UITVOERINGSBESLUIT VAN DE COMMISSIE

van 14 oktober 2013

tot wijziging van Beschikking 2009/767/EG wat betreft het opstellen, bijwerken en publiceren van vertrouwenslijsten van certificatiedienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat

(Kennisgeving geschied onder nummer C(2013) 6543)

(Voor de EER relevante tekst)

(2013/662/EU)

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt ([1]), en met name artikel 8, lid 3,

Overwegende hetgeen volgt:

(1) Beschikking 2009/767/EG van de Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het één-loket in het kader van Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt ([2]) verplicht lidstaten ertoe om de informatie beschikbaar te maken die nodig is voor de validering van geavanceerde elektronische handtekeningen die door een gekwalificeerd certificaat worden ondersteund. Deze informatie moet worden verstrekt door middel van uniforme zogeheten „vertrouwenslijsten" die informatie bevatten over certificatiedienstverleners die overeenkomstig Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen ([3]) gekwalificeerde certificaten afgeven aan het publiek en die onder toezicht staan bij of zijn geaccrediteerd in de lidstaten.

(2) Praktische ervaring met de uitvoering door de lidstaten van Beschikking 2009/767/EG heeft aangetoond dat er bepaalde verbeteringen nodig zijn om de voordelen van vertrouwenslijsten optimaal te kunnen benutten. Bovendien heeft het Europees Instituut voor telecommunicatienormen (ETSI) nieuwe technische specificaties voor vertrouwenslijsten gepubliceerd (TS 119 612) die zijn gebaseerd op de specificaties die thans zijn opgenomen de bijlage bij de beschikking, maar die tegelijkertijd een aantal verbeteringen inhouden van die bestaande specificaties.

(3) Beschikking 2009/767/EG moet daarom worden gewijzigd zodat daarin naar de technische specificaties 119 612 van het ETSI wordt verwezen en de veranderingen worden opgenomen die nodig worden geacht om de toepassing en het gebruik van vertrouwenslijsten te verbeteren en vereenvoudigen.

(4) Teneinde de lidstaten in de gelegenheid te stellen de vereiste technische wijzigingen in hun huidige vertrouwenslijsten aan te brengen, is het passend dat dit besluit met ingang van 1 februari 2014 van toepassing is.

(5) De in dit besluit vervatte maatregelen zijn in overeenstemming met het advies van het Comité dienstenrichtlijn,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

Wijzigingen van Beschikking 2009/767/EG

Beschikking 2009/767/EG wordt als volgt gewijzigd:

1) Artikel 2 wordt als volgt gewijzigd:

a) de leden 1, 2 en 2 bis komen als volgt te luiden:

„1. Elke lidstaat stelt een „vertrouwenslijst" op, werkt deze regelmatig bij en publiceert deze overeenkomstig de technische specificaties in de bijlage. Deze lijst bevat minstens de informatie over de certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek en die onder toezicht staan bij of zijn geaccrediteerd in de lidstaat.

2. De lidstaten stellen een machinaal verwerkbare versie van de vertrouwenslijst op en publiceren deze overeenkomstig de specificaties in de bijlage. Wanneer een lidstaat ervoor kiest een menselijk leesbare versie van zijn vertrouwenslijst te publiceren, voldoet die versie van de vertrouwenslijst aan de specificaties in de bijlage.

2 bis. De lidstaten ondertekenen de machinaal verwerkbare versie van hun vertrouwenslijst elektronisch teneinde de authenticiteit en de integriteit ervan te verzekeren. Wanneer een lidstaat een menselijk leesbare versie van de vertrouwenslijst publiceert, zorgt hij ervoor dat deze versie van de vertrouwenslijst dezelfde gegevens bevat als de machinaal verwerkbare versie en ondertekent hij deze elektronisch met hetzelfde certificaat als voor de machinaal verwerkbare versie is gebruikt.";

([1]) PB L 376 van 27.12.2006, blz. 36.
([2]) PB L 274 van 20.10.2009, blz. 36.
([3]) PB L 13 van 19.1.2000, blz. 12.

b) het volgende lid 2 ter wordt ingevoegd:

„2 ter. De lidstaten zorgen ervoor dat de machinaal verwerkbare versie van hun vertrouwenslijst te allen tijde en onderbroken toegankelijk is op de plaats waar deze is gepubliceerd, tenzij er onderhoudswerkzaamheden moeten worden verricht.";

c) lid 3 wordt vervangen door:

„3. De lidstaten delen de volgende informatie aan de Commissie mede:

a) de instantie of instanties die verantwoordelijk zijn voor het opstellen, bijwerken en publiceren van de machinaal verwerkbare versie van de vertrouwenslijst;

b) de plaats waar de machinaal verwerkbare versie van de vertrouwenslijst wordt gepubliceerd;

c) twee of meer publieke sleutelcertificaten van uitvoerders van de regeling, met niet-gelijklopende geldigheidsperioden van ten minste drie maanden, die overeenkomen met de privésleutels die kunnen worden gebruikt om de machinaal verwerkbare versie van de vertrouwenslijst elektronisch te ondertekenen;

d) alle wijzigingen in de onder a), b) en c) bedoelde informatie.";

d) het volgende lid 3 bis wordt ingevoegd:

„3 bis. Wanneer een lidstaat een menselijk leesbare versie van de vertrouwenslijst publiceert, wordt de in lid 3 bedoelde informatie ook met betrekking tot de menselijk leesbare versie meegedeeld.".

2) De bijlage wordt vervangen door de bijlage bij dit besluit.

Artikel 2

Toepassing

Dit besluit is van toepassing met ingang van 1 februari 2014.

Artikel 3

Adressaten

Deze beschikking is gericht tot de lidstaten.

Gedaan te Brussel, 14 oktober 2013.

Voor de Commissie
Michel BARNIER
Lid van de Commissie

BIJLAGE

TECHNISCHE SPECIFICATIES VOOR EEN GEMEENSCHAPPELIJKE TEMPLATE VOOR DE „VERTROUWENSLIJST VAN ONDER TOEZICHT STAANDE OF GEACCREDITEERDE CERTIFICATIEDIENSTVERLENERS"

ALGEMENE VOORSCHRIFTEN

1. **Inleiding**

Met de gemeenschappelijke template voor de „vertrouwenslijst van onder toezicht staande of geaccrediteerde certificatiedienstverleners" wil men een gemeenschappelijke manier aanreiken waarop elke lidstaat informatie kan verstrekken over de toezicht- of accreditatiestatus van de certificatiediensten van certificatiedienstverleners ([1]) (CDV's) die onder toezicht staan bij of zijn geaccrediteerd in de lidstaat voor naleving van de bepalingen van Richtlijn 1999/93/EG. Dit omvat het verstrekken van historische informatie over de toezicht- of accreditatiestatus van de onder toezicht staande of geaccrediteerde certificatiediensten.

Deze informatie is in de eerste plaats bedoeld ter ondersteuning van de validering van gekwalificeerde elektronische handtekeningen (KEH's) en geavanceerde elektronische handtekeningen (AEH's) ([2]) die door een gekwalificeerd certificaat worden ondersteund ([3]) ([4]).

De vertrouwenslijst moet onder andere ten minste informatie bevatten over onder toezicht staande of geaccrediteerde CDV's die gekwalificeerde certificaten (KC's) ([5]) afgeven overeenkomstig de bepalingen van Richtlijn 1999/93/EG (artikel 3, leden 2 en 3, en artikel 7, lid 1, onder a)), zoals, wanneer dit geen deel van de KC's uitmaakt, informatie over KC's die een elektronische handtekening ondersteunen en of de handtekening al dan niet werd aangemaakt door een veilig middel voor het aanmaken van handtekeningen (VMAH) ([6]).

Bijkomende informatie over andere CDV's die geen KC's afgeven, maar diensten verlenen die betrekking hebben op elektronische handtekeningen (bv. CDV's die tijdstempeldiensten verlenen en tijdstempeltokens afgeven, en CDV's die niet-gekwalificeerde certificaten afgeven enz.), kan op vrijwillige basis in de nationale vertrouwenslijst worden opgenomen, mits zij ofwel op gelijke wijze geaccrediteerd zijn of onder toezicht staan als de CDV's die KC's afgeven of krachtens een andere nationale goedkeuringsregeling zijn goedgekeurd. De nationale goedkeuringsregelingen kunnen in sommige lidstaten verschillen van de regelingen inzake toezicht of vrijwillige accreditering die van toepassing zijn op CDV's die KC's afgeven wat betreft de toepasselijke voorschriften en/of de verantwoordelijke organisatie. De woorden „geaccrediteerd" en/of „onder toezicht" in de onderhavige specificaties hebben ook betrekking op nationale goedkeuringsregelingen, maar de lidstaten zullen in hun vertrouwenslijsten bijkomende informatie verstrekken over de aarde van elke nationale regeling, met inbegrip van een toelichting op de mogelijke verschillen met de accreditatie-/toezichtregelingen die worden toegepast op CDV's die KC's afgeven.

De gemeenschappelijke template is gebaseerd op ETSI TS 119 612 v1.1.1 ([7]) (hierna „ETSI TS 119 612" genoemd) dat betrekking heeft op de opstelling, publicatie, lokalisatie, toegang, authenticatie en integriteit van dergelijke lijsten.

