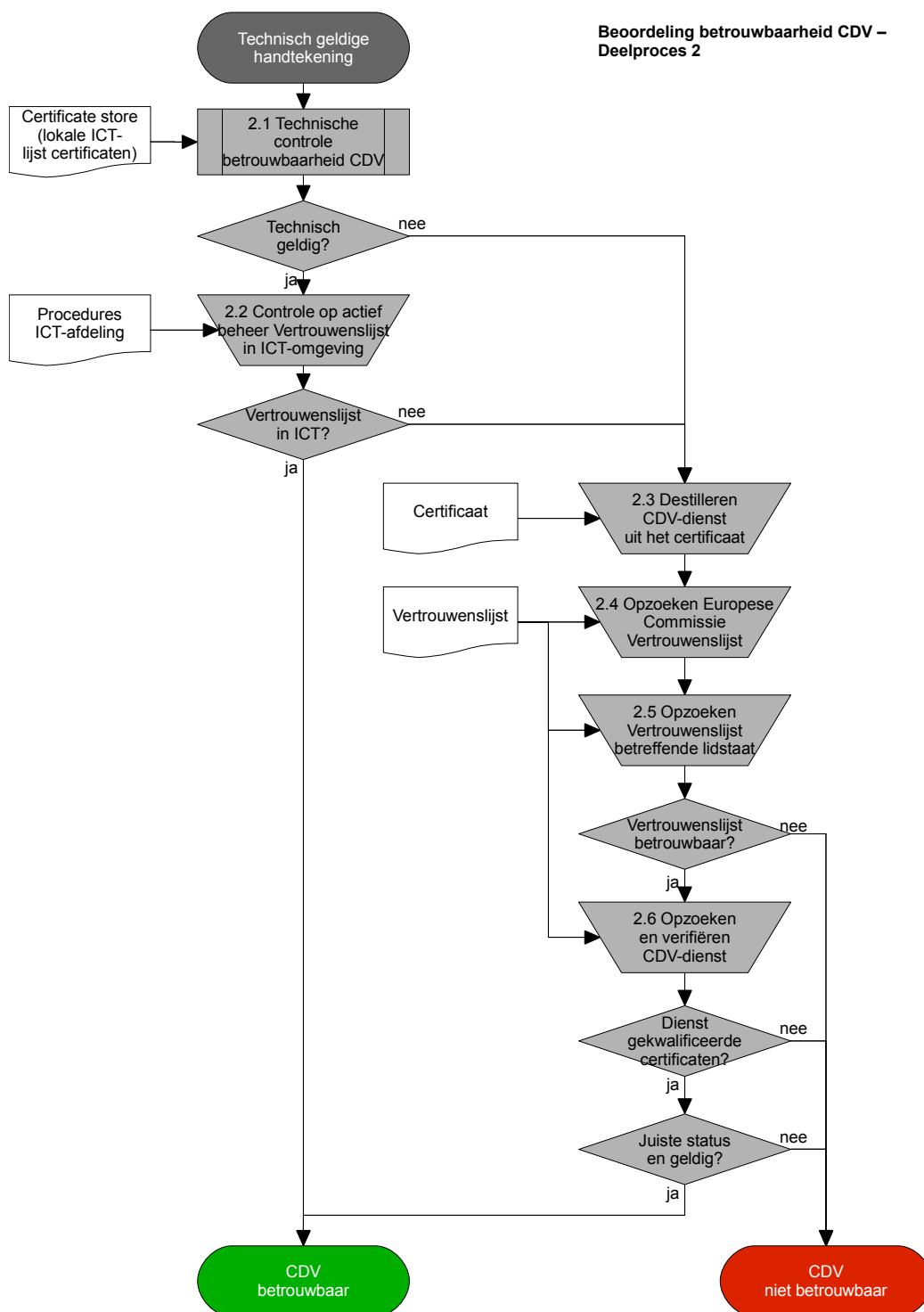
Dit hoofdstuk beschrijft de uitwerking van de handmatige processtappen uit de procesflow zoals benoemd in het voorgaande hoofdstuk. Daarbij geldt als uitgangspunt dat de lijst niet in de ICT-infrastructuur wordt bijgehouden.

5.1 Betrouwbaarheid van de CDV

Deze paragraaf beschrijft in detail de handelingen die uitgevoerd dienen te worden om te beoordelen of er sprake is van een betrouwbare uitgever van gekwalificeerde certificaten. Deze handelingen komen neer op het raadplegen van de Vertrouwenslijst. Afbeelding 2 geeft een grafische weergave van deze stappen.

Daarbij dient opgemerkt te worden dat tijdens de technische controle van een elektronische handtekening door de applicatie de volgende typen resultaten zichtbaar zijn:



1. een groen vinkje (bijvoorbeeld ) of iets van vergelijkbare aard: dit betekent dat de applicatie de elektronische handtekening met succes technisch heeft kunnen controleren. Deze “succesmelding” betekent echter niet dat de betrouwbaarheid van de handtekening volledig is vastgesteld, het betekent dat de technische controle is afgerond. Als vervolgstap dienen alsnog de stappen uit onderstaande paragrafen uitgevoerd te worden;
2. een melding dat het certificaat niet vertrouwd kan worden (bijvoorbeeld aangeduid met een rood kruisje, zoals ). Indien dit betrekking heeft op het niet kunnen vaststellen van de geldigheid van de elektronische handtekening dient u contact op te nemen met uw ICT-afdeling. Als vervolgens blijkt dat er sprake is dat het certificaat van de uitgever niet beschikbaar is, dient dit certificaat alsnog verkregen te worden aan de hand van de informatie in de Vertrouwenslijst. Daarna dient u alsnog de stappen uit te voeren zoals vermeld in de volgende paragrafen.



Afbeelding 2: Detaillering proces Bepalen betrouwbaarheid certificatedienstverlener (uitwerking stap 2 van het hoofdproces)

5.1.1 Destilleren CDV-dienst waarmee het certificaat is uitgegeven

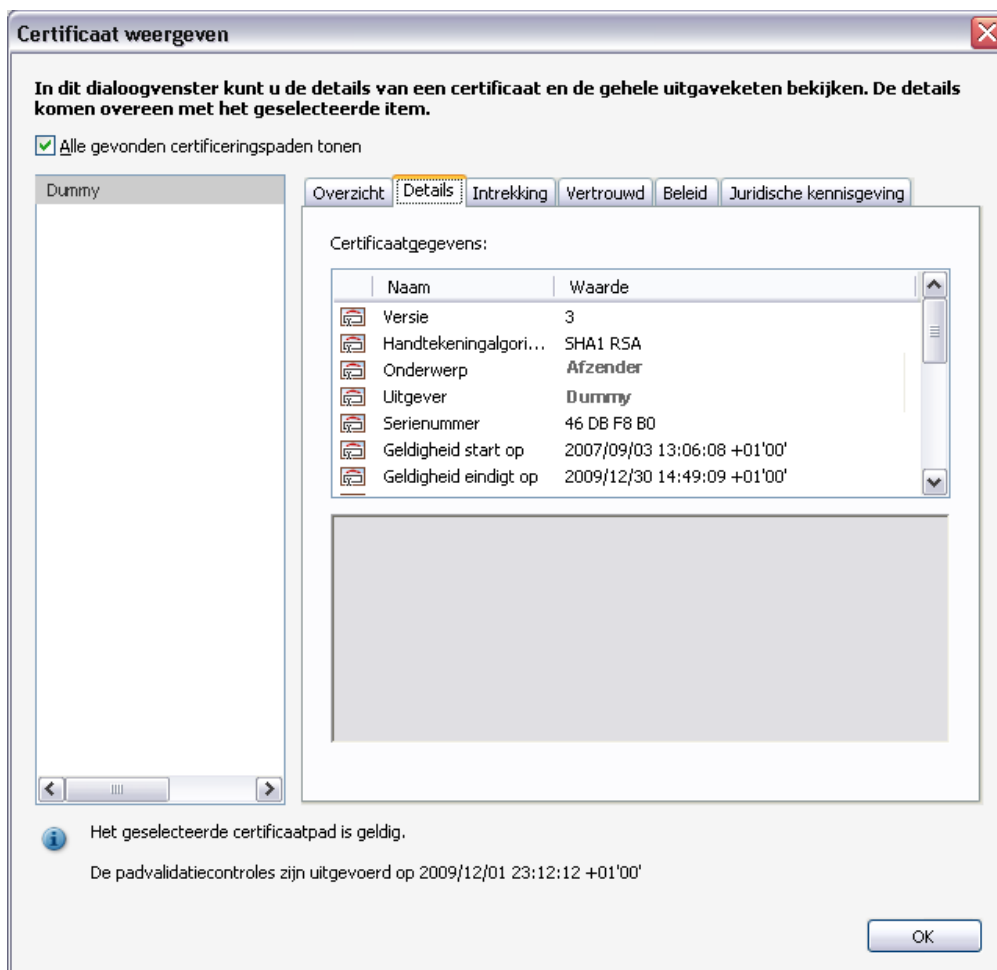
Door het certificaat waarmee het bericht is ondertekend verder te bekijken, kunt u opzoeken wie de uitgevende instantie hiervan is. Daartoe onderneemt u de volgende stappen:

1. Afhankelijk van uw ICT-omgeving en applicatie krijgt u wellicht een melding over de status van de ondertekening of een icoontje, veelal een zegel zoals  of  of (bijvoorbeeld in een PDF-document) een representatie van de handtekening waarin is vermeld dat het document is getekend. In dat geval klikt u op het icoontje of handtekeningrepresentatie en verschijnt een scherm dat er, afhankelijk van uw ICT-omgeving, uitziet zoals in onderstaande weergaven (Microsoft of Adobe);



2. Wederom afhankelijk van uw ICT-omgeving:
 1. vindt u een knopje met een tekst die analoog is aan "Details", "Certificaat bekijken ...", "Certificaat tonen" of "Eigenschappen van handtekening",

- indien nodig om detailgegevens te zien, dient u "Ondertekend door ..." te selecteren gevolgd door "Gegevens bekijken..." of iets van soortgelijke strekking te doen. Er verschijnt een venster met detailgegevens van het certificaat, een scherm dat er uitziet zoals in de twee onderstaande voorbeelden. Hierin is aangegeven wie de **uitgever** is (naast andere gegevens zoals degene die de handtekening gezet heeft).



3. De naam bij de uitgever geeft veelal een afdoende indicatie van de CDV-dienst waarmee het certificaat is uitgegeven. Indien nodig is door het kiezen van het tabblad Certificeringspad (direct zichtbaar of zichtbaar na het klikken op het knopje “Certificaat bekijken”) zien welke diensten in de getoonde hiërarchie nog meer betrokken zijn geweest.
→ **resultaat:** naam van de uitgever (CDV-dienst) en bovenliggende uitgevers.
4. Ga naar de details van het certificaat door te klikken op het knopje “Certificaat bekijken”. In het tabblad vindt u de Uitgever van het certificaat. Als u deze selecteert, worden de detailgegevens getoond. Onder meer staat hier het land van de uitgever aangegeven: achter “C =” wordt de landcode getoond. Deze landcode is nodig om de Vertrouwenslijst van de juiste lidstaat te achterhalen.
→ **resultaat:** lidstaat waarvan de Vertrouwenslijst opgezocht dient te worden.

5.1.2 Opzoeken Vertrouwenslijst van de Europese Commissie

De Europese Commissie publiceert een verzamellijst van verwijzingen naar de Vertrouwenslijst van alle lidstaten. U benadert deze lijst op het internet op:

<http://.....> (nog bekend te stellen door de Europese Commissie)⁴

Zoek hierin de verwijzing naar de benodigde lidstaat, het resultaat uit de vorige stap.

→ **resultaat:** verwijzing naar de benodigde Vertrouwenslijst of (door middel van doorklikken) geopende website of Vertrouwenslijst.

5.1.3 Opzoeken Vertrouwenslijst van de betreffende EU-lidstaat

Indien de voorgaande stap een aan te klikken link heeft opgeleverd, bent u op de site (of in de Vertrouwenslijst) van de betreffende lidstaat terecht gekomen. Indien nog nodig: open de Vertrouwenslijst van de lidstaat.

Indien de voorgaande stap een verwijzing heeft opgeleverd, gebruikt u deze verwijzing als adres in uw internetbrowser. Vervolgens opent u de Vertrouwenslijst van de lidstaat.

Als u de Vertrouwenslijst heeft geopend, verifieert u de volgende gegevens:

1. Controleer aan de hand van het veld **Scheme territory / Gebied van de regeling (clause 5.3.10)** of daadwerkelijk de juiste lidstaat is geselecteerd. In dit veld is de code van de lidstaat opgenomen. Indien dit niet voor zich spreekt, is de codering te vinden in de ISO 3166-1 Alpha-2 standaard (zie http://www.iso.org/iso/english_country_names_and_code_elements).
2. Controleer de betrouwbaarheid van de Vertrouwenslijst zelf:
 1. Indien de lijst is getekend met een elektronische handtekening: controleer of uw applicatie deze handtekening (technisch) geldig verklaart (analoog aan de beschrijving van de beoordeling van de technische geldigheid in het voorgaande hoofdstuk en paragraaf 5.1.1);
 2. Indien de lijst via een beveiligde website ter beschikking wordt gesteld: controleer of er een authentiek certificaat wordt gebruikt voor de verbinding door op het slotje te klikken (veelal te vinden onderin het scherm van de browser of naast de adresbalk in de

⁴Een inleidende tekst over de Vertrouwenslijst, opgesteld door de Europese Commissie, is te vinden op http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_list/index_en.htm. Ook via deze pagina is de Europese Vertrouwenslijst te vinden.



browser). In een scherm wordt aangegeven of het een betrouwbare website is en welke website het betreft;

3. Indien de lijst als beveiligde (maar niet getekende) PDF wordt aangeboden, controleer in de eigenschappen of is aangegeven dat het document beveiligd is.
3. Controleer of de lijst daadwerkelijk CDV's betreft die gekwalificeerde certificaten uitgeven. Daartoe dient in het veld **TSL type / SLV-type (clause 5.3.3)** de waarde *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic* opgenomen te zijn.
4. Controleer aan de hand van de velden **List issue date and time / Publicatiedatum en -uur van de lijst (clause 5.3.14)** en **Next update / Volgende aanpassing (clause 5.3.15)** of de lijst in de tijd geldig is: de actuele tijd dient tussen deze beide tijdstippen te liggen.

Resultaat: de vertrouwenslijst van de betreffende lidstaat betreft de uitgifte van gekwalificeerde certificaten en is betrouwbaar.