2. **Structuur van de gemeenschappelijke template voor de vertrouwenslijst**

De gemeenschappelijke template voor een vertrouwenslijst van een lidstaat bestaat overeenkomstig ETSI TS 119 612 uit de volgende informatiecategorieën:

1. een tag van de vertrouwenslijst waardoor bij elektronische opzoekingen de vertrouwenslijst gemakkelijker kan worden geïdentificeerd;

2. informatie over de vertrouwenslijst en de afgifteregeling;

3. een reeks velden met ondubbelzinnige, identificerende informatie over alle onder toezicht staande of geaccrediteerde CDV's onder de regeling (deze reeks is optioneel, dat wil zeggen wanneer deze niet wordt gebruikt, zal de lijst worden geacht geen inhoud te hebben, wat inhoudt dat in het kader van de vertrouwenslijst geen enkele CDV onder toezicht staat of werd geaccrediteerd in de lidstaat in kwestie);

4. voor elke CDV op de lijst worden de details van zijn specifieke vertrouwensdiensten, waarvan de huidige status in de vertrouwenslijst wordt vermeld, verstrekt in de vorm van een reeks velden waarin ondubbelzinning de onder toezicht staande of geaccrediteerde certificatiediensten van de CDV en hun huidige status worden geïdentificeerd (deze reeks moet minstens één gegeven bevatten);

([1]) Zoals bepaald in artikel 2, lid 11, van Richtlijn 1999/93/EG.
([2]) Zoals bepaald in artikel 2, lid 2, van Richtlijn 1999/93/EG.
([3]) Voor een AEH die door een KC wordt ondersteund, wordt in dit document het acroniem „AEH_{KC}" gebruikt.
([4]) Merk op dat het grensoverschrijdende gebruik van een aantal elektronische diensten die gebaseerd zijn op een gewone AEH, ook kan worden bevorderd indien de ondersteunende certificatiediensten (bv. het afgeven van niet-gekwalificeerde certificaten) deel uitmaken van de onder toezicht staande of geaccrediteerde diensten die als vrijwillige informatie op de vertrouwenslijst van een lidstaat worden opgenomen.
([5]) Zoals bepaald in artikel 2, lid 10, van Richtlijn 1999/93/EG.
([6]) Zoals bepaald in artikel 2, lid 6, van Richtlijn 1999/93/EG.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) — Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. voor elke onder toezicht staande of geaccrediteerde certificatiedienst op de lijst in voorkomend geval de informatie over de geschiedenis van deze status.

6. De op de vertrouwenslijst geplaatste handtekening.

Voor een CDV die KC's afgeeft, maakt de structuur van de vertrouwenslijst en met name de component dienstinformatie (zoals vermeld bij punt 4 hiervoor) bijkomende informatie onder uitbreidingen dienstinformatie mogelijk ter compensatie van die situaties waarin het gekwalificeerde certificaat niet genoeg (machinaal) verwerkbare informatie bevat over zijn kwalificatiestatus en over het al dan niet ondersteund zijn ervan door een VMAH en vooral om het bijkomende probleem aan te pakken dat de meeste (commerciële) CDV's één certificatieautoriteit gebruiken om verschillende soorten eindgebruikerscertificaten, zowel gekwalificeerde als niet-gekwalificeerde, af te geven.

In het kader van diensten voor de afgifte van certificaten (CA-diensten) kan het aantal dienstenartikelen in de lijst voor een CDV worden verminderd wanneer er binnen de PKI van de CDV een of meer hoger geplaatste CA-diensten bestaan (bijvoorbeeld in het kader van een CA-hiërarchie van een root-CA tot verschillende CA's die certificaten afgeven) door dergelijke hoger geplaatste CA-diensten in de lijst op te nemen en niet de CA-diensten voor de afgifte van eindgebruikerscertificaten (bijvoorbeeld het alleen op de lijst opnemen van de root-CA van de CDV. In dergelijke gevallen is de statusinformatie echter van toepassing op de hele hiërarchie van de CA-diensten onder de dienst op de lijst en moet het beginsel dat het ondubbelzinnige verband tussen een certificatiedienst van een CDV_{KC} en de reeks certificaten die als KC's moeten worden geïdentificeerd, gehandhaafd en verzekerd worden.

2.1. *Beschrijving van de informatie in elke categorie*

1. Een tag van de vertrouwenslijst

2. Informatie over de vertrouwenslijst en de afgifteregeling

Onder deze categorie valt de volgende informatie:

— een **identificator van de formaatversie** van de vertrouwenslijst;

— een **volgnummer (of publicatienummer)** van de vertrouwenslijst;

— **type-informatie** over de vertrouwenslijst (bv. om aan te tonen dat deze vertrouwenslijst informatie verschaft over de toezicht- of accreditatiestatus van certificatiediensten van CDV's die bij de lidstaat in kwestie onder toezicht staan of in deze lidstaat zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG);

— informatie over de **uitvoerder (eigenaar) van de regeling** van de vertrouwenslijst (bv. naam, adres, contactinformatie enz. van de instantie van de lidstaat die verantwoordelijk is voor het opstellen, veilig publiceren en bijwerken van de vertrouwenslijst);

— **informatie over de onderliggende toezicht- of accreditatieregeling(en)** waarop de vertrouwenslijst is gebaseerd met inbegrip van maar niet beperkt tot informatie zoals:

  — het land waar de lijst van toepassing is,

  — informatie over of verwijzing naar de plaats waar de informatie over de regeling(en) kan worden gevonden (regelingsmodel, regels, criteria, toepasselijk publiek, type enz.),

  — periode van bijhouden van (historische) informatie;

— **beleid en/of juridische informatie, verplichtingen, verantwoordelijkheden** in het kader van de vertrouwenslijst;

— **publicatiedatum en -uur** van de vertrouwenslijst;

— **de volgende geplande aanpassing** van de vertrouwenslijst.

3. Ondubbelzinnige identificerende informatie over alle onder toezicht staande of geaccrediteerde CDV's onder de regeling

Deze informatie bevat minstens het volgende:

— de organisatienaam van de CDV zoals die gebruikt wordt in formele wettelijke registraties (de gebruikersnaam van de organisatie van de CDV kan ook worden opgegeven als dit in de lidstaat gebruikelijk is);

— het adres en de contactinformatie van de CDV;

— aanvullende informatie over de CDV, ofwel rechtstreeks inbegrepen, ofwel via een verwijzing naar de plaats waarvan deze informatie kan worden gedownload.

4. Voor elke CDV op de lijst een reeks velden met ondubbelzinnige identificerende informatie over een onder toezicht staande of geaccrediteerde certificatiedienst van de CDV in het kader van Richtlijn 1999/93/EG

Deze informatie bevat minstens de volgende informatiecategorieën voor elke certificatiedienst van een CDV op de lijst:

— identificator diensttype: een identificator van het type certificatiedienst (bv. identificator die aangeeft dat de onder toezicht staande of geaccrediteerde certificatiedienst van de CDV een certificatieautoriteit is die KC's afgeeft);

— (handels-) naam van de dienst: (handels-) naam van deze certificatiedienst;

— digitale dienstidentiteit: een ondubbelzinnige, unieke identificator van de certificatiedienst;

— huidige status van de dienst: een identificator van de huidige status van de dienst;

— de begindatum en het begintijdstip van de huidige status;

— uitbreiding dienstinformatie, indien van toepassing: bijkomende informatie over de dienst (bijvoorbeeld rechtstreeks inbegrepen of inbegrepen via een verwijzing naar de plaats waarvan deze informatie kan worden gedownload): door de uitvoerder van de regeling verstrekte informatie over de definitie van de dienst, informatie over toegang tot de dienst, door de CDV verstrekte informatie over de definitie van de dienst en uitbreidingen dienstinformatie. Bijvoorbeeld voor CA/KC-diensten, een optionele reeks informatietupels, waarbij elke tupel de volgende informatie bevat:

  — criteria die kunnen worden gebruikt om onder de geïdentificeerde vertrouwensdienst de exacte reeks dienstproducten (d.w.z. de reeks van gekwalificeerde certificaten) waarvoor bijkomende informatie nodig is of wordt verstrekt over de status ervan, de aanduiding van ondersteuning door een VMAH en/of de afgifte aan een rechtspersoon, verder te identificeren (filteren), alsmede

  — de bijbehorende informatie („qualifiers") of de reeks dienstproducten certificaten identificeert die als gekwalificeerd moeten worden beschouwd en/of over het al dan niet ondersteund zijn van de geïdentificeerde gekwalificeerde certificaten van deze dienst door een VMAH en/of informatie over het al dan niet afgeven van dergelijke KC's aan rechtspersonen (indien dit niet wordt vermeld, wordt verondersteld dat zij aan natuurlijke personen worden afgegeven).

5. Voor elke certificatiedienst op de lijst de historische informatie over de status daarvan

6. Een ten behoeve van authentificatie ten aanzien van alle velden van de VL berekende handtekening met uitzondering van de waarde van handtekening zelf

3. **Richtsnoeren voor het opstellen van gegevens op de vertrouwenslijst**

3.1. *Statusinformatie over onder toezicht staande/geaccrediteerde certificatiediensten en de verleners daarvan in een enkele lijst*

Een vertrouwenslijst van een lidstaat is de „Toezicht- of accreditatiestatuslijst met certificatiediensten van certificatiedienstverleners die bij de lidstaat in kwestie onder toezicht staan of in deze lidstaat zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG".

Een dergelijke vertrouwenslijst is het enige door de betrokken lidstaat te gebruiken instrument voor het verstrekken van informatie over de toezicht- of accreditatiestatus van certificatiediensten en de verleners daarvan:

— **alle certificatiedienstverleners**, zoals bepaald in artikel 2, lid 11, van Richtlijn 1999/93/EG, d.w.z. „een dienst of een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent";

— **die onder toezicht staan of zijn geaccrediteerd** voor naleving van Richtlijn 1999/93/EG.

Op basis van de definities en bepalingen in Richtlijn 1999/93/EG, voornamelijk over de relevante CDV's en hun toezicht-accreditatiesystemen of vrijwilligeaccreditatiesystemen, kunnen CDV's worden onderverdeeld in twee categorieën. De eerste categorie betreft de CDV's die KC's aan het publiek afgeven (CDV_{KC}) en de tweede categorie de CDV's die geen KC's aan het publiek afgeven, maar „andere (ondersteunende) diensten voor elektronische handtekeningen" verlenen:

— **CDV's die KC's afgeven**:

  — zij moeten onder toezicht staan bij de lidstaat waarin zij zijn gevestigd (indien zij in een lidstaat zijn gevestigd) en kunnen ook zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG, waarvan de eisen in bijlage I (eisen voor KC's) en bijlage II (eisen ten aanzien van CDV's die KC's afgeven) deel uitmaken. CDV's die KC's afgeven en die in een lidstaat zijn geaccrediteerd, moeten nog steeds onder het passende toezichtsysteem van die lidstaat vallen tenzij ze niet in die lidstaat zijn gevestigd;

— het toepasselijke „toezichtsysteem" (respectievelijk het „vrijwilligeaccreditatiesysteem") is gedefinieerd en moet voldoen aan de relevante vereisten van Richtlijn 1999/93/EG, in het bijzonder aan de vereisten in artikel 3, lid 3, artikel 8, lid 1, artikel 11, overweging 13 (respectievelijk artikel 2, lid 13, artikel 3, lid 2, artikel 7, lid 1, onder a), artikel 8, lid 1, artikel 11, overwegingen 4 en 11-13);

— **CDV's die geen KC's afgeven**:

— zij kunnen vallen onder een „vrijwilligeaccreditatiesysteem" (zoals bepaald in en overeenkomstig Richtlijn 1999/93/EG) en/of onder een nationaal gedefinieerde „erkende goedkeuringsregeling" die op nationaal niveau werd ingevoerd voor het toezicht op de naleving van de richtlijn en eventueel van nationale bepalingen over het verlenen van certificatiediensten (in de betekenis van artikel 2, lid 11, van Richtlijn 1999/93/EG);

— sommige fysieke of binaire (logische) objecten die werden verkregen of afgegeven bij een certificatiedienst kunnen, op basis van hun overeenkomst met de bepalingen en vereisten op nationaal niveau, een specifieke „kwalificatie" krijgen. De kans is echter groot dat de betekenis van een dergelijke „kwalificatie" slechts op het nationale niveau geldt.

Er mag slechts één vertrouwenslijst per lidstaat worden opgesteld en bijgewerkt om de toezicht- en/of accreditatiestatus aan te geven van de certificatiediensten van de CDV's die onder toezicht staan bij de lidstaat of in deze lidstaat zijn geaccrediteerd. De vertrouwenslijst omvat ten minste die CDV's die KC's afgeven. In de vertrouwenslijst kan ook de status van andere certificatiediensten worden aangegeven die onder een nationaal bepaalde goedkeuringsregeling onder toezicht staan of geaccrediteerd zijn.

3.2. *Eén waardenreeks voor toezicht- en accreditatiestatus*

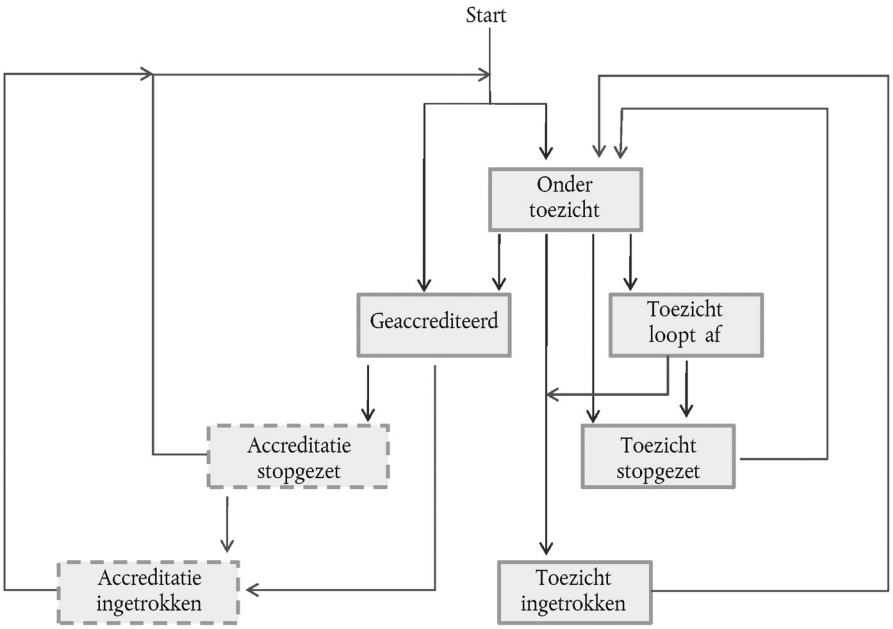
In de vertrouwenslijst geeft de waarde van de huidige status van een dienst aan of deze momenteel „onder toezicht" staat of „geaccrediteerd" is. Bovendien kan een en toezicht- of accreditatiestatus positief zijn („onder toezicht", „geaccrediteerd", „aflopend toezicht"), stopgezet („toezicht stopgezet", „accreditatie stopgezet") of zelfs ingetrokken zijn („toezicht ingetrokken", „accreditatie ingetrokken") en daaraan de daarmee overeenkomende waarde worden toegekend. Eenzelfde certificatiedienst kan tijdens zijn levensduur van een toezichtstatus naar een accreditatiestatus veranderen en omgekeerd ([1]).

Afbeelding 1 hieronder beschrijft voor een enkele certificatiedienst de te verwachten wisselwerkingen tussen de mogelijke toezicht- en accreditatiestatussen:

([1]) Bijvoorbeeld een certificatiedienstverlener die in een lidstaat is gevestigd en die een certificatiedienst verleent die eerst onder toezicht staat bij de lidstaat (toezichthoudende instantie), kan na verloop van tijd beslissen om over te stappen op een vrijwillige accreditatie voor de huidige onder toezicht staande certificatiedienst. Andersom kan een certificatiedienstverlener in een andere lidstaat beslissen om een geaccrediteerde certificatiedienst niet stop te zetten maar om te zetten van een accreditatiestatus naar een toezichtstatus, bv. om bedrijfs- of economische redenen.

Afbeelding 1

Te verwachten wisselwerkingen tussen toezicht- en accreditatiestatus voor één CDV-dienst



Legende:

Overgangsstatus als er een bijbehorend toezichtmodel is (bv. in het geval van een CDV die KC's afgeeft en geaccrediteerd is en onder toezicht staat in de lidstaat waar deze is gevestigd)
Mogelijke huidige status als er geen bijbehorend toezichtmodel is (bv. voor een CDV die geaccrediteerd is in een lidstaat waar deze niet is gevestigd).

Mogelijke huidige status

Een certificatiedienst die KC's afgeeft en in een lidstaat is gevestigd, moet onder toezicht staan (van de lidstaat waar hij gevestigd) en mag vrijwillig geaccrediteerd worden. De statuswaarde van deze dienst moet, indien de dienst is opgenomen in de vertrouwenslijst, een van de hierboven afgebeelde statuswaarden als „huidige statuswaarde" hebben, overeenkomstig zijn huidige status en, in voorkomend geval, veranderen volgens de hierboven afgebeelde statuswisselwerkingen. „Accreditatie stopgezet" en „Accreditatie ingetrokken" zijn echter enkel „overgangstatussen" wanneer de overeenkomstige dienst van de CDV_{KC} is opgenomen in de vertrouwenslijst van de lidstaat waar deze is gevestigde, want een dergelijke dienst moeten automatisch onder toezicht staan (zelfs indien de dienst niet of niet meer geaccrediteerd is); wanneer de overeenkomstige dienst in een andere lidstaat op de lijst staat (is geaccrediteerd) dan de lidstaat waarin hij is gevestigd, kunnen deze waarden definitieve waarden zijn.

Lidstaten die een nationaal gedefinieerde „erkende goedkeuringsregeling" opstellen of hebben opgesteld en op nationaal niveau hebben ingevoerd voor het toezicht op de naleving van Richtlijn 1999/93/EG en van de eventuele nationale bepalingen inzake de verlening van certificatiediensten (in de betekenis van artikel 2, lid 11, van Richtlijn 1999/93/EG) door de diensten van CDV's die **geen** KC's afgeven, moeten dergelijke goedkeuringsregeling(en) onder een van de twee volgende categorieën plaatsen:

— „vrijwillige accreditatie" zoals bepaald en gereguleerd in Richtlijn 1999/93/EG (artikel 2, lid 13, artikel 3, lid 2, artikel 7, lid 1, onder a), artikel 8, lid 1, artikel 11, overwegingen 4 en 11-13);

— „toezicht" zoals opgelegd in Richtlijn 1999/93/EG en ingevoerd door nationale bepalingen en vereisten overeenkomstig de nationale wetgeving.