5.1.4 Opzoeken en verifiëren CDV-dienst

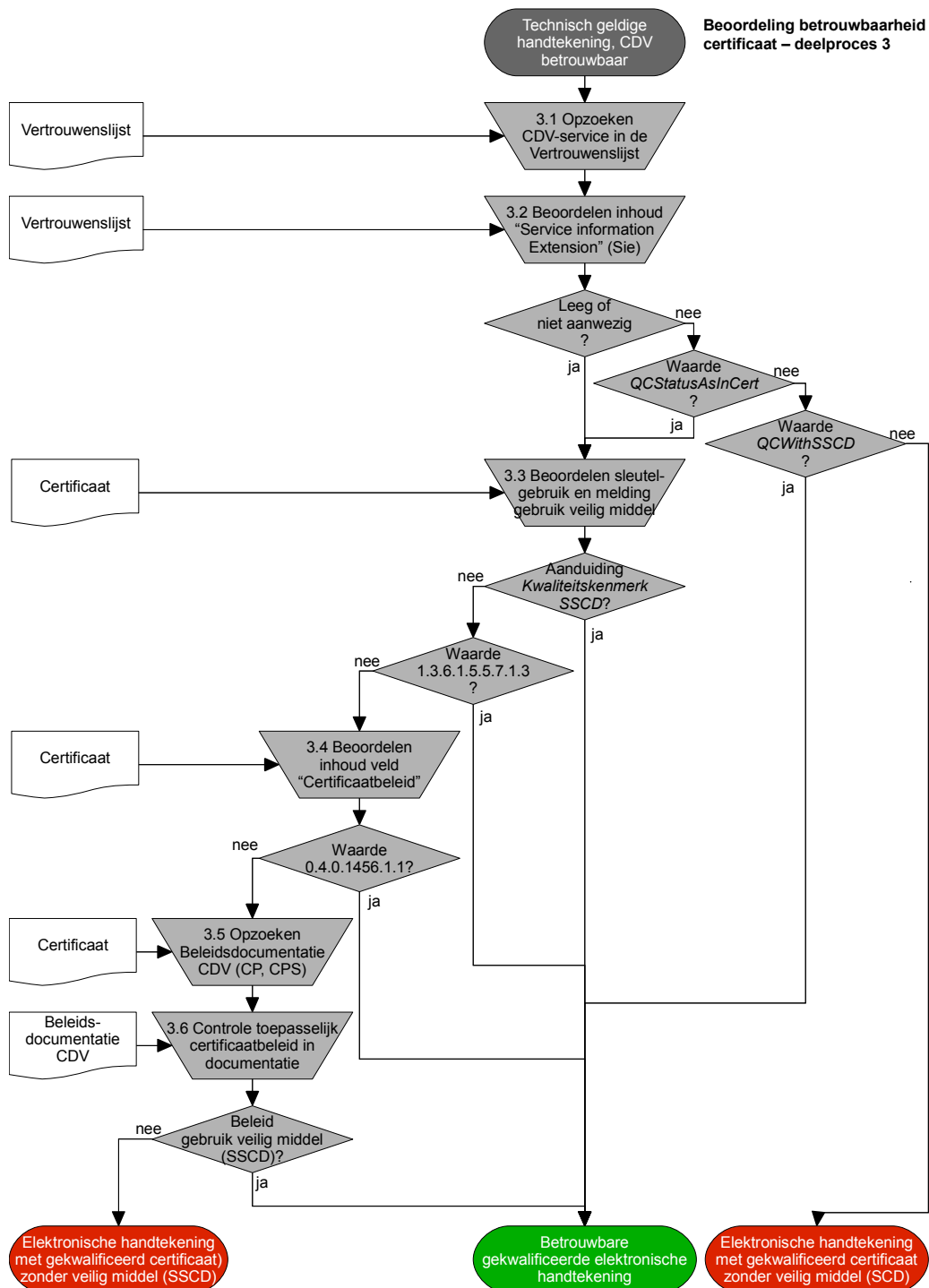
De volgende stappen voorzien in het beoordelen van de relevante CDV-dienst.

1. Zoek in de lijst onder **TSP Information** de juiste CDV-dienst op, gebruik makend van het veld **Service name / Dienstvaam (clause 5.5.2)**. Indien dit veld onvoldoende uitsluitel geeft, kunnen de velden **TSP name / VVD-naam (clause 5.4.1)** of **TSP trade name / VVD-handelsnaam (clause 5.4.2)** als aanvullende informatie gebruikt worden.
2. Het veld **Service type identifier / Identificator diensttype (clause 5.5.1)** dient aan te geven dat het gekwalificeerde certificaten betreft aan de hand van de waarde *http://uri.etsi.org/TrstSvc/Svctype/CA/QC*.
3. Indien de voorgaande test positief uitvalt: het veld **Service current status / Huidige status van de dienst (clause 5.5.4)** geeft aan of de dienst actief is. Daartoe dient de waarde van het veld als volgt te zijn: *Under supervision / onder toezicht, Supervision of Service in Cessation / Toezicht op een aflopende datum* (aanstaande beëindiging van de dienst) of *Accredited / Geaccrediteerd*. Tevens dient het tijdstip van ondertekening van het ontvangen document na de datum- en tijdaanduiding in het veld **Current status starting date and time / Begindatum en -uur van de huidige status (clause 5.5.5)** te liggen.
4. Als deze test positief uitvalt, is sprake van een betrouwbare CDV die gekwalificeerde certificaten uitgeeft. Bij een negatief antwoord op het voorgaande punt, dient u verderop in de lijst te verifiëren of de betreffende dienst in de historische gegevens staat. Ook hier geldt dat de waarde van de **Service previous status / Vorige status van de dienst (clause 5.6.4)** gelijk dient te zijn aan *Under supervision / Onder toezicht, Supervision of Service in Cessation / Toezicht op een aflopende datum* of *Accredited / Geaccrediteerd*. Ook hier dient het tijdstip van ondertekening van het ontvangen document na de datum- en tijdaanduiding in het veld **Current status starting date and time / Huidige begindatum en -uur van de huidige status (clause 5.5.5)** te liggen.

Indien gewenst geven de andere velden nadere informatie over de CDV.

Resultaat: de betreffende dienst levert gekwalificeerde certificaten, uitgegeven door een betrouwbare CDV.

5.2 Betrouwbaarheid van de handtekening



Afbeelding 3: Afbeelding 3: Detaillering proces Beoordelen betrouwbaarheid handtekening (uitwerking stap 3 uit het hoofdproces)

5.2.1 Introductie

Er zijn twee plaatsen waar aangegeven kan zijn dat een certificaat gebruikt wordt in combinatie met een veilig middel (SSCD). Een veilig middel is één van de randvoorwaarden om een handtekening een gekwalificeerde elektronische handtekening te laten zijn. De vereisten die van toepassing zijn voor dit niveau handtekening staan gelijk aan de vereisten voor een juridisch equivalent van een handgeschreven handtekening zoals vastgelegd in de Nederlandse Wet Elektronische handtekeningen en de Europese Richtlijn Elektronische handtekeningen.

Eén plaats waar aangegeven kan zijn dat gebruik wordt gemaakt van een veilig middel is in de Vertrouwenslijst binnen de velden die een TSP service omschrijven. Dit wordt behandeld in paragraaf 5.2.2. Als dit niet wordt vermeld in de Vertrouwenslijst, is het gebruik van een veilig middel aangegeven in het certificaat zelf. In de paragrafen 5.2.3 en 5.2.4 wordt beschreven hoe deze informatie uit het certificaat afgeleid kan worden. De laatste paragraaf gaat nog in op de controle van de juiste tenaamstelling in het certificaat. Afbeelding 3 geeft grafisch de te volgen stappen aan.

5.2.2 Opzoeken gebruik van een SSCD in de Vertrouwenslijst

Indien de informatie over het gebruik van een veilig middel is opgenomen in de Vertrouwenslijst, dan is bij de betreffende CDV-dienst een veld **Service information extensions / Uitbreidingen dienstinformatie (clause 5.5.9)** opgenomen. Als de indicatie over het gebruik van een veilig middel in het certificaat is opgenomen, hoeft het veld **Service information extensions / Uitbreidingen dienstinformatie (clause 5.5.9)** niet aanwezig te zijn. Het ontbreken van dit veld, betekent dan ook dat het certificaat geraadpleegd dient te worden.

Het veld **Service information extensions / Uitbreidingen dienstinformatie (clause 5.5.9)** kan verschillende waarden bevatten (zie ook het volgende hoofdstuk). Als het veld aanwezig is, dan is een voorwaarde voor een gekwalificeerde elektronische handtekening dat het veld de waarde *QCWithSSCD* heeft. De optionele waarde *QCSSCDStatusAsInCert* geeft aan dat de benodigde informatie in het certificaat te vinden is. De optionele waarde *QCForLegalPerson* geeft aan dat het certificaat aan een niet-natuurlijke rechtspersoon (een bedrijf, maar niet een natuurlijke persoon handelend namens dat bedrijf) is uitgegeven conform de wetgeving in de betreffende lidstaat.