Zo kan een certificatiedienst die geen KC's afgeeft, onder toezicht worden geplaatst of vrijwillig zijn geaccrediteerd. De statuswaarde van deze dienst moet, indien de dienst is opgenomen in de vertrouwenslijst, een van de hierboven afgebeelde statuswaarden als „huidige statuswaarde" hebben, overeenkomstig zijn actuele status en moet zich, in voorkomend geval, ontwikkelen volgens de hierboven afgebeelde statuswisselwerkingen.

De vertrouwenslijst moet informatie bevatten over de onderliggende toezicht- of accreditatieregeling(en), met name:

— informatie over het toezichtsysteem dat van toepassing is op alle CDV_{KC}'s;

— informatie, indien van toepassing, over de nationale vrijwilligeaccreditatieregeling die van toepassing is op CDV_{KC}'s;

— informatie, indien van toepassing, over het toezichtsysteem dat van toepassing is op CDV's die geen KC's afgeven;

— informatie, indien van toepassing, over de nationale vrijwilligeaccreditatieregeling die van toepassing is op CDV's die geen KC's afgeven.

De laatste twee soorten informatie zijn van doorslaggevend belang voor derden om de kwaliteit en het veiligheidsniveau te beoordelen van dergelijke toezicht- en accreditatiesystemen die op nationaal worden toegepast voor CDV's die geen KC's afgeven. Indien toezicht- of accreditatiestatusinformatie op de vertrouwenslijst staat voor diensten van CDV's die geen KC's afgeven, worden de hiervoor vermelde soorten informatie op de vertrouwenslijst opgenomen via „Scheme information URI" (clausule 5.3.7 — informatie die door lidstaten wordt verstrekt), „Scheme type/community/rules" (clausule 5.3.9 — door het gebruik van een voor alle lidstaten gemeenschappelijke tekst, en eventuele bijkomende specifieke informatie van een lidstaat) en „TSL policy/legal notice" (clausule 5.3.11 — een voor alle lidstaten gemeenschappelijke tekst met verwijzing naar Richtlijn 1999/93/EG, met de mogelijkheid voor elke lidstaat om lidstaatspecifieke tekst/referenties toe te voegen).

Aanvullende informatie over „kwalificatie" op het niveau van nationale toezicht- of accreditatiesystemen voor CDV's die geen KC's afgeven, kan op dienstenniveau worden verstrekt indien dit van toepassing is en wordt vereist (bv. om onderscheid te maken tussen verschillende kwaliteits-/veiligheidsniveaus) via de uitbreiding „additionalServiceInformation Extension" (clausule 5.5.9.4) onder „Service information extensions" (clausule 5.5.9). De gedetailleerde specificaties in hoofdstuk I bevatten meer informatie over de bijbehorende technische specificaties.

Ondanks het feit dat verschillende instanties in een lidstaat verantwoordelijk kunnen zijn voor het toezicht op en de accreditatie van certificatiediensten in die lidstaat, moet elke certificatiedienst naar verwachting slechts één artikel krijgen. Zijn toezicht- of accreditatiestatus moet dienovereenkomstig worden aangepast.

3.3. *Vertrouwenslijstgegevens om de validering van KEH's en AEH_{KC}'s vlotter te doen verlopen*

Bij het samenstellen van de vertrouwenslijst is het verplichte onderdeel van de vertrouwenslijst, namelijk de „Dienstenlijst" per CDV die KC's afgeeft, van doorslaggevend belang. In dat onderdeel wordt immers correcte en exacte informatie gegeven over het afgeven van KC's door een dergelijke certificatiedienst en bevat elk artikel voldoende informatie om de validering te vergemakkelijken van KEH's en AEH_{KC}'s (in combinatie met de inhoud van het eindgebruikers-KC dat door een CDV onder de certificatiedienst die in dit artikel staat, wordt afgegeven).

De vereiste informatie kan andere informatie bevatten dan de „Digitale dienstidentiteit" van een enkele (root-) CA (certificatieautoriteit), zoals informatie over de KC-status van door een dergelijke CA-dienst afgegeven certificaten en of de ondersteunde handtekeningen al dan niet door een VMAH zijn aangemaakt. De instantie in een lidstaat die is aangeduid voor het opstellen, aanpassen en bijwerken van de vertrouwenslijst moet daarom rekening houden met het huidige profiel en de inhoud in elk afgegeven KC per CDV_{KC} die op de vertrouwenslijst staat.

Elk afgegeven KC zou idealiter de KcCompliantie-vermelding van ETSI [1] moeten bevatten indien opgegeven wordt dat het gaat om een KC, en de KcVMAH-vermelding van ETSI indien opgegeven wordt dat het ondersteund wordt door een VMAH voor het genereren van elektronische handtekeningen, en/of dat elk afgegeven KC een van de KCP/KCP+-Objectidentificatoren (OID's) voor certificatiebeleid die worden omschreven in ETSI EN 319 411-2 [2] omvat. Aangezien CDV's die KC's afgeven, verschillende standaarden gebruiken als referentie, deze standaarden op zeer verschillende manieren worden geïnterpreteerd en het niet algemeen bekend is dat er bepaalde normatieve technische specificaties of standaarden bestaan die voorrang hebben, kan de inhoud van de KC's die momenteel worden afgegeven, verschillen (bv. het al dan niet gebruiken van deze KC-vermeldingen van ETSI). Bijgevolg kunnen de ontvangende partijen niet gewoon vertrouwen op het certificaat van de ondertekenaar (en de bijbehorende keten/bijbehorend pad) om, minstens op een machinaal leesbare manier, te oordelen of het certificaat dat een elektronische handtekening ondersteunt, al dan niet een KC is en of de elektronische handtekening al dan niet werd aangemaakt met een VMAH.

[1] Zie ETSI EN 319 412-5 (Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; deel 5: Extension for Qualified Certificate profile) for the definition of such a statement.

[2] ETSI EN 319 411-2 — Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates (beleidseisen voor certificeringsautoriteit die gekwalificeerde certificaten afgeeft).

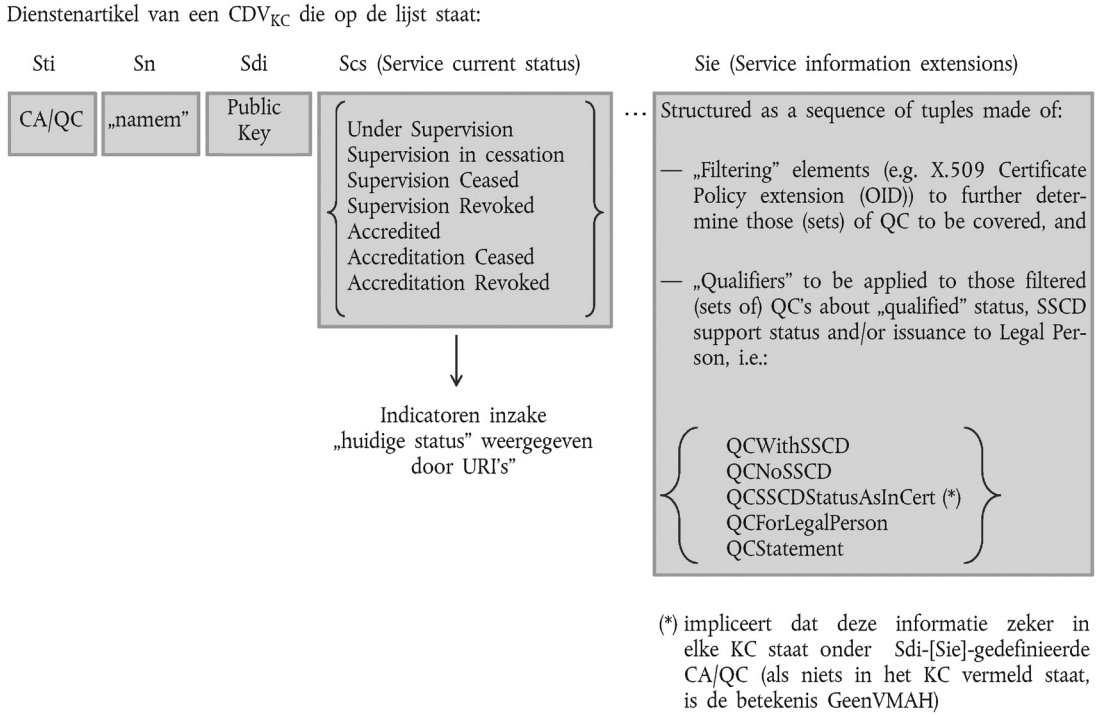
Als de velden „Identificator diensttype" („Idt"), „Dienstnaam" („Dn"), en „Digitale dienstidentiteit" („Ddi") van het dienstenartikel in de vertrouwenslijst worden aangevuld met informatie uit het veld „Uitbreiding dienstinformatie" („Udi"), kan een specifiek type worden vastgesteld van een gekwalificeerd certificaat dat wordt afgegeven door een certificatiedienst van een CDV op de lijst die KC's afgeeft, en wordt informatie verstrekt over het al dan niet ondersteund zijn door een VMAH (indien deze informatie niet wordt vermeld op het afgegeven KC). Specifieke informatie over de „Huidige Dienststatus" („Hds") wordt ook in dit artikel opgenomen. Dit wordt afgebeeld op afbeelding 2 hieronder.

Een dienst op de lijst opnemen door enkel de „Ddi" van een (root-) CA te vermelden impliceert dat (door de CDV die KC's afgeeft, maar ook door de toezichthoudende of accrediterende instantie die instaat voor het toezicht op of de accreditatie van deze CDV) wordt verzekerd dat elk eindgebruikerscertificaat dat onder deze (root-) CA (-hiërarchie) wordt afgegeven, voldoende machinaal verwerkbare ETSI-informatie bevat om te oordelen of het al dan niet om een KC gaat en of het al dan niet is ondersteund door een VMAH. Indien bijvoorbeeld de laatste bewering niet correct is (er is bv. geen gestandaardiseerde, machinaal verwerkbare ETSI-indicatie op het KC over het al dan niet ondersteund zijn door een VMAH), dan wordt door enkel het „Ddi-veld" van die (root-) CA op de lijst te vermelden, slechts verondersteld dat KC's die onder deze (root-) CA-hiërarchie worden afgegeven, niet door een VMAH worden ondersteund. Om aan te duiden dat er vanuit kan worden gegaan dat deze KC's door een VMAH worden ondersteund, moet het „Udi-veld" worden gebruikt (dit wijst er ook op dat de CDV, die KC's afgeeft en onder toezicht staat bij of is geaccrediteerd door respectievelijk de toezichthoudende of accrediterende instantie, deze informatie verzekert).

Afbeelding 2

Dienstenartikel van een CDV die KC's afgeeft en die op de vertrouwenslijst staat

Algemene beginselen – Regels voor het opstellen van CDVKC-artikelen (diensten op de lijst)



De huidige technische specificaties van de gemeenschappelijke template van de vertrouwenslijst laten toe om in het dienstenartikel vijf belangrijke soorten informatie te combineren:

— de „identificator diensttype" („Idt"), die bijvoorbeeld een CA die KC's afgeeft („CA/KC"), identificeert;

— de „Dienstnaam" („Dn");

— de „Digitale dienstidentificator" („Ddi") die een dienst op de lijst identificeert, bv. (minstens) de openbare sleutel van een CA die KC's afgeeft;

— voor CA/KC-diensten, optionele informatie over „Uitbreiding dienstinformatie" („Udi") waardoor een aantal specifieke dienstgerelateerde informatie-elementen kunnen worden opgenomen met betrekking tot de herroepingsstatus van vervallen certificaten, bijkomende kenmerken van KC's, de overname van een CDV door een andere CDV en andere bijkomende dienstinformatie. Bijvoorbeeld de bijkomende kenmerken van KC's worden weergegeven als een opeenvolging van een of meer tupels, waarbij elke tupel de volgende informatie bevat:

  — criteria die kunnen worden gebruikt om onder de in het „Ddi"-veld geïdentificeerde certificatiedienst de exacte reeks van gekwalificeerde certificaten waarvoor bijkomende informatie nodig is of wordt verstrekt over de aanduiding van de „kwalificatiestatus", ondersteuning door een VMAH en/of de afgifte aan een rechtspersoon, verder te identificeren (filteren); alsmede

  — bijbehorende informatie („qualifiers") over het feit of deze reeks van gekwalificeerde certificaten als „gekwalificeerd" moet worden beschouwd en al dan niet ondersteund is door een VMAH, over het feit of deze bijbehorende informatie al dan niet een onderdeel vormt van het KC in een gestandaardiseerde, machinaal verwerkbare vorm, en/of informatie over het feit dat dergelijke KC's aan rechtspersonen worden afgegeven (indien dit niet wordt vermeld, wordt verondersteld dat zij enkel aan natuurlijke personen worden afgegeven);

— informatie over de „huidige situatie" voor dit dienstenartikel met informatie over:

  — het al dan niet onder toezicht staan of geaccrediteerd zijn van de dienst, en

  — de toezicht- of accreditatiestatus zelf.

3.4. *Richtsnoeren over het opstellen en het gebruiken van artikelen over de diensten van CDV_{KC}'s*

De **algemene richtsnoeren voor het opstellen** zijn de volgende:

1. Indien wordt verzekerd (door de CDV die gekwalificeerde certificaten afgeeft en onder toezicht staat bij of is geaccrediteerd door een toezichthoudende of accrediterende instantie) dat, voor een dienst op de lijst die door een „Ddi" wordt geïdentificeerd, alle KC's die door een VMAH worden ondersteund, de KcCompliantie-vermelding van ETSI en de KcVMAH-vermelding en/of de KCP + Objectidentificator (OID) bevatten, dan volstaat het gebruik van een gepaste „Ddi" en kan het „Udi-veld" optioneel worden gebruikt, zonder informatie te hoeven bevatten over de VMAH-ondersteuning.

2. Indien wordt verzekerd (door de CDV die gekwalificeerde certificaten afgeeft en onder toezicht staat bij of is geaccrediteerd door een TI (Toezichtinstantie) of AI (Authorisatie-instantie)) dat, voor een dienst op de lijst die door een „Ddi" wordt geïdentificeerd, alle KC's die niet door een VMAH worden ondersteund, de KcCompliantie-vermelding en/of de KCP OID bevatten, en niet de KcVMAH-vermelding, noch KCP + OID, dan volstaat het gebruik van een gepaste „Ddi" en kan het „Udi-veld" optioneel worden gebruikt, zonder informatie te hoeven bevatten over de ondersteuning van een VMAH (d.w.z. dat het niet door een VMAH wordt ondersteund).

3. Indien wordt verzekerd (door de CDV die gekwalificeerde certificaten afgeeft en onder toezicht staat bij of is geaccrediteerd door een TI of AI) dat, voor een dienst op de lijst die door een „Ddi" wordt geïdentificeerd, alle KC's de KcCompliantie-vermelding bevatten, en sommige van deze KC's worden ondersteund door VMAH's en andere niet (het onderscheid kan worden bepaald bv. door verschillende CDV-specifieke OID's met beleidslijnen over het certificaat of door andere CDV-specifieke informatie op het KC, al dan niet rechtstreeks en machinaal verwerkbaar), maar een certificaat dat wordt ondersteund door een VMAH GEEN KcVMAH-vermelding, NOCH KCP(+) OID van ETSI bevat, dan volstaat mogelijk het gebruik van een passend „Ddi" niet EN moet het „Udi-veld" worden gebruikt om specifieke informatie te geven over de ondersteuning van een VMAH, samen met een eventuele informatie-uitbreiding om de certificatenreeks die hieronder valt, te identificeren. Hiervoor kunnen het best verschillende „informatiewaarden voor VMAH-ondersteuning" voor hetzelfde „Ddi-veld" worden gebruikt bij gebruik van het „Udi-veld".

4. Indien wordt verzekerd (door de CDV die gekwalificeerde certificaten afgeeft en onder toezicht staat bij of is geaccrediteerd door een TI of een AI) dat, voor een dienst op de lijst die door een „Ddi" wordt geïdentificeerd, geen enkele KC een KcCompliantie-vermelding, KCP OID, KcVMAH-vermelding of KCP + OID bevat, maar indien wordt verzekerd dat sommige van deze eindgebruikerscertificaten die onder deze „Ddi" worden afgegeven, KC's zijn en/of worden ondersteund door VMAH's en sommige niet (het onderscheid kan worden bepaald bv. door verschillende CDV_{KC}-specifieke OID's met beleidslijnen over het certificaat of door andere CDV_{KC}-specifieke informatie op het KC, al dan niet rechtstreeks en machinaal verwerkbaar), dan volstaat het gebruik van een passend „Ddi" niet EN moet het „Udi-veld" worden gebruikt voor expliciete informatie over de kwalificatie. Hiervoor kunnen het best verschillende „informatiewaarden voor VMAH-ondersteuning" voor hetzelfde „Ddi-veld" worden gebruikt bij gebruik van het „Udi-veld".

In het algemeen geldt dat voor een CDV die op de vertrouwenslijst staat, één dienstenartikel moet worden aangemaakt per openbare sleutel voor een CA/KC-certificatiedienst (dat wil zeggen per certificatieautoriteit die (rechtstreeks) KC's afgeeft). In bepaalde uitzonderlijke omstandigheden en onder zorgvuldig beheerde voorwaarden, mag de toezichthoudende of accrediterende instelling van een lidstaat beslissen om de privésleutel van een root- of hoger geplaatste CA

binnen de PKI van de CDV (bv. in de context van een CDV-hiërarchie van CA's van een root-CA tot aan verschillende CA's die KC's afgeven) te gebruiken als de „Ddi" van één gegeven op de dienstenlijst van een CDV die op de lijst staat, in plaats van alle ondergeschikte CA-diensten die KC's afgeven op de lijst op te nemen (dit is het opnemen een certificatie-autoriteit die niet rechtstreeks gekwalificeerde eindgebruikerscertificaten afgeeft, maar een hiërarchie van CA's certificeert tot CA's die gekwalificeerde eindgebruikerscertificaten afgeven). De gevolgen (voor- en nadelen) van het gebruik van zo'n openbare sleutel van een root-CA- of hoger geplaatst CA als „Ddi"-waarde in een dienstenartikel op een vertrouwenslijst moeten bij de toepassing daarvan door lidstaten zorgvuldig worden overwogen. Bovendien moeten de lidstaten die deze toegelaten uitzondering op het algemene beginsel gebruiken, de nodige documentatie verstrekken om de opbouw en de controle van de certificatie te vergemakkelijken. Indien bijvoorbeeld een CDV_{KC} een root-CA gebruikt, waaronder meerdere CA's KC's en niet-KC's afgeven, maar waarvoor de KC's enkel de KcCompliantie-vermelding bevatten en geen verwijzing naar een ondersteuning door een VMAH, impliceert het onder „Ddi" vermelden van de root-CA slechts dat, op basis van de hierboven vermelde regels, geen van de KC's die onder deze root-CA worden afgegeven, door een VMAH wordt ondersteund. In geval van KC's die wel door een VMAH worden ondersteund, maar waarbij er in de certificaten geen machinaal verwerkbare vermelding is opgenomen die een dergelijke ondersteuning aangeeft, zou het sterk aanbevolen zijn om de KcVMAH-vermelding te gebruiken voor de KC's die nog zullen worden afgegeven. Intussen (totdat het laatste KC dat deze informatie niet bevat, is vervallen) moet de vertrouwenslijst gebruikmaken van het „Udi-veld" en de bijbehorende „kwalificaties-uitbreiding", bv. door het geven van filterinformatie voor het identificeren van een reeks of reeksen certificaten door het gebruik van specifieke OID('s) voor CDV_{KC} die mogelijk door hen worden gebruikt om verschillende soorten KC's te onderscheiden (die welke door een VMAH worden ondersteund en andere) en door het associëren van expliciete „informatie over de VMAH-ondersteuning" met deze geïdentificeerde (gefilterde) reeks of reeksen certificaten door het gebruik van „Qualifiers".