5.2.3 Detailgegevens certificaat openen

Indien de Vertrouwenslijst geen uitsluitel geeft over het gebruik van een veilig middel, dient deze informatie uit het certificaat afgeleid te worden. Daartoe dient u de detailgegevens van het certificaat te bekijken (zie de beschrijvingen en afbeeldingen in paragraaf 5.1.1).

1. Afhankelijk van uw ICT-omgeving en applicatie krijgt u wellicht een melding over de status van de ondertekening of een icoontje, veelal een zegel. In het laatste geval klikt u op het icoontje;
2. Wederom afhankelijk van uw ICT-omgeving:
 1. vindt u een knopje met een tekst die analoog is aan “Details”, “Certificaat bekijken ...”, “Certificaat tonen” of “Eigenschappen van handtekening”,
 2. indien nodig om detailgegevens te zien, dient u “Ondertekend door ...” te selecteren gevolgd door “Gegevens bekijken...” of
 3. iets van soortgelijke strekking te doen.



Er verschijnt een venster met detailgegevens van het certificaat. Hierin is aangegeven wie de **uitgever** is (naast andere gegevens zoals degene die de handtekening gezet heeft).

3. Vervolgens dient u de detailgegevens van het certificaat zelf te openen. Ook hier is de exacte wijze van bekijken afhankelijk van uw ICT-omgeving en applicatie. Ga naar de details van het certificaat door te klikken op het knopje "Certificaat bekijken". Ga naar het tabblad Details. Vervolgens zijn er verschillende mogelijkheden waarop aangegeven kan zijn dat er sprake is van het gebruik van een veilig middel. Deze alternatieven worden in de volgende paragraaf toegelicht.

5.2.4 Bepalen sleutelgebruik en gebruik van een SSCD voor de handtekening

Als eerste kan in het certificaat de waarde van het veld **Key usage / Sleutelgebruik** bekeken worden ter bevestiging dat het beoogde gebruik van het certificaat overeenstemt met dat van een gekwalificeerde elektronische handtekening. Als in dit veld de waarde *non-repudiation / onweerlegbaarheid (of niet-afwijzing)* of de waarde *document signing / document ondertekenen* (de exacte waarde kan verschillen per toepassing) is vermeld, is sprake van invulling van één van de voorwaarden voor een gekwalificeerd certificaat. Tevens kan het veld **Verklaringen over kwaliteitscontrole** een bevestiging geven dat het een gekwalificeerd certificaat betreft.

Als u de detailgegevens van het certificaat heeft geopend, zijn één of meer van de volgende attributen van belang voor het beoordelen van het gebruik van een SSCD (afhankelijk van de implementatie die de betreffende CDV gekozen heeft):

1. het attribuut **Verklaringen over kwaliteitscontrole**
2. het separaat attribuut **1.3.6.1.5.5.7.1.3**
3. het attribuut **Certificaat beleid**.

Attribuut Verklaringen over kwaliteitscontrole

Ga na of in de detailgegevens van het certificaat het attribuut **Verklaringen over kwaliteitscontrole** is opgenomen. Indien dit attribuut de waarde **SSCD kwaliteitscontrole** bevat, is sprake van een certificaat dat in combinatie met een veilig middel (SSCD) wordt gebruikt.

Attribuut 1.3.6.1.5.5.7.1.3

Ga na of in de detailgegevens van het certificaat het attribuut **1.3.6.1.5.5.7.1.3** is opgenomen. Deze waarde geeft aan dat er sprake is van een gekwalificeerd certificaat op basis van een veilig middel.

Attribuut Certificaat beleid

Er zijn meerdere alternatieven om aan te geven dat sprake is van het gebruik van een veilig middel:

1. Ga na of het attribuut **Certificaat beleid** de waarde 0.4.0.1456.1.1 bevat. Deze waarde geeft aan dat daadwerkelijk een veilig middel is gebruikt voor de elektronische handtekening.
2. Het attribuut **Certificaat beleid** geeft aan volgens welk specifiek beleid van de CDV het certificaat is uitgegeven. In dit geval bevat het attribuut een waarde bestaande uit een reeks van getallen, gescheiden door een punt die door de CDV wordt gebruikt om het soort certificaat aan te geven. In dit geval zijn de volgende vervolgstappen nodig.
 1. Leg de waarde van het attribuut vast (het getal gescheiden door de punten).

→ **resultaat**: zogenaamde policy OID.

2. Ga naar de website van de betrokken CDV, zoals vermeld in de Vertrouwenslijst bij het veld **TSP Information URI / URI van VVD-informatie (clause 5.4.4)**.
3. Hier zoekt u in de documentatieset Algemene voorwaarden of Certificate Profiles de policy OID op (deze documentatieset bestaat uit tenminste een Certification Practice Statement (CPS) en mogelijk Certificate Policy (CP)).
4. In het document dient u na te gaan of het gebruikte OID in het document is gekoppeld aan certificaten die worden gebruikt in combinatie met een veilig middel (SSCD) en dat het certificaat is bedoeld voor onweerlegbaarheid (non-repudiation of document ondertekenen) c.q. gekwalificeerde elektronische handtekening.
5. Indien het niet duidelijk wordt uit de documentatie (bijvoorbeeld wegens het gebruik van een nationale taal), neem dan contact op met de CDV. Gebruik daartoe de gegevens bij het veld **TSP name / VVD-naam (clause 5.4.1)**.

Resultaat: het is duidelijk of de handtekening is aangemaakt met een veilig middel. Zo ja, dan is sprake van een gekwalificeerde elektronische handtekening.

5.2.5 Nagaan overeenstemming aanvrager en ondertekenaar

In de detailgegevens van het certificaat kunt u zien wie de eigenaar van het certificaat is en daarmee wie het bericht heeft ondertekend. Deze naam moet overeenkomen met de naam van degene die om de dienst vraagt. Daarbij dient rekening gehouden te worden met het gegeven dat, afhankelijk van de notatie in het document of formulier, afwijkingen mogelijk zijn zonder dat sprake mag zijn van het afwijzen van een certificaat. In een certificaat zijn namelijk varianten mogelijk ten aanzien van het hanteren van voorletters, voornamen of een combinatie van beide. Tevens kan in certificaten gekozen zijn voor de geslachtsnaam, al of niet in combinatie met de naam van de partner.

5.3 Aanvullende geautomatiseerde ondersteuning vanuit ICT

Deze paragraaf is primair bedoeld voor managers en ICT-afdelingen. Er worden elementen benoemd die in de ICT-infrastructuur of door de ICT-afdeling doorgevoerd kunnen worden om de beoordeling (deels) geautomatiseerd te ondersteunen.

Het beoordelen van een elektronische handtekening kan voor een gebruiker enigszins vereenvoudigd worden. Dit is voor Nederlandse CDV's beschreven in de PKI-overheid handreiking ICT-deskundigen. In essentie bestaat de vereenvoudiging uit het binnen de ICT-infrastructuur opnemen van het certificaat van de CDV's die vaak gebruikt worden door de buitenlandse partijen die elektronisch getekende aanvragen indienen. Een technische certificaatcontrole zal in dit geval bij normale omstandigheden zonder problemen verlopen.

Twee punten dienen bij een dergelijke vereenvoudiging in het oog gehouden te worden:

1. De geldigheid van de certificaten die in de ICT-infrastructuur zijn opgenomen, dienen geregeld getoetst te worden aan de hand van de Vertrouwenslijst. Dit is in dit geval een handeling die behoort bij het ICT-beheer van de certificaten die in de ICT-infrastructuur zijn opgenomen.