Dit zijn de **algemene gebruiksaanwijzingen** voor toepassingen, diensten of producten met elektronische handtekening op een vertrouwenslijst in overeenstemming met deze technische specificaties:

Een „CA/KC-Idt-artikel" (evenals een CA/KC-artikel dat verder wordt gekwalificeerd als een „root-CA/KC" via het gebruik van de „Sie"-additionalServiceInformation Extension)

— toont aan dat van de „Ddi"-geïdentificeerde CA (evenals in de CA-hiërarchie vanaf de Ddi-geïdentificeerde root-CA) alle afgegeven eindgebruikerscertificaten KC's zijn **op voorwaarde** dat dit in het certificaat wordt gesteld door het gebruik van passende machinaal verwerkbare KcVermeldingen (dus KcCompliantie) en/of KCP(+) OID's van ETSI (en dit wordt verzekerd door een toezichthoudende/accrediterende instantie, zie hierboven „algemene richtsnoeren voor het opstellen van gegevens").

Opmerking: indien er geen „Kwalificaties-uitbreiding" in „Udi" staat, of indien een eindgebruikerscertificaat waarvan wordt beweerd dat het een KC is, niet verder wordt geïdentificeerd via een bijbehorende „Kwalificaties-uitbreiding" in „Udi", dan staat de machinaal verwerkbare informatie in het KC onder toezicht of wordt deze informatie geaccrediteerd als zijnde correct. Dit impliceert dat het gebruik (of niet) van de passende KcVermeldingen (dus KcCompliantie, KcVMAH) en/of de in ETSI bepaalde KCP(+) OID's zeker in overeenstemming is met wat door de CDV_{KC} wordt beweerd.

— **en INDIEN** „Kwalificaties-uitbreiding"-informatie in „Udi" staat, dan moeten, naast de hierboven vermelde interpretatieregel voor standaardgebruik, de certificaten die geïdentificeerd worden in de „Kwalificaties-uitbreiding"-informatie in „Udi", die wordt opgebouwd door een opeenvolging van „filters" die een reeks certificaten verder identificeert, in aanmerking worden genomen overeenkomstig de bijbehorende „Qualifiers" die bijkomende informatie verstrekken over de kwalificatiestatus, „VMAH-ondersteuning" en/of „Rechtspersoon als onderwerp" (d.w.z. de certificaten die een specifieke OID in de uitbreiding over het certificaatbeleid bevatten, en/of een specifiek patroon voor „Sleutelgebruik" hebben, en/of worden gefilterd door het gebruik van een specifieke waarde om in een specifiek certificaatveld of -uitbreiding te verschijnen enz.). Deze kwalificatie-informatie vormen een onderdeel van de volgende reeks van „Qualifiers" die worden gebruikt om het tekort aan informatie in de overeenkomstige KC-inhoud te compenseren, en die respectievelijk worden gebruikt om:

  — de kwalificatiestatus aan te duiden: „KCvermelding", wat betekent dat het(de) geïdentificeerde certifica(a)t(en) gekwalificeerd zijn,

    EN/OF

  — de aard van de VMAH-ondersteuning aan te duiden:

    — de qualifier „KCmetVMAH" betekent „KC ondersteund door een VMAH", of

    — de qualifier „KCzonderVMAH" betekent „KC niet ondersteund door een VMAH", of

    — de qualifier „KCVMAHStatusZoalsInCert" betekent dat de informatie over VMAH-ondersteuning zeker is opgenomen in het KC onder de Ddi- en Udi-informatie in dit CA/KC-artikel,

    EN/OF

— om de afgifte aan een rechtspersoon aan te duiden:

— de qualifier „KCvoorRechtspersoon" betekent „Certificaat afgegeven aan een rechtspersoon".

3.5. *Diensten die „CA/KC"-diensten ondersteunen, maar niet vallen onder de „Ddi" van „CA/KC"*

Diensten inzake de geldigheidsstatus van een certificaat met betrekking tot KC's waarvoor de informatie over de geldigheidsstatus van het certificaat (bijvoorbeeld LIC's en OCPS-responses) is ondertekend door een entiteit wiens privésleutel niet is gecertificeerd op grond van een certificatiepad dat leidt tot een CA op de lijst die KC's afgeeft („CA/KC"), worden in de vertrouwenslijst opgenomen door deze diensten in verband met de geldigheidsstatus van een certificaat als zodanig in de vertrouwenslijst op te nemen (dat wil zeggen met een dienstype „OCSP/KC" respectievelijk „LIC/KC") aangezien deze diensten beschouwd kunnen worden als een onderdeel van de onder toezicht staande of geaccrediteerde „gekwalificeerde" diensten die betrekking hebben op de verlening van KC-certificatiediensten. Uiteraard moeten OCSP-responders of LIC-emittenten die certificaten afgeven die door CA's worden ondertekend onder de hiërarchie van een CA/KC-dienst die op de lijst staat, als „geldig" worden beschouwd en de statuswaarde krijgen van de CA/KC-dienst die op de lijst staat.

Deze bepalingen kunnen ook van toepassing zijn op certificatiediensten die niet-gekwalificeerde certificaten afgeven (van een diensttype „CA/IOS" (Certificatieautoriteit/Infrastructuur Openbare Sleutel)).

De vertrouwenslijst omvat diensten in verband met de geldigheidsstatus van een certificaat wanneer daarmee verband houdende informatie over de plaats van zulke diensten niet is opgenomen in de eindgebruikerscertificaten waarop deze diensten betrekking hebben.

4. **Definities en afkortingen**

Voor dit document zijn de volgende definities en acroniemen van toepassing:

Term	Acroniem	Definitie
Certificatiedienstverlener	CDV	Zoals bepaald in artikel 2, punt 11, van Richtlijn 1999/93/EG.
Certificatieautoriteit	CA	1. een certificatiedienstverlener die publieke sleutelcertificaten maakt en toewijst, of 2. een technische dienst voor het verkrijgen van certificaten die wordt gebruikt door een certificatiedienstverlener die publieke sleutelcertificaten maakt en toewijst. *OPMERKING*: zie clausule 4 van EN 319 411-2 [1] voor verdere uitleg van het begrip certificatieautoriteit.
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.
Certificaat	Certificaat	Zoals gedefinieerd in artikel 2, punt 9, van Richtlijn 1999/93/EG.
Gekwalificeerd certificaat	KC	Zoals gedefinieerd in artikel 2, punt 10, van Richtlijn 1999/93/EG.
Ondertekenaar	Ondertekenaar	Zoals gedefinieerd in artikel 2, punt 3, van Richtlijn 1999/93/EG.
Toezicht	Toezicht	Verwijst naar toezicht in de zin van artikel 3, punt 3, van Richtlijn 1999/93/EG. Richtlijn 1999/93/EG 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 gedefinieerd in artikel 2, punt 13, van Richtlijn 1999/93/EG.
Vertrouwenslijst	VL	Wijst op de lijst met de toezicht- of accreditatiestatus van certificatiediensten van certificatiedienstverleners die bij de lidstaat in kwestie onder toezicht staan of in deze lidstaat zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG.

Term	Acroniem	Definitie
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 119 612.
Vertrouwensdienst		Dienst ter bevordering van het vertrouwen in elektronische transacties (meestal, maar niet noodzakelijk, met het gebruik van cryptografische technieken of met betrekking tot vertrouwelijke gegevens) (ETSI TS 119 612). *OPMERKING*: deze term kent een ruimere toepassing dan certificatiedienst die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent.
Verlener van vertrouwensdiensten	VVD	Instantie die een of meer (elektronische) vertrouwensdiensten uitvoert (deze term kent een ruimere toepassing dan CDV).
Token vertrouwensdiensten	TVD	Een fysiek of binair (logisch) object dat wordt verkregen of afgegeven als gevolg van het gebruik van een vertrouwensdienst. Voorbeelden van binaire TVD's zijn certificaten, lijsten van ingetrokken certificaten (LIC's), tijdstempeltokens (TST's) en Online Certificate Status Protocol (OCSP) responses.
Gekwalificeerde elektronische handtekening	KEH	Een AEH die door een gekwalificeerd certificaat wordt ondersteund en die door een veilig middel voor het aanmaken van handtekeningen wordt aangemaakt zoals gedefinieerd in artikel 2 van Richtlijn 1999/93/EG.
Geavanceerde elektronische handtekening	AEH	Zoals gedefinieerd in artikel 2, punt 2, van Richtlijn 1999/93/EG.
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 gedefinieerd in artikel 2 van Richtlijn 1999/93/EG.
Veilig middel voor het aanmaken van handtekeningen	VMAH	Zoals gedefinieerd in artikel 2, punt 6, van Richtlijn 1999/93/EG.