2. De benoemde vereenvoudiging kan ertoe leiden dat de gebruiker minder geneigd is om de Vertrouwenslijst te raadplegen. Deze raadpleging is echter alsnog nodig om de vereiste details te destilleren conform de beschrijving in paragraaf 5.2.

5.4 Wat te doen bij twijfel over de betrouwbaarheid van een elektronische handtekening?

In alle gevallen geldt dat als u twijfelt over de betrouwbaarheid van de gebruikte elektronische handtekening of u technische problemen ondervindt bij het beoordelen van de elektronische handtekening, raadpleeg dan de leidinggevende of de beveiligingsmanager. De voorliggende handreiking is tevens voor hen bedoeld. Daarnaast zijn er specifieke op deze doelgroepen gerichte handreikingen beschikbaar op de website van PKIoverheid, zie ref. [5]. Zij kunnen tevens de ICT-afdeling inschakelen, onder meer indien het noodzakelijk blijkt om aanvullende applicaties in te zetten (op het netwerk of online) om elektronische handtekeningen te beoordelen. Een dergelijke technische complicatie kan aan de orde zijn indien een getekend document wordt ontvangen van een formaat dat niet wordt herkend.

6 Interpretatie Vertrouwenslijst (Trusted List)

Dit hoofdstuk beschrijft de relevante delen van de Vertrouwenslijst zodat deze, relatief complexe, bestanden eenvoudiger gelezen en geïnterpreteerd kunnen worden. De beschrijving is gebaseerd op het interpreteren van de informatie in een als PDF-document gepubliceerde Vertrouwenslijst.

6.1 Introductie

De Vertrouwenslijst bevat verschillende hoofdcomponenten:

1. Identificatie van de Vertrouwenslijst en de beheerder van de Vertrouwenslijst
2. De regels op basis waarvan partijen op de lijst worden opgenomen
3. De wijze van beheer van de Vertrouwenslijst
4. Een overzicht van de partijen die in de betreffende lidstaat gekwalificeerde certificaten uitgeven (zogenaamde Certificatiedienstverleners, CDV of Trust Service Providers, TSP), gespecificeerd naar de verschillende diensten (services) die een CDV levert op het gebied van gekwalificeerde certificaten.

Deze hoofdcomponenten worden in de volgende paragrafen nader toegelicht waarbij alleen de daadwerkelijk relevante onderdelen van de Vertrouwenslijst worden benoemd. Informatie die wel in een Vertrouwenslijst is opgenomen, maar minder relevant is voor de daadwerkelijke interpretatie van de lijst (m.n. technische informatie) hoeven niet in deze handreiking beschreven te worden.

In de onderstaande paragrafen worden de verschillende elementen van de Vertrouwenslijst aangegeven met drie gegevens:

1. de Engelstalige benaming: verwacht mag worden dat de Vertrouwenslijsten van alle lidstaten de Engelse benamingen bevatten;
2. de Nederlandstalige benaming: de Nederlandse lijst zal de Nederlandstalige benaming hanteren, daarnaast zal in enkele gevallen de Nederlandse vertaling eenvoudiger te begrijpen zijn dan de Engelstalige term;
3. een verwijzing naar een clause: dit is een verwijzing naar het nummer van de clause in de technische standaard die van toepassing is op de samenstelling van de Vertrouwenslijst. Deze verwijzing is opgenomen voor eventuele gevallen waarbij de Vertrouwenslijst in een niet beheerste taal is weergegeven, maar de clause nummering kan helpen om de juiste uitleg erbij te vinden.

De namen van elementen die in de Vertrouwenslijst voorkomen zijn in onderstaande tekst vetgedrukt weergegeven om de herkenbaarheid te vergroten. In het geval de waarde van een veld is aangegeven, is dit met cursief gedrukte tekst herkenbaar gemaakt. Indien een waarde van een veld een specifieke waarde dient te hebben, is dit aangegeven met "MOET".

6.2 Identificatie en beheerder Vertrouwenslijst

De identificatie van de Vertrouwenslijst en de gegevens van de beheerder van de Vertrouwenslijst zijn in de Vertrouwenslijst te vinden onder de noemer **Information on the Trusted List Issuing Scheme / Informatie over de afgifteregeling voor Vertrouwenslijsten**.



6.2.1 TSL type / SLV-type (clause 5.3.3)

Het veld **TSL type / SLV-type (clause 5.3.3)** MOET de waarde *http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLtype/generic* bevatten. Daarmee wordt aangegeven dat de lijst betrekking heeft op elektronische handtekeningen in het kader van de Europese Richtlijn Elektronische handtekeningen.

6.2.2 Scheme operator name / Naam uitvoerder van de regeling (clause 5.3.4)

Onder het veld **Scheme operator name / Naam uitvoerder van de regeling (clause 5.3.4)** zijn de contactgegevens te vinden van degene die verantwoordelijk is voor het publiceren en beheren van de Vertrouwenslijst. Deze contactgegevens zijn van belang indien er strikte noodzaak is om contact op te nemen met de beheerder. Dit geldt indien er:

- vermoedelijke problemen zijn met de inhoud van de lijst, in de zin van actualiteit of onjuistheid van de inhoud van de lijst;
- technische problemen zijn met de lijst;
- (bij uitzondering) er twijfel is over de daadwerkelijke betrouwbaarheid van een Trusted Service Provider en de door de CDV ter beschikking gestelde informatie onvoldoende uitsluitsel biedt.

6.3 De regels op basis waarvan partijen op de lijst worden opgenomen

De regels om tot de lijst te mogen toetreden bepalen de betrouwbaarheid van de lijst. Deze regels dienen beschikbaar te zijn voor gebruikers die een elektronische handtekening ontvangen. De hiervoor relevante informatie is eveneens opgenomen onder de kop **Information on the Trusted List Issuing Scheme / Informatie over de afgifteregeling voor Vertrouwenslijsten**.

6.3.1 Scheme information URI / URI met informatie over de regeling (clause 5.3.7)

Onder het veld **Scheme information URI / RI met informatie over de regeling (clause 5.3.7)** zijn de verwijzingen opgenomen naar de regeling met eisen waaraan een Vertrouwensdienstverlener om opgenomen te worden in de Vertrouwenslijst. Op basis van de Europese Richtlijn Elektronische handtekeningen en de beschikking C(2009) 7806 in het kader van de Europese Dienstenrichtlijn geldt dat iedere partij op de lijst beschouwd mag en moet worden als een betrouwbare partij voor de uitgifte van gekwalificeerde certificaten. De regelingen waarnaar verwezen wordt, hebben dan ook primair een informatief karakter.

6.3.2 Status determination approach / Bepaling van de status (clause 5.3.8)

Het veld **Status determination approach / Bepaling van de status (clause 5.3.8)** MOET de waarde *URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate* bevatten. Alleen dan is sprake van een regeling waarbij de betrouwbaarheid van de certificatedienstverleners wordt gegarandeerd door toezicht en mogelijk vrijwillige accreditatie zoals bedoeld in de Richtlijn Elektronische Handtekeningen.



6.3.3 **Scheme territory / Gebied van de regeling (clause 5.3.10)**

Het veld **Scheme territory / Gebied van de regeling (clause 5.3.10)** geeft aan voor welke lidstaat de Vertrouwenslijst van toepassing is. De in de lijst opgenomen certificatieinstanties treden dan ook toe volgens de afspraken die gelden in de betreffende lidstaat.

6.3.4 **TSL policy/legal notice / SLV-beleid/juridische informatie (clause 5.3.11)**

Het veld **TSL policy/legal notice / SLV-beleid/juridische informatie (clause 5.3.11)** geeft de juridische waarde van de Vertrouwenslijst aan.

6.4 **Beheer van de Vertrouwenslijst**

Het beheer van de Vertrouwenslijst betreft de wijze waarop de informatie in de lijst wordt beheerd. Met name de geldigheid en periode van historische gegevens zijn relevante begrippen in dit deel van de lijst. De onderwerpen zijn in de lijst te vinden onder de noemer **Information on the Trusted List Issuing Scheme / Informatie over de afgiferegeling voor Vertrouwenslijsten**.

6.4.1 **Historical information period / Periode van historische informatie (clause 5.3.12)**

Het veld **Historical information period / Periode van historische informatie (clause 5.3.12)** geeft aan hoe lang historische gegevens over certificatieinstanties onderdeel blijven van de Vertrouwenslijst (tenminste 10 jaar). Gegevens uit eerdere perioden zijn niet meer af te leiden uit de Vertrouwenslijst.

6.4.2 **Pointers to other TSL's / Verwijzingen naar andere SLV's (clause 5.3.13)**

Het veld **Pointers to other TSL's / Verwijzingen naar andere SLV's (clause 5.3.13)** verwijst naar de lijst van de Europese Commissie. Deze lijst bevat verwijzingen naar alle Vertrouwenslijsten binnen de Europese Unie en kan daarmee als ingang gebruikt worden om te zoeken naar de Vertrouwenslijst van een specifiek land.

6.4.3 **List issue date and time en next update / Publicatiedatum en -uur van de lijst en volgende aanpassing (clause 5.3.14 en 5.3.15)**

De velden **List issue date and time** en **next update / Publicatiedatum en -uur van de lijst en volgende aanpassing (clause 5.3.14 en 5.3.15)** bevatten de datum en tijd van uitgifte van de voorliggende Vertrouwenslijst en de datum en tijd van de eerstvolgende nieuwe versie van de Vertrouwenslijst. Het is van belang te allen tijde uit te gaan van de nieuwste versie van de Vertrouwenslijst. Deze versie zal dan ook altijd een **Next Update** datum en tijd hebben die later in de tijd ligt dan het actuele tijdstip, anders zou de lijst immers niet meer geldig zijn. De in de Vertrouwenslijst opgenomen tijd ten opzichte van de tijd in Nederland is 1 uur (in de zomertijd) of 2 uur (in de wintertijd) vroeger.



6.5 Overzicht van partijen die gekwalificeerde certificaten uitgeven

6.5.1 Introductie

De kern van de Vertrouwenslijst is het gedeelte waar daadwerkelijk de informatie van de verleners van vertrouwensdiensten (VVD, in het Engels TSP) zelf is opgenomen. In de lijst is per VVD een groep gegevens opgenomen. Ook deze informatie valt, per VVD, uiteen in verschillende categorieën:

1. Contactgegevens van de VVD;
2. Beleid en voorwaarden van de VVD;
3. VVD diensten (TSP services): dit zijn één of meerdere diensten van de VVD waarmee gekwalificeerde certificaten worden uitgegeven, per dienst uiteen vallend in twee delen:
 1. Beschrijving van de actuele geldige dienst;
 2. Historie van betreffende VVD dienst: dit zijn diensten van de VVD die niet meer actief zijn, maar in het verleden wel actief zijn geweest. Naast het stopzetten van een dienst kan ook een wijziging in de dienst tot gevolg hebben dat er historische informatie ontstaat.

6.5.2 Contactgegevens van de VVD

TSP name / VVD-naam (clause 5.4.1)

Dit veld bevat de naam van de rechtspersoon die verantwoordelijk is voor de diensten waarmee gekwalificeerde certificaten worden uitgegeven. NB: dit is niet noodzakelijk de naam die in de certificaten zelf zichtbaar is als de certificaatuitgever, zie ook bij de **TSP services**.

TSP address / VVD-adres (clause 5.4.3)

Dit veld bevat de contactgegevens van de CDV. Deze gegevens kunnen gebruikt worden indien er sprake is van een (vermoedelijk) probleem met een uitgegeven certificaat of als er specifieke informatie gewenst wordt die niet uit achterliggende documentatie gehaald kan worden. Een voorbeeld van een dergelijke situatie is de wens om meer te weten over het uitgifteproces van certificaten. Binnen de bestaande regels is het mogelijk dat de op het internet gepubliceerde informatie over het uitgifteproces uitsluitend in de nationale taal beschikbaar is. Het is voor de hand liggend om aan te nemen dat niet iedere taal die binnen de EU wordt erkend, beheerst wordt door de ontvangers van elektronische handtekeningen. In dit geval biedt de documentatie geen nadere informatie en dient terug gevallen te worden op andere wijzen van contact.

Opmerking hierbij, is dat elektronische handtekeningen (gebaseerd op een gekwalificeerd certificaat en eventueel een veilig middel) in principe niet geweigerd mogen worden. Binnen de EU geldt feitelijk dat partijen die door een nationale toezichthouder van een lidstaat zijn toegelaten op de Vertrouwenslijst, geaccepteerd dienen te worden.

6.5.3 Beleid en voorwaarden van de VVD

TSP information URI / URI van VVD-informatie (clause 5.4.4)

Dit veld bevat de verwijzing naar de plaats (URI) waar informatie gevonden kan worden over de details en de voorwaarden van de VVD bij uitgifte van certificaten. Dit betreft veelal een verwijzing naar documenten genaamd Certificate Policy, Certification Practice Statement, Algemene Voorwaarden of namen van gelijke strekking. Aan de hand van deze documentatie kan de betrouwbaarheid van uitgegeven certificaten vastgesteld worden, onder meer aan de hand van:

1. De juridische voorwaarden waaronder certificaten worden uitgegeven: aansprakelijkheid, garanties, verantwoordelijkheid, etc.
2. De typen certificaten die worden uitgegeven (al of niet gekwalificeerd, het beoogde gebruik van een certificaat: elektronische handtekening, doelgroep, etc.). Zo zal een CP- of CPS-document een nummer (Object Identifier, OID) dienen te bevatten dat het type certificaat aangeeft. Het beschreven stappenplan geeft aan wanneer deze documentatie en de OID-specificatie daarin geraadpleegd moet worden. Zo is in Nederland, in het stelsel van PKI-overheid, bijvoorbeeld de waarde 2.16.528.1.1003.1.2.5.2 de OID voor certificaten voor elektronische handtekeningen voor organisaties.
3. Het proces dat wordt gevolgd voor het aanvragen en uitgeven van certificaten, met name de wijze van vaststelling van de identiteit van de persoon aan wie een certificaat wordt uitgegeven (bijvoorbeeld al dan niet door middel van fysieke verschijning van de betrokkene die het certificaat gaat gebruiken).
4. Of er sprake is van certificaten die op naam van een pseudoniem worden uitgegeven.

Opname van een VVD op de Vertrouwenslijst van een lidstaat betekent dat deze VVD betrouwbaar is volgens de nationale wetgeving. Op basis van de gemaakte afspraken binnen Europa geldt dat andere lidstaten daarmee de VVD eveneens als afdoende betrouwbaar dienen te beschouwen. Slechts in het geval dat er sprake is van een vermoeden dat er ernstige en aantoonbare twijfel is ten aanzien van de betrouwbaarheid, kunnen verdere stappen ondernomen worden. Welke stappen dat zijn, is afhankelijk van de betreffende situatie en uw juridische afweging. Daarbij dient u rekening te houden met verschillen tussen de wetgeving in de verschillende lidstaten.

6.5.4 TSP list of services / VVD-dienstenlijst

De velden in deze paragraaf zijn per VVD per dienst opgenomen zijn op de Vertrouwenslijst. Iedere VVD heeft één of meerdere diensten waarmee certificaten worden uitgegeven. Per dienst is er sprake van een vaststaand aantal velden met informatie.

6.5.4.1. Service information / Dienstinformatie actuele dienst

Per dienst zijn tenminste de velden beschreven die in deze paragraaf worden genoemd.

Service type identifier / Identificator diensttype (clause 5.5.1)

Dit veld geeft, voor iedere VVD, het type dienst aan dat de VVD levert. Voor het uitgeven van gekwalificeerde certificaten MOET dit veld de waarde "<http://uri.etsi.org/TrstSvc/Svctype/CA/QC>" hebben.

Daarnaast kan dit veld gebruikt worden om andere typen diensten aan te geven, zoals diensten voor niet-gekwalificeerde certificaten en timestamping (het voorzien van de mogelijkheid om een elektronische handtekening te completeren met een betrouwbare tijdsaansduiding). De in de eerste alinea aangeduide waarde is echter het meest relevant omdat deze aangeeft dat er gekwalificeerde certificaten worden uitgegeven.

Service name / Dienstnaam (clause 5.5.2)

Dit veld geeft, voor iedere VVD, de naam van elke dienst weer waaronder gekwalificeerde certificaten worden uitgegeven. Veelal zal deze naam gelijk zijn aan de naam van de uitgevende instantie die in het certificaat is opgenomen als “issuer”.

Service digital identity / Digitale identiteit van de dienst (clause 5.5.3)

Dit veld bestaat uit een groot aantal subvelden waarvan de meeste leesbare en een enkele niet-leesbare velden bevatten. Hierna worden de relevante velden beschreven.

- **Digital ID:** dit veld kan ofwel een lange reeks van tekens bevatten ofwel de naam van de uitgevende partij in een specifieke notatie. In het geval dat er sprake is van de lange reeks van tekens, dan is dit de weergave van het certificaat dat behoort bij de dienst waarmee gekwalificeerde certificaten worden uitgegeven. Uw ICT-afdeling kan dit certificaat installeren in uw ICT infrastructuur zodat deze automatisch vertrouwd wordt door uw applicaties.
In het alternatief is de naam van de dienst op een specifieke wijze opgenomen, de zogenaamde Distinguished Name (DN). De naam volgens deze notatie is als volgt opgebouwd, gebruik makend van voorbeeldgegevens:
CN = naam Z (Common Name)
O = organisatie X (Organization)
OU = afdeling Y (Organizational Unit)
C = NL (Country = Nederland)
- **Valid from / Geldig vanaf en Valid to / Geldig tot:** deze twee datum-/tijdaanduidingen geven de geldigheidsperiode van de betreffende dienst aan. Indien het moment van plaatsen van een handtekening met een certificaat, uitgegeven door deze dienst, heeft plaatsgevonden buiten deze geldigheidsperiode dan is de handtekening niet betrouwbaar.
- **Subject / Onderwerp:** de naam van de betreffende dienst (uitgever). In praktische implementaties is het mogelijk dat ofwel het veld **Subject / Onderwerp** is opgenomen ofwel de Digital ID.
- **Thumbprint / Duimafdruk:** een reeks van letters en cijfers die uniek zijn voor het certificaat van de betreffende dienst. Bij een controle van een handtekening kan ook het certificaat van de uitgever (de dienst) worden bekeken. De duimafdruk van het certificaat kan dan vergeleken worden met de waarde die op de Vertrouwenslijst is opgenomen. Deze dienen overeen te komen.

Service current status / Huidige status van de dienst (clause 5.5.4)

Dit veld geeft aan op welke wijze de betrouwbaarheid van een dienst is vastgesteld: *onder toezicht (supervision)* en/of *geaccrediteerd (accredited)*.

- *Under supervision / Onder toezicht* wil zeggen dat de CDV zich heeft gemeld bij de toezichthouder (supervisory body) als een partij die gekwalificeerde certificaten uitgeeft. De toezichthouder plaatst de CDV vervolgens op de Vertrouwenslijst. De procedure waarlangs dit gebeurt, is opgenomen op de plaats waarnaar wordt verwezen in de “**Scheme information URI / URI met informatie over de regeling**” (zie paragraaf 6.3. Deze procedure beschrijft dan ook hoe betrouwbaar dit proces is. Hierover zijn geen vastomlijnde afspraken over binnen de Europese Unie. Elke lidstaat is verplicht tot het geregeld hebben van toezicht.

- *Accredited / Geaccrediteerd* wil zeggen dat de CDV zich heeft onderworpen aan een accreditatie: een toets door een onafhankelijke derde partij of er wordt voldaan aan de vereisten uit de Richtlijn elektronische handtekening of onderliggende standaarden. Accreditatie is op vrijwillige basis.

Additioneel biedt dit veld nadere detaillering bij de statussen *under supervision / onder toezicht* of *accredited / geaccrediteerd*. Dit betreft de aanduiding of de status actief (*under supervision / onder toezicht* of *accredited / geaccrediteerd*), *ceased / stopgezet* of *revoked / ingetrokken* is, dan wel *supervision in cessation / toezicht op een aflopende datum* is.

Bij de controle van de Vertrouwenslijst is het van belang dat de status ten tijde van het geplaatst zijn van de handtekening gelijk is aan *under supervision / onder toezicht*, *accredited / geaccrediteerd* of *supervision in cessation / toezicht op een aflopende datum*. Alleen dan is de betrouwbaarheid van de dienst van de VVD gewaarborgd.

Current status starting date and time / Begindatum en -uur van de huidige status (clause 5.5.5)

Dit veld geeft aan vanaf wanneer de aangegeven status is ingegaan. De in de Vertrouwenslijst opgenomen tijd ten opzichte van de tijd in Nederland is 1 uur (in de zomertijd) of 2 uur (in de wintertijd) vroeger

Service information extensions / Uitbreidingen dienstinformatie (clause 5.5.9)

Dit veld is uitsluitend aanwezig indien het niet eenduidig uit het certificaat zelf is af te leiden of het certificaat in combinatie met een veilig middel (VMAH of SSCD) is uitgegeven. Met andere woorden, indien uit het certificaat niet is af te leiden of een handtekening het predicaat gekwalificeerd of geavanceerd op basis van een gekwalificeerd certificaat verdient. Het verschil tussen beide handtekeningen wordt immers bepaald door het gebruik van een veilig middel.

Als het veld aanwezig is, hebben de waarden de volgende betekenis:

- *QCWithSSCD*: het certificaat is uitgegeven in combinatie met een veilig middel en is daarmee geschikt voor het plaatsen van een gekwalificeerde elektronische handtekening. De handtekening die gecontroleerd wordt, staat, mits geldig, daarmee gelijk aan een handgeschreven handtekening.
- *QCNoSSCD*: het certificaat is uitgegeven zonder combinatie met een veilig middel en is daarmee geschikt voor het plaatsen van een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat. De handtekening dient dan ook, mits geldig, geaccepteerd te worden tenzij vereist wordt dat de handtekening met een veilig middel is aangemaakt.
- *QCSSCDStatusAsInCert*: het certificaat dat behoort bij de handtekening die gecontroleerd wordt, bevat zelf de aanduiding of een certificaat is uitgegeven in combinatie met een veilig middel.
- *QCForLegalPerson*: het certificaat is uitgegeven aan een (niet-natuurlijk) rechtspersoon. Er zal dan ook geen koppeling zijn met een natuurlijk persoon.

Daarnaast kan het veld ook een OID als waarde hebben (zie paragraaf 6.5.3). Deze OID stemt overeen met de aanduiding in de beleidsdocumentatie (Certificate Policy, Certification Practise

Statement) van de VVD. Uit deze documentatie dient vervolgens afgeleid te worden of er sprake is van certificaten voor een elektronische handtekening (non-repudiation of onweerlegbaarheid).

6.5.4.2. *Historie van een VVD service (TSP Service History)*

Historische gegevens zijn per dienst opgenomen in het deel **Service Approval History / Geschiedenis van de goedkeuring van de dienst**. Dit zijn diensten die in het verleden met de aangegeven status (bijvoorbeeld *under supervision*) bestonden, maar zijn vervallen of zijn vervangen door een nieuwe (status van) een dienst. Elke wijziging in de beschrijving van een dienst leidt tot een nieuwe groep van historische gegevens bij deze dienst. Daarbij zijn de oude dienstbeschrijvingen opgenomen in aflopende volgorde van het moment van wijziging: de meest recente wijziging staat bovenaan. Historische gegevens worden bewaard voor de duur zoals gespecificeerd in het veld **Historical information period / Periode van historische informatie (clause 5.3.10)** zoals beschreven in paragraaf 6.4.1.

Per historische dienst is er sprake van een vaststaand aantal velden met informatie. Ook in dit geval wordt volstaan met de toelichting bij de meest relevante velden. Daarbij zijn uitsluitend de velden opgenomen die afwijken van de velden die in de lijst met actuele diensten zijn opgenomen. De betekenis van deze velden is gelijk.

Service previous status / Vorige status van de dienst (clause 5.6.4)

Dit veld geeft aan op welke wijze de betrouwbaarheid van een historische dienst is vastgesteld: onder toezicht (supervision) en/of geaccrediteerd (accredited).

- *Under supervision / Onder toezicht* wil zeggen dat de CDV zich heeft gemeld bij de toezichthouder (supervisory body) als een partij die gekwalificeerde certificaten uitgeeft. De toezichthouder plaatst de CDV vervolgens op de Vertrouwenslijst. De procedure waarlangs dit gebeurt, is opgenomen op de plaats waarnaar wordt verwezen in de "**Scheme information URI / URI met informatie over de regeling**" (zie paragraaf 6.3. Deze procedure beschrijft dan ook hoe betrouwbaar dit proces is. Hierover zijn geen vastomlijnde afspraken over binnen de Europese Unie. Elke lidstaat is verplicht tot het geregeld hebben van toezicht.
- *Accredited / Geaccrediteerd* wil zeggen dat de CDV zich heeft onderworpen aan een accreditatie: een toets door een onafhankelijke derde partij of er wordt voldaan aan de vereisten uit de Richtlijn elektronische handtekening of onderliggende standaarden. Accreditatie is op vrijwillige basis.

Additioneel biedt dit veld nadere detaillering bij de statussen *under supervision / onder toezicht* of *accredited / geaccrediteerd*. Dit betreft de aanduiding of de status actief (*under supervision / onder toezicht* of *accredited / geaccrediteerd*), *ceased / stopgezet* of *revoked / ingetrokken*, dan wel *supervision in cessation / toezicht op een aflopende datum* is.

Previous status starting date and time / Begindatum en -uur van de vorige status (clause 5.6.5)

Dit veld geeft aan vanaf wanneer de aangegeven historische status is ingegaan. De in de Vertrouwenslijst opgenomen tijd ten opzichte van de tijd in Nederland is 1 uur (in de zomertijd) of 2 uur (in de wintertijd) vroeger.

Bijlage 1 Definities

Deze bijlage dient gezien te worden als aanvulling op de definities zoals te vinden op <http://www.pkioverheid.nl> (ref. [5]).

Term	Acroniem	Definitie
Certificatiedienst-verlener	CDV	Zoals bepaald in artikel 2, lid 11, van Richtlijn 1999/93/EG (EN: CSP)
Certificatieautoriteit	CA	Een CA is een CDV die verschillende technische privéondertekensleutels van CA's kan gebruiken, die elk een bijbehorend certificaat hebben, om eindgebruikerscertificaten af te geven. Een CA is een autoriteit die door een of meer gebruikers in vertrouwen wordt genomen om certificaten aan te maken en toe te wijzen. De certificatieautoriteit mag ook gebruikerssleutels aanmaken [ETSI TS 102 042]. De CA kan worden geïdentificeerd via de identificatie-informatie in het Emittent-veld op het CA-certificaat verbonden met (de certificering van) de openbare sleutel die gelinkt is aan de privéondertekensleutel van de CA en die effectief door de CA wordt gebruikt om gebruikerscertificaten af te geven. Een CA kan verscheidene ondertekensleutels bevatten. Elke CA-ondertekensleutel wordt op unieke wijze geïdentificeerd door een unieke identifier die in het veld Identifier autoriteitsleutel op het CA-certificaat staat.
Certificatieautoriteit die gekwalificeerde certificaten afgeeft	CA/KC	Een CA die voldoet aan de vereisten in bijlage II bij Richtlijn 1999/93/EG en gekwalificeerde certificaten afgeeft die voldoen aan de vereisten in bijlage I bij Richtlijn 1999/93/EG (EN: CA/QC)
Certificaat	–	Zoals bepaald in artikel 2, lid 9, van Richtlijn 1999/93/EG.
Gekwalificeerd certificaat	KC	Zoals bepaald in artikel 2, lid 10, van Richtlijn 1999/93/EG (EN: QC) .
Ondertekenaar	–	Zoals bepaald in artikel 2, lid 3, van Richtlijn 1999/93/EG.
Object Identifier	OID	Een pseudowillekeurig getal dat gebruikt wordt in softwaretoepassingen, en dat verondersteld wordt wereldwijd uniek te zijn.
Toezicht	–	“Toezicht” wordt gebruikt in de betekenis van Richtlijn 1999/93/EG (artikel 3, lid 3). De richtlijn verplicht lidstaten een passend systeem op te richten om toezicht te kunnen houden op de op hun grondgebied gevestigde CDV's die gekwalificeerde certificaten aan het publiek afgeven zodat ervoor wordt gezorgd dat deze richtlijn wordt nageleefd.
Vrijwillige accreditatie	Accreditatie	Zoals bepaald in artikel 2, lid 13, van Richtlijn 1999/93/EG.

Vertrouwenslijst	VL	Wijst op de lijst met de toezicht- of accreditatiestatus van certificatieinstanties van certificatieinstantieverleners die bij de lidstaat in kwestie onder toezicht staan of in deze lidstaat zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG (EN: TL).
Statuslijst van Vertrouwensdiensten	SLV	Vorm van ondertekende lijst die wordt gebruikt als basis voor het verstrekken van statusinformatie over de vertrouwensdienst overeenkomstig de specificaties in ETSI TS 102 231 (EN: TSL).
Vertrouwensdienst	–	Dienst ter bevordering van het vertrouwen en geloof in elektronische transacties (meestal, maar niet noodzakelijk, met het gebruik van cryptografische technieken of met betrekking tot vertrouwelijke gegevens) (ETSI TS 102 231).
Verlener van vertrouwensdiensten	VVD	Instantie die een of meer (elektronische) vertrouwensdiensten uitvoert (deze term kent een ruimere toepassing dan CDV) (EN: TSP)
Token vertrouwensdiensten	TVD	Een fysisch of binair (logisch) object dat wordt verkregen of afgegeven als gevolg van het gebruik van een vertrouwensdienst. Voorbeelden van binaire TVD's zijn certificaten, LIC's, tijdstempeltokens en OCSP-responses (EN: TrST).
Gekwalificeerde elektronische handtekening	KEH	Een AEH die door een gekwalificeerd certificaat wordt ondersteund en die door een VMAH wordt aangemaakt zoals bepaald in artikel 2 van Richtlijn 1999/93/EG (EN: QES)
Geavanceerde elektronische handtekening	AEH	Zoals bepaald in artikel 2, lid 2, van Richtlijn 1999/93/EG (EN: AdES).
Geavanceerde elektronische handtekening die door een gekwalificeerd certificaat wordt ondersteund	AEH _{KC}	Impliceert een elektronische handtekening die voldoet aan de vereisten van een AEH en die door een KC wordt ondersteund zoals bepaald in artikel 2 van Richtlijn 1999/93/EG (EN: AdES _{KC})
Veilig middel voor het aanmaken van handtekeningen	VMAH	Zoals bepaald in artikel 2, lid 6, van Richtlijn 1999/93/EG (EN: SSCD).