([1]) EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates (beleidseisen voor certificeringsautoriteit die gekwalificeerde certificaten afgeeft).

In de volgende hoofdstukken hebben de sleutelwoorden „MOETEN" (MUST), „NIET MOGEN" (MUST NOT), „VERPLICHT" (REQUIRED), „DIENEN TE" (SHALL), „DIENEN NIET TE" (SHALL NOT), „ZOUDEN" (SHOULD), „ZOUDEN NIET" (SHOULD NOT), „AANBEVOLEN" (RECOMMENDED), „KUNNEN" (MAY) en „OPTIONEEL" (OPTIONAL) de betekenis die omschreven is in RFC 2119 ([1]).

HOOFDSTUK I

GEDETAILLEERDE SPECIFICATIES VOOR DE GEMEENSCHAPPELIJKE TEMPLATE VOOR DE VERTROUWENSLIJST VAN ONDER TOEZICHT STAANDE OF GEACCREDITEERDE CERTIFICATIEDIENSTVERLENERS

De onderhavige specificaties zijn gebaseerd op de specificaties en vereisten in ETSI TS 119 612 v1.1.1 (hierna „ETSI TS 119 612" genoemd).

Indien de onderhavige specificaties geen specifieke vereisten stellen, DIENEN de vereisten van clausules 5 en 6 van ETSI TS 119 612 volledig van toepassing te zijn. Indien de onderhavige specificaties specifieke vereisten stellen, DIENEN deze vereisten de overhand te hebben op de overeenkomstige vereisten in ETSI TS 119 612. In het geval van afwijkingen tussen de onderhavige specificaties en de specificaties in ETSI TS 119 612, DIENEN de onderhavige specificaties de norm te zijn.

Scheme operator name (clausule 5.3.4)

Dit veld DIENT te worden gebruikt en DIENT te voldoen aan de specificaties van clausule 5.3.4. van TS 119 612.

([1]) IETF RFC 2119: „Key words for use in RFCs to indicate Requirements Levels".

Een land KAN meerdere toezicht- en accreditatie-instanties hebben en zelfs bijkomende instanties voor alle mogelijke gerelateerde operationele activiteiten. Elke lidstaat moet zelf een Scheme operator aanduiden voor de vertrouwenslijst van de lidstaat. De toezichthoudende instantie, de accrediterende instantie en de uitvoerder van de regeling (als het om verschillende instanties blijkt te gaan) zullen naar verwachting elk hun eigen verantwoordelijkheden en verplichtingen hebben.

Alle situaties waarin verschillende instanties verantwoordelijk zijn voor toezicht, accreditatie of operationele aspecten DIENEN op een consistente manier aldus vermeld en geïdentificeerd te worden in de informatie over de regeling in de vertrouwenslijst, en meer bepaald in de regelingsspecifieke informatie aangeduid door de „Scheme information URI" (clausule 5.3.7).

Scheme name (clausule 5.3.6)

Dit veld DIENT te worden gebruikt en DIENT te voldoen aan de specificaties van clausule 5.3.6. van TS 119 612, waar de volgende naam voor de regeling DIENT te worden gebruikt:

„EN_naam_waarde" = „Toezicht- of accreditatiestatuslijst van certificatiediensten van certificatiedienstverleners die onder toezicht staan bij of zijn geaccrediteerd in de lidstaat in kwestie die de regeling uitvoert voor naleving van Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.".

Scheme information URI (clausule 5.3.7)

Dit veld DIENT te worden gebruikt en DIENT te voldoen aan de specificaties van clausule 5.3.7. van TS 119 612, waar de passende informatie over de regeling minstens het volgende DIENT te bevatten:

— inleidende informatie die voor alle lidstaten gemeenschappelijk is. Deze informatie betreft het toepassingsgebied en de context van de vertrouwenslijst en de onderliggende toezicht- of accreditatieregeling(en). De gemeenschappelijke tekst die moet worden gebruikt, is de onderstaande, waarin de tekenreeks „[*naam van de betrokken lidstaat*]" DIENT te worden vervangen door de naam van de betrokken lidstaat:

„The present list is the „Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 december 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— allowing for a trusted validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including, when this is not part of the QCs, information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable „supervision" system (respectively „voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8.(1), Article 11 (respectively, Article 2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List at a national level on a voluntary basis.";

— specifieke informatie over de onderliggende toezicht- of accreditatieregeling(en), met name ([1]):

  — informatie over het toezichtsysteem dat van toepassing is op alle CDV_{KC}'s,

  — informatie, indien van toepassing, over de nationale vrijwilligeaccreditatieregeling die van toepassing is op alle CDV_{KC}'s,

  — informatie, indien van toepassing, over het toezichtsysteem dat van toepassing is op CDV's die geen KC's afgeven,

  — informatie, indien van toepassing, over de nationale vrijwilligeaccreditatieregeling die van toepassing is op alle CDV's die geen KC's afgeven;

  deze specifieke informatie DIENT voor elke hierboven vermelde onderliggende regeling ten minste de volgende informatie te bevatten:

  — een algemene beschrijving,

  — informatie over de procedure die door de toezichthoudende of accrediterende instantie wordt gevolgd voor toezicht op of accreditatie van CDV's en door de CDV's om onder toezicht te staan of geaccrediteerd te zijn,

  — informatie over de criteria die worden gehanteerd voor het toezicht op of de accreditatie van CDV's;

— sommige fysieke of binaire (logische) objecten die worden verkregen of afgegeven als gevolg van een certificatiedienst, kunnen, indien van toepassing, op basis van hun overeenkomst met de bepalingen en vereisten op nationaal niveau, specifieke informatie krijgen over de specifieke kwalificaties en over de betekenis van dergelijke kwalificatie en de bijhorende nationale bepalingen en vereisten.

Bijkomende lidstaatspecifieke informatie over de regeling KAN op een vrijwillige basis worden gegeven, zoals:

— informatie over de criteria en regels om toezichthouders/auditoren te selecteren en over hoe zij op CDV's toezicht houden (controleren) en hen accrediteren (auditeren);

— andere contactgegevens of algemene informatie over de uitvoering van de regeling.

Scheme type/community/rules (clausule 5.3.9)

Dit veld DIENT te worden gebruikt en DIENT te voldoen aan de specificaties van clausule 5.3.9. van TS 119 612 en DIENT minstens twee URI's te bevatten:

— een URI die voor alle vertrouwenslijsten van de lidstaten gemeenschappelijk is en die leidt naar een beschrijvende tekst die van toepassing DIENT TE zijn voor alle vertrouwenslijsten, als volgt:

  URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

  Beschrijvende tekst:

  „*Participation in a scheme*

  Each Member State must create a „Trusted List of supervised/accredited Certification Service Providers" providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

  The present implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's Trusted List, compiled by the European Commission.

  Policy/rules for the assessment of the listed services

  The Trusted List of a Member State must provide, as a minimum, information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Article 3(2) and (3) and Article 7(1)(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

([1]) De laatste twee soorten informatie zijn van cruciaal belang voor derden om de kwaliteit en het veiligheidsniveau te beoordelen van dergelijke toezicht- en accreditatiesystemen die van toepassing zijn op CDV's die geen KC's afgeven. Deze soorten informatie zullen worden opgenomen op de vertrouwenslijst via „Scheme information URI" (clausule 5.3.7 — informatie die door lidstaten wordt verstrekt), „Scheme type/community/rules" (clausule 5.3.9 — door het gebruik van een voor alle lidstaten gemeenschappelijke tekst) en „TSL policy/legal notice" (clausule 5.3.11 — een voor alle lidstaten gemeenschappelijke tekst met verwijzing naar Richtlijn 1999/93/EG, met de mogelijkheid voor elke lidstaat om lidstaatspecifieke tekst/referenties toe te voegen). Bijkomende informatie over nationale toezicht- of accreditatiesystemen voor CDV's die geen KC's afgeven, kan op dienstenniveau worden verstrekt indien dit van toepassing is en wordt vereist (bv. om onderscheid te maken tussen verschillende kwaliteits-/veiligheidsniveaus) via „Scheme service definition URI" (clausule 5.5.6).

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including compliance with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable „supervision" system (respectively „voluntary accreditation" system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Article 3(3), Article 8)(1), Article 11 (respectively, Article2(13), Article 3(2), Article 7(1)(a), Article 8(1), Article 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a „voluntary accreditation" system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined „recognised approval scheme" implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Article 2(11) of Directive 1999/93/EC). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific „qualification" on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a „qualification" is likely to be limited solely to the national level.

Interpretation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

A „CA/QC" „Service type identifier" („Sti") entry (similarly a CA/QC entry further qualified as being a „RootCA/QC" through the use of „Service information extension" („Sie") additionalServiceInformation Extension)

— indicates that from the „Service digital identifier" („Sdi") identified CA (similarly within the CA hierarchy starting from the „Sdi" identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate EN 319 412-5 defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or EN 319 411-2 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

Note: if no „Sie" „Qualifications Extension" information is present or if an end-entity certificate that is claimed to be a QC is not further identified through a related „Sie" „Qualifications Extension" information, then the „machine-processable" information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcCompliance, QcSSCD, etc.) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF** „Sie" „Qualifications Extension" information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this „Sie" „Qualifications Extension" information, which is constructed on the principle of a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing some additional information regarding the qualified status, the „SSCD support" and/or „Legal person as subject" (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific „Key usage" pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). Those qualifiers are part of the following set of „Qualifiers" used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the qualified status: „QCStatement" meaning the identified certificate(s) is(are) qualified;

AND/OR

— to indicate the nature of the SSCD support:

— „QCWithSSCD" qualifier value meaning „QC supported by an SSCD", or

— „QCNoSSCD" qualifier value meaning „QC not supported by an SSCD", or

— „QCSSCDStatusAsInCert" qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the „Sdi"-„Sie" provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— „QCForLegalPerson" qualifier value meaning „Certificate issued to a Legal Person".

The general interpretation rule for any other „Sti" type entry is that the listed service named according to the „Sn" field value and uniquely identified by the „Sdi" field value has a current supervision/accreditation status according to the „Scs" field value as from the date indicated in the „Current status starting date and time". Specific interpretation rules for any additional information with regard to a listed service (e.g. „Service information extensions" field) may be found, when applicable, in the Member State specific URI as part of the present „Scheme type/community/rules" field.

Please refer to the Technical specifications for a Common Template for the „Trusted List of supervised/accredited Certification Service Providers" in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the Member States' Trusted Lists.".

— Een specifieke URI voor de vertrouwenslijst van elke lidstaat die leidt naar een beschrijvende tekst DIENT van toepassing te zijn op de VL van deze lidstaat:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC waarbij CC = de ISO 3166-1 ([1]) alpha-2-landcode die in het veld „Scheme territory" (clausule 5.3.10) wordt gebruikt

— waar gebruikers de lidstaatspecifieke beleidslijnen/regels kunnen vinden die DIENEN te worden gebruikt voor de beoordeling van de diensten op de lijst overeenkomstig het passende toezichtsysteem en de vrijwilligeaccreditatie-regelingen van de lidstaat;

— waar gebruikers een lidstaatspecifieke beschrijving kunnen vinden over hoe de inhoud van de vertrouwenslijst over de certificatiediensten die geen verband houden met het afgeven van KC's, kan worden gebruikt en geïnterpreteerd. Dit kan worden gebruikt om een mogelijke onderverdeling in de nationale toezicht- of accreditatiesystemen voor CDV's die geen KC's afgeven, aan te duiden en om uit te leggen hoe de velden „Scheme service definition URI" (clausule 5.5.6) en „Service information extension" (clausule 5.5.9) in dit kader worden gebruikt.

Lidstaten KUNNEN bijkomende URI's definiëren, vertrekkende vanuit de bovenvermelde lidstaatspecifieke URI (d.w.z. URI's die worden gedefinieerd vanuit deze hiërarchische, specifieke URI).

TSL policy/legal notice (clausule 5.3.11)

Dit veld DIENT te worden gebruikt en DIENT te voldoen aan de specificaties van clausule 5.3.11 van TS 119 612 volgens welke de beleidslijnen/juridische informatie over de juridische status van de regeling, of de wettelijke vereisten waaraan de regeling voldoet in het rechtsgebied waarin de regeling wordt ingevoerd, en/of de beperkingen en voorwaarden die gelden voor het bijwerken en publiceren van de vertrouwenslijst, een meertalige tekenreeks (eenvoudige tekst) DIENEN te zijn die uit twee delen bestaat:

1. een eerste, verplicht deel (in Brits Engels als verplichte taal en eventueel in een of meer nationale talen) dat voor de vertrouwenslijsten van alle lidstaten gemeenschappelijk is en waarin staat dat het toepasselijke wettelijke kader Richtlijn 1999/93/EG is en dat het veld „Scheme Territory" de implementatie van dit wettelijk kader in de wetgeving van de lidstaten vermeldt.

   Engelstalige versie van de gemeenschappelijke tekst:

   „The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.".

([1]) ISO 3166-1:2006 „Codes for the representation of names of countries and their subdivisions Part 1: Country codes".

Tekst in de nationale taal/talen van de lidstaat:

„Het toepasselijke wettelijke kader voor deze SLV-implementatie van de vertrouwenslijst van onder toezicht staande of geaccrediteerde certificatiedienstverleners voor [naam van de relevante lidstaat] is Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen en de implementatie daarvan in de wetgeving van [naam van de relevante lidstaat].";

2. een tweede, optioneel deel (in Brits Engels als verplichte taal en eventueel in een of meer nationale talen), specifiek voor elke vertrouwenslijst met verwijzingen naar specifieke toepasselijke nationale wettelijke kaders (bv. in het bijzonder over nationale toezicht- of accreditatieregelingen voor CDV's die geen KC's afgeven).

HOOFDSTUK II

CONTINUÏTEIT VAN VERTROUWENSLIJSTEN

De overeenkomstig artikel 3, onder c), van de onderhavige beschikking aan de Commissie mee te delen certificaten DIENEN zodanig te worden verstrekt dat:

— tussen hun geldigheidsdata minstens drie maanden liggen;

— zij gecreëerd worden op grond van nieuwe sleutelparen aangezien een eerder gebruikt sleutelpaar niet opnieuw mag worden gecertificeerd.

In geval van compromittering of het buiten gebruik stellen van EEN van de privésleutels die overeenkomen met de openbare sleutel die zou kunnen worden gebruikt voor het valideren van de handtekening op de vertrouwenslijst, die aan de Commissie is meegedeeld en die is gepubliceerd in de centrale lijsten van verwijzingen van de Commissie, DIENEN de lidstaten:

— onverwijld een nieuwe vertrouwenslijst te publiceren die ondertekend is met een niet-gecompromitteerde privésleutel wanneer de gepubliceerde vertrouwenslijst was ondertekend met een gecompromitteerde of buiten gebruik gestelde privésleutel;

— de Commissie onmiddellijk de nieuwe lijst mee te delen van publieke sleutelcertificaten die overeenkomen met de privésleutels die voor de ondertekening van de vertrouwenslijst zouden kunnen worden gebruikt.

In geval van compromittering of het buiten gebruik stellen van ALLE privésleutels die overeenkomen met de openbare sleutels die zou kunnen worden gebruikt voor het valideren van de handtekening op de vertrouwenslijst en die aan de Commissie zijn meegedeeld en zijn gepubliceerd in de centrale lijsten van verwijzingen van de Commissie, DIENEN de lidstaten:

— nieuwe sleutelparen te genereren die zouden kunnen worden gebruikt voor de ondertekening van de vertrouwenslijst en hun corresponderende publieke sleutelcertificaten;

— onverwijld opnieuw een nieuwe vertrouwenslijst te publiceren die ondertekend is met een van deze nieuwe privésleutels en waarvan het corresponderende certificaat met openbare sleutel moet worden meegedeeld;

— de Commissie onmiddellijk de nieuwe lijst mee te delen van publieke sleutelcertificaten die overeenkomen met de privésleutels die voor de ondertekening van de vertrouwenslijst zouden kunnen worden gebruikt.

HOOFDSTUK III

SPECIFICATIES VOOR DE MENSELIJK LEESBARE VERSIE VAN DE VERTROUWENSLIJST

Wanneer een menselijk leesbare versie van de vertrouwenslijst wordt opgesteld en gepubliceerd ZOU deze moeten worden verstrekt als een Portable Document Format (PDF)-document overeenkomstig ISO 32000 ([1]) dat MOET worden geformatteerd volgens het PDF/A-profiel (ISO 19005 ([2])).

De inhoud van de menselijk leesbare versie van de vertrouwenslijst in PDF/A, ZOU moeten voldoen aan de volgende vereisten.

— de structuur van de menselijke leesbare versie ZOU het logische model uit TS 119 612 moeten weergeven;

— elk veld ZOU zichtbaar moeten zijn en de volgende informatie moeten weergeven:

  — de titel van het veld (bv. „Identificator diensttype"),

  — de waarde van het veld (bv. „CA/KC"),

  — de betekenis (omschrijving) van de waarde van het veld, indien van toepassing (bv. „Een certificatieautoriteit die publieke sleutelcertificaten afgeeft."),

  — indien van toepassing, meerdere versies in natuurlijke talen zoals bepaald in de vertrouwenslijst;

([1]) ISO 32000-1:2008: Document management — Portable document format — Part 1: PDF 1.7
([2]) ISO 19005-2:2011: Document management — Electronic document file format for long-term preservation — Part 2: Use of ISO 32000-1 (PDF/A-2)

— de volgende velden en overeenkomstige waarden van de digitale certificaten in het veld „Service digital identity" ZOUDEN, minstens, in de menselijk leesbare versie moeten worden vermeld:

  — Versie

  — Volgnummer

  — Algoritme van de handtekening

  — Emittent

  — Geldig vanaf

  — Geldig tot

  — Onderwerp

  — Openbare sleutel

  — Certificaatbeleid

  — Onderwerpsleutelidentificator

  — LIC-verdeelpunten

  — Identificator autoriteitsleutel

  — Gebruik sleutel

  — Basisbeperkingen

  — Algoritme duimafdruk

  — Duimafdruk

— De menselijk leesbare versie ZOU gemakkelijk moeten kunnen worden afgedrukt

— De menselijk leesbare versie MOET worden ondertekend door de uitvoerder van de regeling volgens het PAdES baseline-profiel ([1]).

([1]) ETSI TS 103 172 (maart 2012) — Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile