Dit document vormt slechts een documentatiehulpmiddel en verschijnt buiten de verantwoordelijkheid van de instellingen

►**B** ►**C1** **BESCHIKKING 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

(Kennisgeving geschied onder nummer C(2009) 7806)

(Voor de EER relevante tekst)

(2009/767/EG) ◄

(PB L 274 van 20.10.2009, blz. 36)

Gewijzigd bij:

		Publicatieblad		
		nr.	blz.	datum
►**M1**	Besluit 2010/425/EU van de Commissie van 28 juli 2010	L 199	30	31.7.2010

Gerectificeerd bij:

►**C1** Rectificatie PB L 299 van 14.11.2009, blz. 18 (2009/767/EG)
►**C2** Rectificatie PB L 98 van 13.4.2011, blz. 17 (2009/767/EG)

▼B
▼C1

BESCHIKKING 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

(Kennisgeving geschied onder nummer C(2009) 7806)

(Voor de EER relevante tekst)

(2009/767/EG)

DE COMMISSIE VAN DE EUROPESE GEMEENSCHAPPEN,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap,

Gelet op 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 op artikel 8, lid 3,

Overwegende hetgeen volgt:

(1) De verplichtingen voor lidstaten inzake administratieve vereenvoudiging waarvan sprake is in hoofdstuk II van Richtlijn 2006/123/EG, en met name in de artikelen 5 en 8, bestaan onder andere uit het vereenvoudigen van de procedures en formaliteiten die van toepassing zijn voor de toegang tot en de uitoefening van dienstenactiviteiten en uit het verzekeren dat deze procedures en formaliteiten eenvoudig, op afstand en met elektronische middelen via de één-loketten door dienstverleners kunnen worden afgewikkeld.

(2) De procedures en formaliteiten via de „één-loketten" moeten grensoverschrijdend tussen de lidstaten kunnen worden afgewikkeld overeenkomstig artikel 8 van Richtlijn 2006/123/EG.

(3) Om te kunnen voldoen aan de verplichting om procedures en formaliteiten te vereenvoudigen en om het grensoverschrijdende gebruik van de „één-loketten" te vergemakkelijken, moeten elektronische procedures gebaseerd zijn op eenvoudige oplossingen, inclusief het gebruik van elektronische handtekeningen. Indien na een passende risicobeoordeling van concrete procedures en formaliteiten, een hoog veiligheidsniveau of een equivalent van een handgeschreven handtekening noodzakelijk wordt geacht, kan aan de dienstverleners worden gevraagd om voor bepaalde procedures en formaliteiten geavanceerde elektronische handtekeningen te gebruiken die op een gekwalificeerd certificaat zijn gebaseerd, al dan niet met een veilig middel voor het aanmaken van handtekeningen.

([1]) PB L 376 van 27.12.2006, blz. 36.

▼C1

(4) Het gemeenschappelijk kader voor elektronische handtekeningen werd vastgesteld bij Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen ([1]). Om een doeltreffend, grensoverschrijdend gebruik van geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat te bevorderen, moet het vertrouwen in deze elektronische handtekeningen worden verhoogd, ongeacht de lidstaat waarin de ondertekenaar of de certificatiedienstverlener die het gekwalificeerde certificaat afgeeft, is gevestigd. Dit kan worden bereikt door de informatie die nodig is om de elektronische handtekeningen te valideren, en in het bijzonder de informatie over certificatiedienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat, en over de diensten die zij aanbieden, gemakkelijker en in een betrouwbare vorm beschikbaar te stellen.

(5) Er moet voor worden gezorgd dat de lidstaten deze informatie publiek beschikbaar maken via een gemeenschappelijke template zodat er gemakkelijker gebruik van kan worden gemaakt en genoeg details kunnen worden opgenomen zodat de ontvangende partij de elektronische handtekening kan valideren,

HEEFT DE VOLGENDE BESCHIKKING GEGEVEN:

Artikel 1

Gebruik en aanvaarding van elektronische handtekeningen

1. Indien het, na een passende beoordeling van de mogelijke risico's gerechtvaardigd is en overeenkomstig artikel 5, leden 1 en 3, van Richtlijn 2006/123/EG, kunnen de lidstaten voor de afwikkeling van bepaalde procedures en formaliteiten via de één-loketten volgens artikel 8 van Richtlijn 2006/123/EG, de dienstverlener verplichten geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat, al dan niet met een veilig middel voor het aanmaken van handtekeningen, gebruiken, zoals bepaald in en onderworpen aan Richtlijn 1999/93/EG.

2. De lidstaten aanvaarden alle geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat, al dan niet met een veilig middel voor het aanmaken van handtekeningen, voor het afwikkelen van de procedures en formaliteiten als bedoeld in lid 1. De lidstaten behouden echter wel de mogelijkheid om deze aanvaarding te beperken tot geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat en die zijn aangemaakt met een veilig middel voor het aanmaken van handtekeningen, als dit na de risicobeoordeling als bedoeld in lid 1, nodig blijkt.

3. De lidstaten stellen geen eisen voor de aanvaarding van geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat, al dan niet met een veilig middel voor het aanmaken van handtekeningen, als die eisen dienstverleners hinderen in het gebruikmaken van elektronische procedures via de één-loketten.

([1]) PB L 13 van 19.1.2000, blz. 12.

▼C1

4. De lidstaten mogen, onverminderd lid 2, andere elektronische handtekeningen aanvaarden dan de geavanceerde elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat, al dan niet met een met een veilig middel voor het aanmaken van handtekeningen.

Artikel 2

Opstellen, bijwerken en publiceren van vertrouwenslijsten

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

▼M1

2. De lidstaten stellen een vertrouwenslijst op en publiceren deze in zowel een menselijk leesbare als een machinaal verwerkbare versie overeenkomstig de specificaties in de bijlage.

2 bis. De lidstaten ondertekenen elektronisch de machinaal verwerkbare versie van hun vertrouwenslijst en publiceren ten minste de menselijk leesbare versie van de vertrouwenslijst via een beveiligd kanaal teneinde de authenticiteit en de integriteit ervan te verzekeren.

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

a) de instantie of instanties verantwoordelijk voor het opstellen, bijwerken en publiceren van de menselijk leesbare en de machinaal verwerkbare versies van de vertrouwenslijst;

b) de plaatsen waar de menselijk leesbare en de machinaal verwerkbare versies van de vertrouwenslijst worden gepubliceerd;

c) het publieke sleutelcertificaat waarvan is gebruikgemaakt om het beveiligde kanaal op te zetten waarlangs de menselijk leesbare versie van de vertrouwenslijst is gepubliceerd of, indien de menselijk leesbare lijst elektronisch is ondertekend, het publieke sleutelcertificaat waarvan is gebruikgemaakt om de lijst te ondertekenen;

d) het publieke sleutelcertificaat waarvan is gebruikgemaakt om de machinaal verwerkbare versie van de vertrouwenslijst elektronisch te ondertekenen;

e) alle wijzigingen in de onder a) tot en met d) bedoelde informatie.

4. Via een beveiligd kanaal naar een geauthenticeerde webserver stelt de Commissie aan alle lidstaten de in lid 3 bedoelde, door de lidstaten meegedeelde informatie beschikbaar, zowel in een menselijk leesbare versie als in een ondertekende machinaal verwerkbare versie.

▼C1

Artikel 3

Toepassing

Deze beschikking wordt van toepassing vanaf 28 december 2009.

Artikel 4

Adressaten

Deze beschikking is gericht tot de lidstaten.

▼C1

BIJLAGE

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

WOORD VOORAF

1. **Algemeen**

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 een historische informatie over de toezicht- of accreditatiestatus van de onder toezicht staande of geaccrediteerde certificatiediensten.

De vertrouwenslijst (VL) moet onder andere minimuminformatie bevatten over onder toezicht staande of geaccrediteerde CDV's die gekwalificeerde certificaten (KC's) ([2]) afgeven overeenkomstig de bepalingen van Richtlijn 1999/93/EG (artikel 3, leden 2 en 3, en artikel 7, lid 1, onder a)), zoals 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) ([3]).

Bijkomende informatie over andere onder toezicht staande of geaccrediteerde CDV's die geen KC's afgeven, maar diensten verlenen die betrekking hebben op elektronische handtekeningen (bv. tijdstempeldiensten en het afgeven van tijdstempeltokens, het afgeven van niet-gekwalificeerde certificaten, enz.), kunnen op vrijwillige basis in de nationale vertrouwenslijst worden opgenomen.

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) ([4]) die door een gekwalificeerd certificaat ([5]) ([6]) worden ondersteund.

De voorgestelde gemeenschappelijke template is compatibel met een implementatie die gebaseerd is op de specificaties van ETSI TS 102 231 (Elektronische handtekeningen en infrastructuur) ([7]). Deze specificaties worden gebruikt voor de opstelling, publicatie, lokalisatie, toegang, authentificatie en het betrouwbaar maken van dergelijke lijsten.

([1]) Zoals bepaald in artikel 2, lid 11, van Richtlijn 1999/93/EG.
([2]) Zoals bepaald in artikel 2, lid 10, van Richtlijn 1999/93/EG.
([3]) Zoals bepaald in artikel 2, lid 6, van Richtlijn 1999/93/EG.
([4]) Zoals bepaald in artikel 2, lid 2, van Richtlijn 1999/93/EG.
([5]) Voor een AEH die door een KC wordt ondersteund, wordt in dit document het acroniem AEH_{KC} gebruikt.
([6]) 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.
([7]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information (verschaffing van geharmoniseerde statusinformatie van vertrouwensdiensten).

▼C1

2. **Richtsnoeren voor het opstellen van gegevens op de VL**

2.1. *Een VL met voornamelijk onder toezicht staande of geaccrediteerde certificatiediensten*

Relevante certificatiediensten en certificatiedienstverleners op één lijst

Een vertrouwenslijst van een lidstaat wordt gedefinieerd als 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 vertrouwenslijst moet het volgende bevatten:

— **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 zij 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 „vrijwillig-accreditatiesysteem" (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 de richtlijn).

  — Sommige fysische 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 dergelijke „kwalificatie" slechts op het nationale niveau geldt.

▼C1

De vertrouwenslijst van een lidstaat moet minimuminformatie verschaffen over onder toezicht staande of geaccrediteerde CDV's die gekwalificeerde certificaten aan het publiek afgeven overeenkomstig de bepalingen in Richtlijn 1999/93/EG (artikel 3, leden 2 en 3, en artikel 7, lid 1, onder a)), informatie over KC's die de elektronische handtekening ondersteunen en of de handtekening al dan niet werd aangemaakt door een veilig middel voor het aanmaken van handtekeningen.

Bijkomende informatie over andere onder toezicht staande of geaccrediteerde diensten van CDV's die geen KC's aan het publiek afgeven (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.

De vertrouwenslijst heeft als doelstelling:

— het opnemen op een lijst en verstrekken van betrouwbare informatie over de toezicht- of accreditatiestatus van certificatiediensten van certificatiedienstverleners die bij de lidstaat, die verantwoordelijk is voor het opstellen en het bijwerken van de lijst, onder toezicht staan of in deze lidstaat zijn geaccrediteerd voor naleving van Richtlijn 1999/93/EG;

— de validering vergemakkelijken van elektronische handtekeningen die door de onder toezicht staande of geaccrediteerde certificatiediensten op de lijst van de CDV's worden ondersteund.

Eén waardenreeks voor toezicht- en accreditatiestatus

Er mag slechts één VL 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.

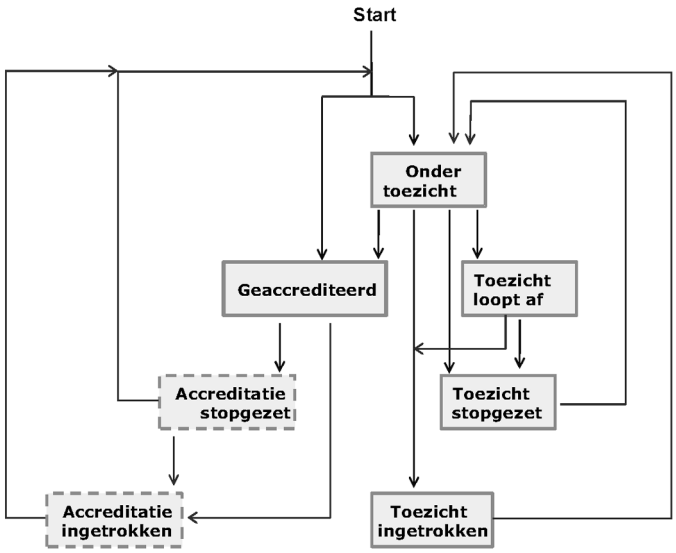
Het feit dat een dienst momenteel onder toezicht staat of is geaccrediteerd, vormt een onderdeel van zijn huidige status. Bijkomend kan een toezicht- of accreditatiestatus ook lopend, aflopend, stopgezet of zelfs ingetrokken zijn. Eenzelfde certificatiedienst kan tijdens zijn levensduur van een toezichtstatus naar een accreditatiestatus veranderen en omgekeerd ([1]).

De volgende afbeelding (afbeelding 1) 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.

▼C1

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



Legende:

Overgangstatus als er een bijbehorend toezichtmodel is (bv. in het geval van een CDV die een KC afgeeft en in een lidstaat is gevestigd).

Mogelijke huidige status als er geen bijbehorend toezichtmodel is (bv. voor CDV's die geen KC's afgeven).

Mogelijke huidige status.

Afbeelding 1

Een certificatiedienst die KC's afgeeft, moet onder toezicht staan (indien de dienst in een lidstaat is gevestigd) en mag vrijwillig geaccrediteerd worden. De statuswaarde van deze dienst kan, indien de dienst is opgenomen in de vertrouwenslijst, een van de hierboven afgebeelde statuswaarden als huidige statuswaarde hebben. Er dient echter te worden opgemerkt dat accreditatie stopgezet en accreditatie ingetrokken enkel overgangstatussen zijn in het geval van diensten van een in een lidstaat gevestigde CDV_{KC}, want dergelijke diensten moeten automatisch onder toezicht staan (zelfs indien de dienst niet of niet meer geaccrediteerd is).

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 de richtlijn) 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.

▼C1

Zo kan een certificatiedienst die geen KC's afgeeft, onder toezicht worden geplaatst of vrijwillig zijn geaccrediteerd. De statuswaarde van deze dienst kan, indien de dienst is opgenomen in de vertrouwenslijst, een van de hierboven afgebeelde statuswaarden als huidige statuswaarde hebben (zie afbeelding 1).

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

— informatie over het toezichtsysteem dat van toepassing is op 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 VL staat voor diensten van CDV's die geen KC's afgeven, wordt de hiervoor vermelde soorten informatie op de vertrouwenslijst opgenomen via „URI met informatie over de regeling" (clausule 5.3.7 — informatie die door lidstaten wordt verstrekt), „Type regeling/publiek/regelgeving" (clausule 5.3.9 — door het gebruik van een voor alle lidstaten gemeenschappelijke tekst, en eventuele bijkomende specifieke informatie van een lidstaat) en „SLV-beleidslijnen/juridische informatie" (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 „bijkomendeDienstInformatie" (clausule 5.8.2) onder „Uitbreiding dienstinformatie" (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, krijgt elke certificatiedienst (die aan de hand van de „Digitale identiteit van de dienst" overeenkomstig ETSI TS 102 231 ([1]) wordt geïdentificeerd) naar verwachting slechts één artikel. Zijn toezicht- of accreditatiestatus zal dienovereenkomstig worden aangepast. In clausule 5.5.4 van de gedetailleerde technische specificaties in hoofdstuk I wordt uitgelegd wat de hierboven vermelde statussen betekenen.

2.2. *VL-gegevens om de validering van KEH's en AEH_{KC}'s vlotter te doen verlopen*

Bij het samenstellen van de VL is het verplichte onderdeel van de VL, 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 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).

([1]) ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information (verschaffing van geharmoniseerde statusinformatie van vertrouwensdiensten).

▼C1

In zoverre er geen echt koppelbaar en grensoverschrijdend profiel voor het KC bestaat, kan de vereiste informatie andere informatie bevatten dan de „Digitale dienstidentiteit" van een enkele (root-) CA (certificatieautoriteit), zoals informatie over de KC-status van het afgegeven certificaat 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 VL (de Uitvoerder van de regeling overeenkomstig ETSI TS 102 231) moet daarom rekening houden met het huidige profiel en de inhoud in elk afgegeven KC per CDV_{KC} die op de VL staat.

Elk afgegeven KC zou idealiter de KcCompliantie ([1]) -vermelding van ETSI 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+-Objectidentificators (OID's) voor certificatiebeleid die worden omschreven in ETSI TS 101 456 omvat ([2]). 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. al dan niet het gebruik 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.

Als de velden ([3])„Identificator diensttype" (Idt), „Dienstnaam" (Dn), en „Digitale dienstidentiteit" (Ddi) worden aangevuld met informatie uit het veld „Uitbreiding dienstinformatie" (Udi), kan aan de hand van de voorgestelde gemeenschappelijke template van de VL 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 informatie worden 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 uiteraard 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 er vanuit te kunnen gaan dat deze KC's door een VMAH worden ondersteund, moet het Udi-veld worden gebruikt om deze ondersteuning aan te duiden (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, dit verzekert).

([1]) Zie ETSI TS 101 862 — Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile (gekwalificeerd profiel van het certificaat).

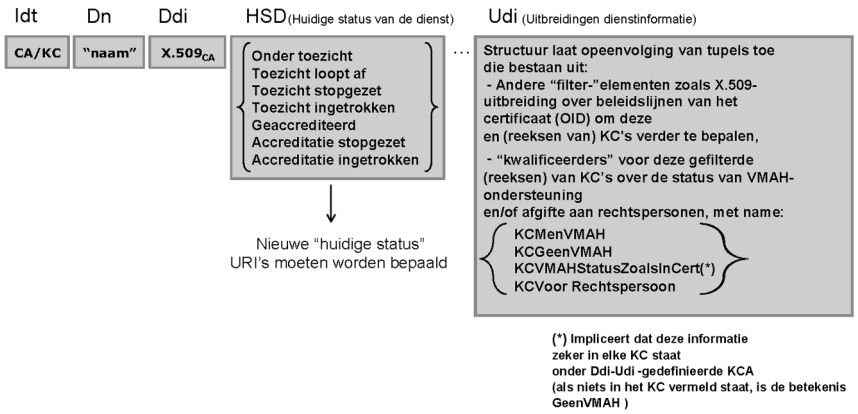
([2]) ETSI TS 101 456 — Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates (beleidseisen voor certificeringsautoriteit die gekwalificeerde certificaten afgeeft).

([3]) Met minstens een X.509 v3-certificaat van de autoriteit die een gekwalificeerd certificaat afgeeft of een hoger geplaatste CA in het certificatiepad.

▼C1

Algemene beginselen — Regels voor het opstellen van CDV_{KC}-artikelen (diensten op de lijst)

Dienstenartikel voor een CDV_{KC} die op de lijst staat:



Afbeelding 2

Dienstenartikel van een CDV die KC's afgeeft en die op de VL staat, die in SLV-formaat wordt geïmplementeerd

De technische specificaties van de gemeenschappelijke template van de huidige VL 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) het X.509v3-certificaat van een CA die KC's afgeeft;

— voor CA/KC-diensten, optionele informatie over Uitbreiding dienstinformatie (Udi) waardoor een reeks van een of meer tupels kan worden opgenomen. Een tupel kan de volgende informatie verschaffen:

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

  — bijbehorende informatie („kwalificeerder") over het al dan niet ondersteund zijn van deze verder geïdentificeerde dienstenreeks van gekwalificeerde certificaten door een VMAH, of over het feit dat 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);

▼C1

— 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.

2.3. *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, ofwel 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 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 GEEN KcVMAH-vermelding, NOCH KCP(+) OID van ETSI, 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 CDVKC-specifieke OID's met beleidslijnen over het certificaat of door andere CDVKC-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 ondersteuning van een VMAH. Hiervoor kunnen het best verschillende informatiewaarden voor VMAH-ondersteuning voor hetzelfde Ddi-veld worden gebruikt bij gebruik van het Udi-veld.

▼C1

In het algemeen geldt dat voor een CDV die op de vertrouwenslijst staat, één dienstenartikel moet worden aangemaakt per X.509v3-certificaat voor een CA/KC-certificatiedienst (dit is een certificatieautoriteit die (rechtstreeks) KC's afgeeft). In bepaalde weloverwogen omstandigheden en onder zorgvuldig beheerde voorwaarden, mag een toezichthoudende/accrediterende instantie van een lidstaat beslissen om het X.509v3-certificaat te gebruiken van een root- of hogergeplaatste CA (dit is een certificatieautoriteit die niet rechtstreeks gekwalificeerde eindgebruikerscertificaten afgeeft, maar een hiërarchie van CA's certificeert tot CA's die gekwalificeerde eindgebruikerscertificaten afgeven) als de Ddi van een enkel artikel van de dienstenlijst van een CDV die op de lijst staat. De gevolgen (voor- en nadelen) van het gebruik van zo'n X.509v3-root-CA of hogergeplaatste CA als Ddi-waarden van dienstenartikels op de vertrouwenslijst, moeten door lidstaten zorgvuldig worden overwogen en goedgekeurd. Bovendien moeten 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.

Het volgende voorbeeld illustreert de algemene richtsnoeren voor het opstellen van artikelen: Indien een CDVKC 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, alle KC's die onder deze root-CA-hiërarchie worden afgegeven, NIET door een VMAH worden ondersteund. Indien deze KC's wel door een VMAH worden ondersteund, 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 die deze informatie niet bevat, is vervallen) moet de SLV (Statuslijst van vertrouwensdiensten) gebruikmaken van het Udi-veld en de bijbehorende kwalificaties-uitbreiding, bv. door het filteren van certificaten door middel van specifieke OID('s) voor CDVKC die mogelijk door hen worden gebruikt om verschillende soorten KC's te onderscheiden (degene die door een VMAH worden ondersteund en andere) en door het opnemen van expliciete „informatie over de VMAH-ondersteuning"voor deze gefilterde certificaten door het gebruik van kwalificeerders.

Dit zijn de **algemene gebruiksaanwijzingen** voor toepassingen, diensten of producten met elektronische handtekening op basis van een SLV-implementatie van een vertrouwenslijst overeenkomstig 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 Udi-uitbreiding bijkomende-DienstInformatie

— 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 de passende KcVermeldingen (dus KcC, KcVMAH) 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 „Kwalificatie"-informatie in Udi staat, of indien een eindgebruikerscertificaat waarvan wordt beweerd dat het een KC is, niet „verder wordt geïdentificeerd" via een bijbehorend Udi-artikel, 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 KcC, KcVMAH) en/of de in ETSI bepaalde KCP(+) OID's zeker in overeenstemming is met wat door de CDVKC wordt beweerd;

▼C1

— **en INDIEN** Kwalificatie-informatie in Udi staat, dan moeten, naast de hierboven vermelde interpretatieregel voor standaardgebruik, de certificaten die geïdentificeerd worden via het gebruik van dit Kwalificatie-artikel in Udi, dat wordt opgebouwd door een opeenvolging van filters die een reeks certificaten verder identificeert en bijkomende informatie verstrekt over 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 een specifieke waarde in een specifiek certificaatveld of -uitbreiding, enz.), in aanmerking worden genomen overeenkomstig de volgende kwalificeerders om het tekort aan informatie in de overeenkomstige KC te compenseren:

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

  — de kwalificeerder KCmetVMAH betekent KC ondersteund door een VMAH, of

  — de kwalificeerder KCzonderVMAH betekent KC niet ondersteund door een VMAH, of

  — de kwalificeerder 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

— de kwalificeerders om de afgifte aan een rechtspersoon aan te duiden:

  — de kwalificeerder KCVoorRechtspersoon betekent Certificaat afgegeven aan een rechtspersoon.

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

De gevallen waarin de LIC's en OCPS-responses worden ondertekend door sleutels die niet van CA's komen die KC's afgeven (CA/KC), moeten ook worden besproken. 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, kunnen deze diensten worden opgenomen in de SLV-implementatie van de VL (met een „Identificator diensttype" die verder wordt gekwalificeerd door de uitbreiding „bijkomendeDienstInformatie" die een OCSP- of een LIC-dienst weergeeft als een onderdeel van de verstrekking van KC's). 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)) op basis van de OCSP- en LIC-standaarddiensttypes overeenkomstig ETSI TS 102 231.

Merk op dat de SLV-implementatie van de VL herroepingsdiensten MOET bevatten indien de betrokken informatie niet in het AIA-veld van eindcertificaten staat, of indien een CA die niet op de lijst staat, heeft ondertekend.

2.5. *Naar een koppelbaar KC-profiel*

Als algemene regel geldt dat moet worden getracht het aantal dienstenartikels (verschillende Ddi's) zo veel mogelijk te vereenvoudigen (verminderen). Anderzijds moeten de diensten die betrekking hebben op het afgeven van KC's en het verstrekken van betrouwbare informatie over het al dan niet ondersteund zijn van deze KC's door een VMAH, nog steeds correct worden geïdentificeerd indien deze informatie niet op het afgegeven KC vermeld staat.

▼C1

Idealiter zou het gebruik van het Udi-veld en de Kwalificatie-uitbreiding (enkel) moeten worden voorbehouden voor de specifieke gevallen waarin het KC niet voldoende informatie bevat over de kwalificatiestatus en het al dan niet ondersteund worden door een VMAH.

Lidstaten zouden zo veel als mogelijk de aanneming en het gebruik van koppelbare KC-profielen moeten doordrukken.

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

De voorgestelde gemeenschappelijke template voor een vertrouwenslijst van een lidstaat zal bestaan uit de volgende informatiecategorieën:

1. informatie over de vertrouwenslijst en de afgifteregeling;

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

3. voor elke CDV op de lijst een reeks velden met ondubbelzinnige identificerende informatie over een onder toezicht staande of geaccrediteerde certificatiedienst van de CDV (deze reeks moet minstens één gegeven bevatten);

4. voor elke onder toezicht staande of geaccrediteerde certificatiedienst op de lijst, identificatie van de huidige status van de dienst en de geschiedenis van deze status.

Voor een CDV die KC's afgeeft, moet bij de ondubbelzinnige identificatie van een onder toezicht staande of geaccrediteerde certificatiedienst die op de lijst moet komen, rekening worden gehouden met die situaties waarin het KC niet genoeg informatie bevat over zijn kwalificatiestatus, over het al dan niet ondersteund zijn door een VMAH en vooral met het bijkomende probleem dat de meeste (commerciële) CDV's één gekwalificeerde CA gebruiken om verschillende soorten eindgebruikerscertificaten, zowel gekwalificeerde als niet-gekwalificeerde, af te geven.

Het aantal artikelen op de lijst per erkende CDV kan worden verminderd indien een of meer hoger geplaatste CA-diensten bestaan, bv. in het kader van een commerciële CA-hiërarchie van een root-CA tot CA's die certificaten afgeven. Zelfs in die gevallen moet echter het ondubbelzinnige verband tussen een certificatiedienst van een CDVKC en de reeks certificaten die als KC's moeten worden geïdentificeerd, gehandhaafd en verzekerd worden.

1. *Informatie over de vertrouwenslijst en de afgifteregeling*

Onder deze categorie valt de volgende informatie:

— een **tag** van de vertrouwenslijst waardoor bij elektronische opzoekingen de vertrouwenslijst gemakkelijker kan worden geïdentificeerd en in de menselijk leesbare versie haar doelstellingen worden bevestigd;

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

— een **opvolgingsnummer (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);

▼C1

— informatie over de **eigenaar 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 waarin 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 en de volgende voorziene aanpassing** van de vertrouwenslijst.

2. *Ondubbelzinnige identificerende informatie over alle CDV's die door de regeling worden erkend*

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.

3. *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:

— 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 deze certificatiedienst;

— een ondubbelzinnige, unieke identificator van de certificatiedienst;

— bijkomende informatie over de certificatiedienst (ofwel rechtstreeks inbegrepen ofwel via een verwijzing naar de plaats waarvan deze informatie kan worden gedownload of waar informatie over de dienst kan worden verkregen);

— voor CA/KC-diensten, een optionele reeks informatietupels met elk de volgende informatie:

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

  ii) de bijbehorende „kwalificeerders" met informatie over het al dan niet ondersteund zijn van de reeks gekwalificeerde certificaten van deze verder geïdentificeerde 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).

▼C1

4. *Voor elke certificatiedienst op de lijst, de identificatie van de huidige status van de dienst en de historiek van deze status*

Deze informatie bevat minstens het volgende:

— een identificator van de huidige status,

— de begindatum en het begintijdstip van de huidige status,

— historische informatie over deze status.

4. **Definities en afkortingen**

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

Term	Acroniem	Definitie
Certificatiedienst-verlener	CDV	Zoals bepaald in artikel 2, lid 11, van Richtlijn 1999/93/EG
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 identificator die in het veld Identificator 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.
Certificaat	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.
Ondertekenaar	Ondertekenaar	Zoals bepaald in artikel 2, lid 3, van Richtlijn 1999/93/EG.
Toezicht	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 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.

▼C1

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 102 231.
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).
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.
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.
Geavanceerde elektronische handtekening	AEH	Zoals bepaald in artikel 2, lid 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 bepaald in artikel 2 van Richtlijn 1999/93/EG.
Veilig middel voor het aanmaken van handtekeningen	VMAH	Zoals bepaald in artikel 2, lid 6, van Richtlijn 1999/93/EG.

HOOFDSTUK 1

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

In het volgende onderdeel van dit document hebben de sleutelwoorden „MOETEN" (MUST), „NIET HOEVEN" (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]).

►M1 De onderhavige specificaties zijn gebaseerd op de specificaties en vereisten in ETSI TS 102 231 v3.1.2. Indien de onderhavige specificaties geen specifieke vereisten stellen, DIENEN de vereisten van ETSI TS 102 231 v.3.1.2 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 102 231 terwijl ze wel worden aangevuld door de formaatspecificaties in ETSI TS 102 231. In het geval van afwijkingen tussen de onderhavige specificaties en de specificaties in ETSI TS 102 231, DIENEN de onderhavige specificaties de norm te zijn.

([1]) IETF RFC 2119: Key words for use in RFCs to indicate Requirements Levels (sleutelwoorden voor het gebruik in RFC's om niveauvereisten aan te duiden).

▼C1

Taalondersteuning DIENT minstens in het Engels (EN) en eventueel ook in een of meer nationale talen uitgevoerd en verstrekt te worden.

Datum- en tijdsaanduiding DIENT overeen te komen met clausule 5.1.4 van ETSI TS 102 231.

Het gebruik van URI's (internet-protocolelement) DIENT overeen te komen met clausule 5.1.5 van ETSI TS 102 231.

Informatie over de afgifteregeling voor vertrouwenslijsten

▼C2

Tag

TSL tag (clausule 5.2.1)

▼C1

Dit veld is VERPLICHT en DIENT te voldoen aan clausule 5.2.1 van ETSI TS 102 231.

▼M1

———————

▼C2

Scheme Information

TSL version identifier (clausule 5.3.1)

▼C1

Dit veld is VERPLICHT en DIENT te worden ingesteld op „3" (geheel getal).

▼C2

TSL sequence number (clausule 5.3.2)

▼M1

Dit veld is VERPLICHT. Het DIENT het volgnummer van de TSL te bevatten. Bij de eerste uitgave van de TSL wordt „1" gebruikt. Deze eenheid DIENT te worden verhoogd bij elke volgende uitgave van de TSL. Het MAG NIET terug op „1" worden gezet wanneer de bovenvermelde „TSL version identifier" wordt verhoogd.

▼C2

TSL type (clausule 5.3.3)

▼M1

Dit veld is VERPLICHT en geeft het type TSL weer. Het DIENT te worden ingesteld op http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Opmerking: Om te kunnen voldoen aan clausule 5.3.3 van ETSI TS 102 231 en om het specifieke SLV-type aan te duiden met verwijzing naar onderhavige specificaties voor de SLV-implementatie van de vertrouwenslijst van de lidstaten ([1]), en met het gebruik van een parser om te bepalen in welke vorm de volgende velden ([2]) kunnen voorkomen, indien deze velden specifieke (of alternatieve) betekenissen hebben volgens het SLV-type (in het geval van een vertrouwenslijst van een lidstaat), DIENT de hierboven vermelde specifieke URI als volgt genoteerd en beschreven te worden:

([1]) De Toezicht- en accreditatiestatuslijst van certificatiediensten van certificatiedienstverleners die onder toezicht staan bij of worden geaccrediteerd door de lidstaat in kwestie voor naleving van Richtlijn 1999/93/EG (kortom, de vertrouwenlijst).

([2]) Hiermee worden de velden bedoeld die worden gespecificeerd in ETSI TS 102 231 — Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information en een specifieke inhoud krijgen op basis van deze specificaties om de opstelling van de vertrouwenslijst van de lidstaten te omschrijven.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Beschrijving: Een SLV-implementatie van een toezicht- of accreditatiestatuslijst van certificatiediensten van certificatiedienstverleners die onder toezicht staan bij of zijn geaccrediteerd in de lidstaat in kwestie die de SLV-implementatie beheert voor naleving van Richtlijn 1999/93/EG via een procedure van direct toezicht (vrijwillig of wettelijk).

▼C2

Scheme operator name (clausule 5.3.4)

▼C1

Dit veld is VERPLICHT. Het DIENT de naam van de instantie van de lidstaat die verantwoordelijk is voor het opstellen, publiceren en bijwerken van de nationale vertrouwenslijst te vermelden. Het DIENT de formele naam te vermelden waaronder de aan deze instantie verbonden rechtspersoon of afgevaardigde instantie (bv. voor administratieve overheidsagentschappen) werkzaam is. Het MOET de naam zijn die wordt gebruikt in de formele wettelijke registratie of autorisatie en waaraan alle formele correspondentie kan worden geadresseerd. Het DIENT een opeenvolging te zijn van meertalige tekenreeksen en DIENT in het Engels (EN) te worden uitgevoerd als verplichte taal en eventueel in een of meer nationale talen.

Opmerking: Een land KAN meerdere toezicht- en accreditatie-instanties hebben en zelfs bijkomende instanties voor alle mogelijke gerelateerde operationele activiteiten. ►M1 Elke lidstaat moet zelf een Scheme operator aanduiden voor de TSL-implementatie van de TL 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 VL, en meer bepaald in de regelingsspecifieke informatie aangeduid ►C2 door de „Scheme information URI" (clausule 5.3.7) ◄.

▼M1

De genoemde Scheme Operator (clausule 5.3.4) is de entiteit die de TSL zal ondertekenen.

▼C2

Scheme Operator address (clausule 5.3.5)

▼C1

Dit veld is VERPLICHT. Het DIENT het adres te vermelden van de rechtspersoon of afgevaardigde organisatie ►C2 die in het veld „Scheme operator name" werd vermeld (clausule 5.3.4) ◄ voor correspondentie via de post of via elektronische weg. ►C2 Het DIENT zowel het „PostalAddress" (straat, plaats, [staat of provincie], [postcode] en ISO 3166-1 alpha-2-landcode) overeenkomstig clausule 5.3.5.1, als het „ElectronicAddress" (e-mail en/of URI van de website) overeenkomstig clausule 5.3.5.2 te bevatten. ◄

▼C2

Scheme name (clausule 5.3.6)

▼C1

Dit veld is VERPLICHT en DIENT de naam waaronder de regeling loopt, weer te geven. Het DIENT een opeenvolging te zijn van meertalige tekenreeksen en wordt (in EN als verplichte taal en eventueel in een of meer nationale talen) op de volgende manier gedefinieerd:

▼C1

— ►C2 De EN- versie DIENT een tekenreeks te zijn ◄ met de volgende structuur:

CC:EN_naam_waarde

waarbij:

— ►C2 „CC” = de ISO 3166-1 alpha-2-landcode die in het veld „Scheme territory field” (clausule 5.3.10) wordt gebruikt; ◄

— „:” = „:” wordt gebruikt als scheidingsteken;

▼M1

— „EN_name_value” = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws.

▼C1

— De versie in de nationale taal van de lidstaat DIENT een tekenreeks te zijn met de volgende structuur:

CC:naam_waarde

waarbij:

— „CC” = de ISO 3166-1 alpha-2-landcode die in het veld „Gebied van de regeling” (clausule 5.3.10) wordt gebruikt;

— „:” = „:” wordt gebruikt als scheidingsteken;

— „naam_waarde” = vertaling van de bovenvermelde „EN_naam_waarde” in de officiële nationale taal.

De naam van de regeling is verplicht ►C2 om op een unieke wijze de regeling waarnaar in „the Scheme information URI” wordt verwezen, ◄ met de naam te kunnen identificeren, en om ervoor te zorgen dat, wanneer een uitvoerder van een regeling meer dan één regeling uitvoert, de regelingen elk een andere naam hebben.

De lidstaten en uitvoerders van een regeling DIENEN ervoor te zorgen dat, wanneer een lidstaat of een uitvoerder van een regeling meer dan één regeling uitvoert, de regelingen elk een verschillende naam hebben.

▼C2

Scheme information URI (clausule 5.3.7)

▼C1

Dit veld is VERPLICHT en DIENT de URI('s) te vermelden waar gebruikers (derden) regelingsspecifieke informatie kunnen verkrijgen (in EN als verplichte taal en eventueel in een of meer nationale talen). Dit DIENT een opeenvolging te zijn van meertalige aanwijzingen (in EN als verplichte taal en eventueel in een of meer nationale talen). De URI('s) in kwestie MOETEN leiden naar passende informatie over de regeling.

De passende informatie over de regeling DIENT minstens het volgende te bevatten:

— Algemene 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). ►C2 De gemeenschappelijke tekst die moet worden gebruikt, is de volgende:

▼C1

„The present list is the TSL implementation of [name of the relevant Member State] „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;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Artikel 3,3, 3.2 and Artikel 7.1(a)), including 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 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 Artikel 3,3, Artikel 8,1, Artikel 11 (respectively, Artikel 2,13, Artikel 3,2, Art 7.1(a), Artikel 8,1, Artikel 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 and the present TSL implementation 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;

([1]) De laatste twee soorten informatie zijn heel belangrijk voor derden om de kwaliteit en het veiligheidsniveau te beoordelen van dergelijke toezicht- of accreditatiesystemen. Deze soorten informatie zullen worden opgenomen op de VL via „Informatie over de regeling — URI" (clausule 5.3.7 — informatie die door lidstaten wordt verstrekt), „Type regeling/publiek/regelgeving" (clausule 5.3.9 — door het gebruik van een voor alle lidstaten gemeenschappelijke tekst) en „Beleids/juridische informatie SLV" (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 „URI met definitie van de dienst onder de regeling" (clausule 5.5.6).

▼C1

— 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 minstens voor elke hierboven vermelde onderliggende regeling 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 fysische 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 bovendien op een vrijwillige basis worden gegeven. Dit DIENT te omvatten:

— 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.

▼C2

Status determination approach (clausule 5.3.8)

▼C1

Dit veld is VERPLICHT en DIENT de identificator van de benadering voor de bepaling van de status te vermelden. De volgende specifieke URI DIENT worden gebruikt zoals die op de volgende manier wordt genoteerd en omschreven:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Beschrijving: De status van diensten die op de lijst staan, wordt bepaald door of in naam van de uitvoerder van de regeling onder een passend systeem voor een lidstaat in kwestie dat „toezicht" toelaat (en, indien van toepassing, „vrijwillige accreditatie") van certificatiedienstverleners die op het grondgebied van de lidstaat zijn gevestigd (of in een derde land zijn gevestigd in het geval van „vrijwillige accreditatie") en die gekwalificeerde certificaten aan het publiek afgeven overeenkomstig artikel 3, lid 3 (respectievelijk artikel 3, lid 2, of artikel 7, lid 1, onder a)) van Richtlijn 1999/93/EG en, indien van toepassing, dat „toezicht"/„vrijwillige accreditatie" toelaat van certificatiedienstverleners die geen gekwalificeerde certificaten afgeven overeenkomstig een nationaal bepaald en opgesteld erkende goedkeuringsregeling die op nationaal niveau werd ingevoerd voor het toezicht op de naleving door diensten van CDV's die geen KC's afgeven van Richtlijn 1999/93/EG en mogelijk uitgebreid door nationale bepalingen over de verlening van dergelijke certificatiediensten.

▼C2

Scheme type/community/rules (clausule 5.3.9)

▼C1

Dit veld is VERPLICHT en DIENT minstens de volgende geregistreerde URI's te bevatten:

— ►C2 een URI die voor alle vertrouwenslijsten van de lidstaten gemeenschappelijk is en die leidt naar een beschrijvende tekst die voor alle TLs van toepassing DIENT te zijn: ◄

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

▼C2

— waarbij de deelname wordt aangegeven van de regeling van de lidstaat (geïdentificeerd via de velden „TSL type" (clausule 5.3.3) en „Scheme name" (clausule 5.3.6)) aan een regeling van regelingen (d.w.z. een TSL met verwijzingen naar alle lidstaten die een TL in de vorm van een TSL publiceren en bijwerken);

▼C1

— waar gebruikers beleidslijnen/regels kunnen vinden die DIENEN te worden gebruikt voor de beoordeling van de diensten op de lijst en op basis waarvan het type SLV (zie clausule 5.3.3) kan worden bepaald;

— waar gebruikers een beschrijving kunnen vinden over hoe de inhoud van de SLV-implementatie van de vertrouwenslijst kan worden gebruikt en geïnterpreteerd. Deze gebruiksregels DIENEN gemeenschappelijk te zijn voor alle vertrouwenslijsten van de lidstaten ongeacht het type van de dienst op de lijst en de toezicht- of accreditatiesystemen.

▼C2

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 TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their 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 a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Artikel 3.3, 3,2 and Artikel 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.

▼C2

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 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 Artikel 3,3, Artikel 8,1, Artikel 11 (respectively, Artikel 2.13, Artikel 3,2, Art 7.1(a), Artikel 8,1, Artikel 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 and the present TSL implementation 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 Artikel 2,11 of the Directive). 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 TSL implementation of the Trusted List

The general user guidelines for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/EC 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 ETSI TS 101862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C2

Note: if no „Sie”„Qualification” information is present or if an end-entity certificate that is claimed to be a QC is not „further identified” through a related Sie entry, 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. QcC, QcSSCD) 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”„Qualification” information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this Sie Qualification entry, 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 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 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 TSL implementation of the Member States' Trusted Lists.”

▼C1

— Een specifieke URI voor alle vertrouwenslijsten van de lidstaten die leidt naar een beschrijvende tekst die van toepassing ZAL zijn op de VL van deze lidstaat:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

waarbij CC = de ISO 3166-1 alpha-2-landcode die in het veld „Gebied van de regeling" (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 vrijwilligeaccreditatieregelingen van de lidstaat;

— waar gebruikers een lidstaatspecifieke beschrijving kunnen vinden over hoe de inhoud van de SLV-implementatie 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 ►C2 om uiteen te zetten hoe de velden „Scheme service definition URI" (clausule 5.5.6) en „Service information extension" 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).

▼C2

Scheme territory (clausule 5.3.10)

▼C1

In het kader van deze specificaties, is dit veld VERPLICHT en DIENT het land te vermelden waarin de regeling wordt ingevoerd (ISO 3166-1 alpha-2-landcode).

▼C2

TSL policy/Legal notice (clausule 5.3.11)

▼C1

Voor onderhavige specificaties is dit veld VERPLICHT en DIENT het de beleidslijnen van de regeling vermelden, of informatie over de juridische status van de regeling, of de wettelijke vereisten waaraan de regeling voldoet voor het rechtsgebied waarin de regeling wordt ingevoerd, en/of de beperkingen en voorwaarden die gelden voor het bijwerken en publiceren van de VL.

Dit DIENT een meertalige tekenreeks te zijn (eenvoudige tekst) die uit twee delen bestaat:

— een eerste, verplicht deel (in het EN als verplichte taal en eventueel in een of meer nationale talen) dat voor de VL's van alle lidstaten gemeenschappelijk is en waarin staat dat het toepasselijke wettelijke kader Richtlijn 1999/93/EG is ►C2 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.".

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];

▼C1

— een tweede, optioneel deel (in het EN als verplichte taal en eventueel in een of meer nationale talen), specifiek voor elke VL 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).

▼C2

Historical information period (clausule 5.3.12)

▼C1

Dit veld is VERPLICHT en DIENT de duur te vermelden (geheel getal) van de historische informatie die in de SLV wordt gegeven. De geheel getal moet worden uitgedrukt in aantal dagen. In het kader van de onderhavige specificaties DIENT dit geheel getal groter of gelijk aan 3 653 te zijn (d.w.z. dat de SLV-implementatie van de VL's van de lidstaten historische informatie MOET bevatten van minimum tien jaar). Voor grotere waarden moet rekening worden gehouden met de wettelijke vereisten van de lidstaat inzake het bijhouden van ►C2 gegevens die worden vermeld in het veld „Scheme Territory" (clausule 5.3.10). ◄

▼C2

Pointers to other TSLs (clausule 5.3.13)

▼C1

In het kader van deze specificaties is dit veld VERPLICHT en DIENT het, indien beschikbaar, de verwijzing naar een op ETSI TS 102231 gebaseerde versie te vermelden van de verzamellijst van de EC met de links (verwijzingen) naar alle SLV-implementaties van vertrouwenslijsten van de lidstaten. Specificaties van clausule 5.3.13 van ETSI TS 102231 zijn van toepassing bij het gebruik van de optionele digitale identiteit die de emittent vertegenwoordigt van de SLV waarnaar wordt verwezen en die overeenkomstig clausule 5.5.3 wordt geformatteerd.

Opmerking: Dit veld DIENT NIET gebruikt te worden in afwachting van de op ETSI TS 102231 gebaseerde implementatie van de verzamellijst van de EC met links naar de SLV-implementatie van de VL's van de lidstaten.

▼C2

List issue date and time (clausule 5.3.14)

▼C1

Dit veld is VERPLICHT en DIENT de datum en het uur te vermelden (UTC, ook Zulu-tijd genoemd) waarop de SLV werd gepubliceerd, met de datum- en uurwaarde uit clausule 5.1.4 van ETSI TS 102231.

▼C2

Next update (clausule 5.3.15)

▼C1

Dit veld is VERPLICHT en DIENT de datum en het uur te vermelden (UTC, ook Zulu-tijd genoemd) waarop de volgende SLV ten laatste zal worden gepubliceerd of heeft als waarde nul om aan te duiden dat de SLV is afgesloten (met de datum- en uurwaarde uit clausule 5.1.4 van ETSI TS 102231).

Indien er geen tussentijdse statusveranderingen zijn aan VVD's of diensten die onder de regeling vallen, MOET de SLV opnieuw worden gepubliceerd voor de vervaldatum van de laatst gepubliceerde SLV.

In het kader van deze specificaties DIENT ►C2 het verschil tussen de datum en het uur van de „Next update" en de „List issue date and time" ◄ NIET meer dan **zes (6)** maanden te bedragen.

▼C2

Distribution points (clausule 5.3.16)

▼C1

Dit veld is OPTIONEEL. Indien dit veld wordt gebruikt, DIENT het de plaatsen te vermelden waar de huidige SLV-implementatie van de VL wordt gepubliceerd en waar aanpassingen aan de huidige SLV kunnen worden gevonden. Indien meerdere verdeelpunten worden vermeld, MOETEN zij allemaal identieke kopieën van de huidige SLV of zijn aangepaste versie verstrekken. Indien dit veld wordt gebruikt, wordt het geformatteerd als een niet-lege opeenvolging van reeksen, waarbij elke reeks overeenkomt met RFC 3986 ([1]).

▼C2

Scheme extensions (clausule 5.3.17)

▼C1

Dit veld is OPTIONEEL en wordt niet gebruikt in het kader van de onderhavige specificatie.

▼C2

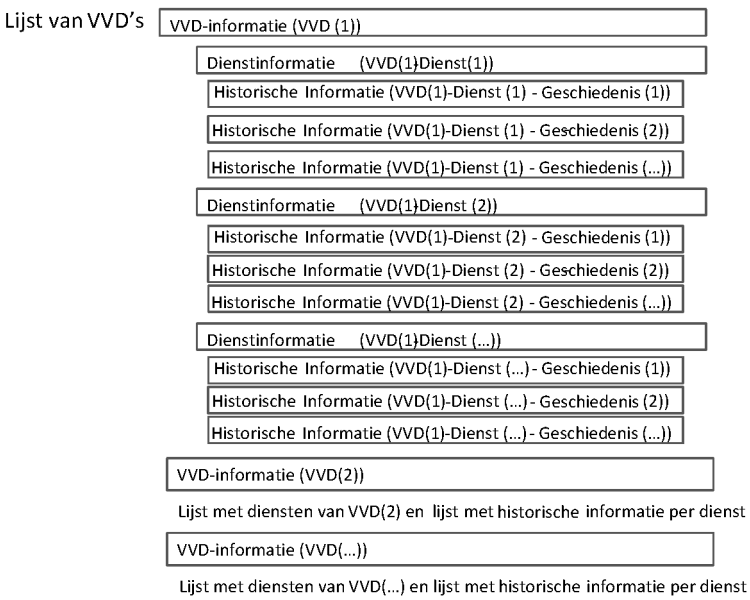
List of Trust Service Providers

▼C1

Dit veld is OPTIONEEL.

Dit veld DIENT afwezig te zijn als er in een lidstaat geen CDV's in het kader van de regeling onder toezicht staan of stonden, of worden of werden geaccrediteerd. Er is echter een akkoord dat, zelfs wanneer een lidstaat geen CDV heeft die door de regeling onder toezicht staat of is geaccrediteerd, de lidstaten een SLV DIENEN te implementeren zonder dit veld. Indien er geen CDV op de lijst staat, DIENT dit te impliceren dat geen CDV's onder toezicht staan of geaccrediteerd zijn in het land dat in het veld „Gebied van de regeling" staat.

Indien een of meer CDV-diensten onder toezicht staan of stonden, of worden of werden geaccrediteerd door de regeling, dan ZAL het veld een opeenvolging bevatten met alle CDV's die een of meer onder toezicht staande of geaccrediteerde diensten verstrekken, met gedetailleerde informatie over de toezicht- of accreditatiestatus en de statusgeschiedenis van alle diensten van de CDV's (VVD = CDV in de onderstaande afbeelding).



([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI): Generic syntax".

▼C2

De lijst met VVD's wordt opgesteld zoals afgebeeld in de bovenstaande figuur. Voor elke VVD is er een veldenreeks met informatie over de VVD („TSP Information"), gevolgd door een lijst met de diensten. Voor elke dienst op de lijst is er een veldenreeks met informatie over de dienst („Service Information") en een veldenreeks over de statusgeschiedenis van de goedkeuring van de dienst („Service approval history").

TSP Information

TSP(1)

TSP name (clausule 5.4.1)

▼C1

Dit veld is VERPLICHT en DIENT de naam te vermelden van de **rechtspersoon** die verantwoordelijk is voor de diensten van de CDV's die onder de regeling onder toezicht staan of stonden, of worden of werden geaccrediteerd. Dit is een opeenvolging van meertalige tekenreeksen (in EN als verplichte taal en eventueel in een of meer nationale talen). Het MOET de naam zijn die wordt gebruikt in formele, wettelijke noteringen en waaraan alle formele correspondentie kan worden geadresseerd.

▼C2

TSP trade name (clausule 5.4.2)

▼C1

Dit veld is OPTIONEEL en DIENT, indien het wordt gebruikt, een alternatieve naam te vermelden waaronder de CDV zichzelf identificeert voor het verlenen van zijn diensten die in deze SLV ►C2 in het artikel „TSP name" (clausule 5.4.1) staan ◄.

Opmerking: Indien één CDV-rechtspersoon diensten verleent onder verschillende handelsnamen of in verschillende specifieke contexten, zijn er evenveel CDV-gegevens als specifieke contexten (bv. Naam-/Handelsnaam-gegevens). Een andere mogelijkheid is het slechts eenmaal opnemen op de lijst van elke CDV (rechtspersoon) en het verstrekken van specifieke contextinformatie over de diensten. De uitvoerder van de regeling van de lidstaat moet de meest geschikte optie bespreken en overeenkomen met de CDV.

▼C2

TSP address (clausule 5.4.3)

Dit veld is VERPLICHT en DIENT het adres te vermelden van de rechtspersoon of afgevaardigde organisatie die in het veld „TSP name" wordt vermeld (clausule 5.4.1) voor correspondentie via de post of elektronische weg. Het DIENT zowel het „PostalAddress" (straat, plaats, [staat of provincie], [postcode] en ISO 3166-1 alpha-2-landcode) overeenkomstig clausule 5.3.5.1 te bevatten, als het „ElectronicAddress" (e-mail en/of URI van de website) overeenkomstig clausule 5.3.5.2.

TSP information URI (clausule 5.4.4)

▼C1

Dit veld is VERPLICHT en DIENT de URI('s) te vermelden waar gebruikers (derden) CDV-specifieke informatie kunnen verkrijgen. Dit DIENT een opeenvolging te zijn van meertalige aanwijzingen (in EN als verplichte taal en eventueel in een of meer nationale talen). De URI('s) waarnaar wordt verwezen, MOETEN leiden naar informatie over de algemene voorwaarden van de CDV, zijn praktijken, wettelijke informatie, klantenservicebeleid en andere algemene informatie over alle diensten die in zijn CDV-artikel op de SLV staan.

Opmerking: Indien één CDV-rechtspersoon diensten verleent onder verschillende handelsnamen of in verschillende specifieke contexten, en dit werd weergegeven in evenveel VVD-gegevens als er specifieke contexten zijn, DIENT dit veld informatie te vermelden over de specifieke diensten die in een bepaald VVD-/HandelsNaam-gegevens zijn opgesomd.

▼C2

TSP information extensions (clausule 5.4.5)

▼C1

Dit veld is OPTIONEEL en KAN, indien het wordt gebruikt, door de uitvoerder van de regeling worden gebruikt overeenkomstig de specificaties in ETSI TS 102231 (clausule 5.4.5), om specifieke informatie te verstrekken die op basis van de regels van de specifieke regeling moet worden geïnterpreteerd.

▼C2

List of Services

▼C1

Dit veld is VERPLICHT en DIENT een reeks te vermelden van alle erkende diensten van de CDV en de goedkeuringsstatus (en de geschiedenis van die status) van die diensten. Minstens een service moet worden vermeld (zelfs al is de informatie volledig historisch).

Aangezien het onder deze specificaties VERPLICHT is historische informatie over de diensten op de lijst bij te houden, MOET die historische informatie worden bijgehouden, ook al vereist de huidige status van de dienst dit normaal niet (bv. als de dienst is ingetrokken). Om de geschiedenis te bewaren, MOET dus een CDV worden opgenomen, ook al is zijn enige dienst op de lijst in een dergelijke status.

▼C2

Service Information

TSP(1) Service(1)

Service type identifier (clausule 5.5.1)

▼M1

Dit veld is VERPLICHT en DIENT de identificator te vermelden van het diensttype overeenkomstig het type van deze TSL-specificaties (d.w.z. „/eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

Indien de dienst die op de lijst staat, betrekking heeft op het afgeven van gekwalificeerde certificaten, is de URI http://uri.etsi.org/TrstSvc/Svctype/CA/QC (een certificatieautoriteit die gekwalificeerde certificaten afgeeft).

Indien de dienst die op de lijst staat betrekking heeft op het afgeven van tokens voor vertrouwensdiensten die geen KC's zijn, noch de afgifte van KC's ondersteunen, DIENT de URI een van de URI's te zijn die in ETSI 102231 zijn omschreven en in clausule D.2, die betrekking heeft op dit veld, zijn opgesomd. Dit DIENT zelfs van toepassing te zijn op alle tokens voor vertrouwensdiensten die onder toezicht staan of geaccrediteerd zijn om te voldoen aan bepaalde specifieke kwalificaties die door de nationale wetgeving van lidstaten worden vereist (bv. zogenaamde gekwalificeerde tijdstempeltokens in DE of HU). De URI DIENT een van de URI's te zijn die in ETSI 102231 zijn omschreven en in clausule D.2, die betrekking heeft op dit veld, zijn opgesomd (bv. TSA (Tijdstempelauthoriteit) voor nationaal gekwalificeerde tijdstempeltokens). Indien dit van toepassing is, MAG deze specifieke nationale kwalificatie van tokens voor vertrouwensdiensten in het dienstgegeven worden vermeld. ►C2 De uitbreiding additionalServiceInformation extension (clausule 5.8.2) in clausule 5.5.9 („Service information extension”) DIENT hiervoor te worden gebruikt. ◄

▼C1

In het algemeen geldt dat per X.509v3-certificaat één gegeven DIENT te worden aangemaakt (bv. voor een CA/KC-certificatiedienst) onder de certificatiediensten op de lijst van een CDV die op de vertrouwenslijst staat (bv. een certificatieautoriteit die (rechtstreeks) KC's afgeeft). In bepaalde weloverwogen omstandigheden en onder zorgvuldig beheerde en goedgekeurde voorwaarden, MAG een toezichthoudende of accrediterende instelling van een lidstaat beslissen om het X.509v3-certificaat te gebruiken van een root- of hoger geplaatste CA (bv. een certificatieautoriteit die niet rechtstreeks eindgebruikers-KC's afgeeft, maar een hiërarchie van CA's certificeert tot CA's die KC's aan eindgebruikers afgeven) als ►C2 de „Sdi" van één gegeven op de dienstenlijst van een CDV ◄ die op de lijst staat. De gevolgen (voor- en nadelen) van het gebruik van zo'n X.509v3-root-CA- of hoger geplaatst CA-certificaat als ►C2 „Sdi"-waarde van dienstgegevens op de vertrouwenslijst ◄, moeten door lidstaten zorgvuldig worden overwogen en goedgekeurd ([1]). Bovendien MOETEN 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.

Opmerking: VVD's zoals OCSP-responders en LIC-emittenten die deel uitmaken van de certificatiediensten van de CDV_{KC}'s en waarvoor aparte sleutelparen worden gebruikt om respectievelijk OCSP-responses en LIC's te ondertekenen, KUNNEN ook worden opgenomen in deze SLV-template door de volgende URI-combinatie te gebruiken:

— ►C2 „Service type identifier" (clausule 5.5.1): ◄

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

▼C2

in combinatie met de volgende uitbreiding „additionalServiceInformation extension" (clausule 5.8.2) in het veld „Service information extension" (clausule 5.5.9):

▼C1

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Omschrijving: een certificaatstatusverlener die een OCSP-server beheert als deel van een dienst van een CDV die gekwalificeerde certificaten afgeeft.

— ►C2 „Service type identifier" (clausule 5.5.1): ◄

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

▼C2

in combinatie met de volgende uitbreiding „additionalServiceInformation extension" (clausule 5.8.2) in het veld „Service information extension" (clausule 5.5.9):

▼C1

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Omschrijving: een certificaatstatusverlener die een LIC beheert als deel van een dienst van een CDV die gekwalificeerde certificaten afgeeft.

— ►C2 „Service type identifier" (clausule 5.5.1): ◄

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Door een X.509v3-certificaat van een root-CA als „Ddi"-waarde voor een dienst op de lijst te gebruiken, moet de uitvoerder van de regeling de hele reeks certificatiediensten onder een dergelijke root-CA als een geheel beschouwen voor wat de „toezicht- of accreditatiestatus betreft". Een statusverandering op vraag van één CA onder de root-hiërarchie op de lijst, zal er dus bijvoorbeeld voor zorgen dat die statusverandering in de hele hiërarchie van toepassing wordt.

▼C2

in combinatie met de volgende uitbreiding „additionalServiceInformation extension” (clausule 5.8.2) in het veld „Service information extension” (clausule 5.5.9):

▼C1

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Omschrijving: een root-certificatieautoriteit van waaruit een certificatiepad kan worden opgesteld tot aan een certificatieautoriteit die gekwalificeerde certificaten afgeeft.

— ►C2 „Service type identifier” (clausule 5.5.1): ◄

http://uri.etsi.org/TrstSvc/Svctype/TSA

▼C2

in combinatie met de volgende uitbreiding „additionalServiceInformation extension” (clausule 5.8.2) in het veld „Service information extension” (clausule 5.5.9):

▼C1

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Omschrijving: een tijdstempeldienst als onderdeel van een dienst van een certificatiedienstverlener die gekwalificeerde certificaten afgeeft en TST's (Tijdstempeltoken) die kunnen worden gebruikt in de gekwalificeerde handtekeningcontroleprocedure om de geldigheid van de handtekening te verifiëren en uit te breiden indien het KC is vervallen of ingetrokken.

▼C2

Service name (clausule 5.5.2)

▼C1

Dit veld is VERPLICHT en DIENT de naam te vermelden waaronder de CDV ►C2 die is vermeld in „TSP name” (clausule 5.4.1) ◄ de dienst verleent ►C2 die is vermeld in „Service type identifier” (clausule 5.5.1). ◄ Dit DIENT een opeenvolging te zijn van meertalige tekenreeksen (in EN als verplichte taal en eventueel in een of meer nationale talen).

▼C2

Service digital identity (clausule 5.5.3)

▼C1

Dit veld is VERPLICHT en DIENT minstens één voorstelling van een digitale identificator te vermelden die uniek is voor het diensttype ►C2 dat is vermeld in „Service type identifier” (clausule 5.5.1) ◄ en waardoor de dienst ondubbelzinnig kan worden geïdentificeerd.

In de onderhavige specificaties DIENT de digitale identificator die in dit veld wordt gebruikt, het relevante X.509v3-certificaat te zijn dat de voorstelling is van de openbare sleutel(s) die de CDV gebruikt voor het verlenen van het diensttype ►C2 dat vermeld staat in „Service type identifier” (clausule 5.5.1) ◄ (d.w.z. de sleutel die wordt gebruikt door een root-CA/KC, de sleutel die wordt gebruikt voor het ondertekenen van certificaten [1], of ook voor het afgeven van tijdstempeltokens, het ondertekenen van LIC's of OCSP-responses). Dit X.509v3-certificaat DIENT te worden gebruikt als de minimaal vereiste digitale identificator (die de voorstelling is van de openbare sleutel(s) die de CDV gebruikt om de dienst te verlenen die op de lijst staat). Bijkomende identificators KUNNEN als volgt worden gebruikt, maar MOETEN allemaal verwijzen naar dezelfde identiteit (d.w.z. het verwante X.509v3-certificaat):

[1] Dit kan het certificaat zijn van een CA die eindgebruikerscertificaten afgeeft (bv. CA/IOS, CA/KC) **of** het certificaat van een betrouwbare root-CA waarvan een pad kan worden gevormd tot gekwalificeerde eindgebruikerscertificaten. Deze informatie („Digitale dienstidentiteit”) moet worden aangevuld met informatie in „Uitbreidingen dienstinformatie” (zie clausule 5.5.9) indien deze informatie en de informatie in elk eindgebruikerscertificaat dat onder deze betrouwbare root wordt afgegeven, niet kan worden gebruikt om op een ondubbelzinnige wijze de passende eigenschappen van gekwalificeerde certificaten te bepalen.

▼C1

a) de kenmerkende naam (KN) van het certificaat die kan worden gebruikt om elektronische handtekeningen te controleren van de CDV-dienst ►C2 die wordt gespecificeerd in „Service type identifier" (clausule 5.5.1); ◄

b) de verwante identificator van de openbare sleutel (d.w.z. X.509v3-Subject-SleutelIdentificator of SSI-waarde);

c) de verwante openbare sleutel.

In het algemeen geldt dat de digitale identificator (d.w.z. het verwante X.509v3-certificaat) NIET meer dan eenmaal in de vertrouwenslijst DIENT voor te komen, dus dat per X.509v3-certificaat één gegeven DIENT te worden aangemaakt voor een certificatiedienst onder de certificatiediensten op de lijst van een CDV die op de vertrouwenslijst staat. ►C2 Andersom DIENT één X.509v3-certificaat te worden gebruikt in één dienstgegeven als de „Sdi"-waarde. ◄

Opmerking 1: Het enige geval waarin het bovenvermelde algemene beginsel niet van toepassing is, is de situatie waarin een enkel X.509v3-certificaat wordt gebruikt bij het afgeven van verschillende soorten tokens voor vertrouwensdiensten waarvoor verschillende toezicht- of accreditatieregelingen van toepassing zijn. Een voorbeeld hiervan is het gebruik door een CDV van een enkel X.509v3-certificaat om enerzijds KC's af te geven onder een passend toezichtsysteem en anderzijds om niet-gekwalificeerde certificaten af te geven onder een andere toezicht- of accreditatiestatus. ►C2 In dit geval en dit voorbeeld, zouden twee artikelen met verschillende „Sti"-waarden (respectievelijk CA/KC en CA/IOS) en met dezelfde „Sdi"-waarde (het verwante X.509v3-certificaat) kunnen worden gebruikt. ◄

Implementaties zijn ASN.1- en XML-afhankelijk en DIENEN in overeenstemming te zijn met de specificaties van ETSI TS 102231 (zie bijlage A van ETSI TS 102231 voor ASN.1 en bijlage B van ETSI TS 102231 voor XML).

Opmerking 2: Indien aanvullende kwalificatie-informatie nodig is voor het gegeven over de geïdentificeerde dienst, ►C2 DIENT de uitvoerder van de regeling eventueel de uitbreiding „additionalServiceInformation" (clausule 5.8.2) onder het veld „Service information extension" (clausule 5.5.9) te gebruiken ◄ om dergelijke bijkomende kwalificatie-informatie te verstrekken. ►C2 De uitvoerder van de regeling kan optioneel ook gebruikmaken van clausule 5.5.6 („Scheme service definition URI"). ◄

▼C2

Service current status (clausule 5.5.4)

▼C1

Dit veld is VERPLICHT en DIENT de identificator van de status van de dienst te vermelden door het gebruik van een van de volgende URI's:

▼C2

— Under Supervision (onder toezicht) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision);

— Supervision of Service in Cessation (toezicht op een aflopende dienst) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation);

— Supervision Ceased (toezicht stopgezet) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased);

— Supervision Revoked (toezicht ingetrokken) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked);

— Accredited (geaccrediteerd) (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited);

— Accreditation Ceased (accreditatie stopgezet) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased);

— Accreditation Revoked (accreditatie ingetrokken) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Bovenstaande statussen DIENEN op basis van onderhavige specificaties van de vertrouwenslijst als volgt te worden geïnterpreteerd:

— ***onder toezicht:*** ►C2 De dienst die in „Service digital identity" (clausule 5.5.3) wordt geïdentificeerd ◄ en door de certificatiedienstverlener (CDV) ►C2 die wordt geïdentificeerd in „TSP name" (clausule 5.4.1) ◄, wordt verleend, staat momenteel onder toezicht voor naleving van Richtlijn 1999/93/EG bij de lidstaat die ►C2 wordt geïdentificeerd in „Scheme territory" (clausule 5.3.10) ◄ waarin de CDV is gevestigd;

▼M1

— ***toezicht op een aflopende dienst:*** de dienst die in „Service digital identity" (clausule 5.5.3) wordt geïdentificeerd en wordt verleend door de CSP die in „TSP name" (clausule 5.4.1) wordt geïdentificeerd, zit momenteel in een aflopende fase, maar staat nog steeds onder toezicht totdat het toezicht wordt stopgezet of ingetrokken. Indien een andere rechtspersoon dan de rechtspersoon die in „TSP name" wordt geïdentificeerd, de verantwoordelijkheid voor deze aflopende fase heeft overgenomen, DIENT deze nieuwe of reserve-rechtspersoon (reserve-CSP) te worden vermeld in „Scheme service definition URI" (clausule 5.5.6) en in de uitbreiding „TakenOverBy" (clausule L.3.2) van het dienstenartikel;

▼C1

— ***toezicht stopgezet:*** de geldigheid van de toezichtbeoordeling is verstreken zonder dat ►C2 de dienst die in „Service digital identity" (clausule 5.5.3) wordt geïdentificeerd ◄, opnieuw werd beoordeeld. De dienst staat momenteel niet meer onder toezicht vanaf de datum van de huidige status en er wordt verondersteld dat de dienst geen activiteiten meer uitvoert;

— ***toezicht ingetrokken:*** de dienst van de CDV en eventueel ook de CDV zelf die voorheen onder toezicht stonden, voldoen niet meer aan Richtlijn 1999/93/EG, ►C2 zoals vastgesteld door de lidstaat die wordt geïdentificeerd in „Scheme territory" (clausule 5.3.10) ◄ waarin de CDV is gevestigd. De dienst mag daarom zijn activiteiten niet meer uitvoeren en moet worden beschouwd als stopgezet op basis van de bovenvermelde reden.

Opmerking 1: De status „Toezicht ingetrokken" kan een definitieve status zijn, ook als de CDV zijn activiteit dan volledig stopzet. In dit geval moet de status niet worden omgezet naar „Toezicht op een aflopende dienst" of „Toezicht stopgezet". De enige manier om de status „Toezicht ingetrokken" te wijzigen, is door opnieuw te voldoen aan Richtlijn 1999/93/EG overeenkomstig het passende toezichtsysteem dat van kracht is in de lidstaat die de VL beheert, en op die manier de status „Onder toezicht" terug te winnen. De statussen „Toezicht op een aflopende dienst" of „Toezicht stopgezet" worden enkel gebruikt als een CDV zijn diensten onder toezicht onmiddellijk stopzet, en niet wanneer het toezicht werd ingetrokken;

— ***geaccrediteerd:*** een accreditatiebeoordeling werd door de accreditatie-instelling uitgevoerd ►C2 namens de lidstaat die wordt geïdentificeerd in „Scheme territory" (clausule 5.3.10) en de dienst die wordt geïdentificeerd in „Service digital identity" (clausule 5.5.3) en wordt verleend door de CDV ([1]) die wordt geïdentificeerd in „TSP name" (clausule 5.4.1) ◄, is in overeenstemming met Richtlijn 1999/93/EG.

([1]) Merk op dat deze geaccrediteerde CDV in een andere lidstaat kan gevestigd zijn dan in de lidstaat in „Gebied van de regeling" van de SLV-implementatie van de VL of in een derde land (zie artikel 7, lid 1, onder a) van Richtlijn 1999/93/EG).

▼C1

Opmerking 2: Indien dit wordt gebruikt voor een CDV die KC's afgeeft en ►C2 is gevestigd in het „Scheme territory" (clausule 5.3.10) ◄, MOETEN de statussen „Accreditatie ingetrokken" en „Accreditatie stopgezet" worden beschouwd als „overgangstatussen" en MOGEN zij niet worden gebruikt als een waarde voor de „Huidige status van de dienst". Indien deze statussen wel worden gebruikt, MOETEN zij onmiddellijk worden gevolgd in „Geschiedenis van de goedkeuring van de dienst" of in „Huidige status van de dienst" door een status „Onder toezicht", eventueel gevolgd door een andere toezichtstatus die hierboven werd gedefinieerd en in Figuur 1 werd afgebeeld. Indien dit wordt gebruikt voor een CDV die geen KC's afgeeft wanneer er slechts een „vrijwilligeaccreditatieregeling" is zonder toezichtregeling of voor een CDV die KC's afgeeft, maar ►C2 niet is gevestigd in het „Scheme territory" (clausule 5.3.10) ◄ (bv. in een derde land), KUNNEN de statussen „Accreditatie ingetrokken" en „Accreditatie stopgezet" worden gebruikt als een waarde voor „Huidige status van de dienst";

— ***accreditatie stopgezet:*** de geldigheid van de accreditatiebeoordeling is verstreken ►C2 zonder dat de dienst die in „Service digital identity" (clausule 5.5.3) wordt geïdentificeerd, opnieuw werd beoordeeld ◄;

— ***accreditatie ingetrokken:*** ►C2 De dienst die in „Service digital identity" (clausule 5.5.3) wordt geïdentificeerd, door de certificatiedienstverlener (CDV) die wordt geïdentificeerd in „TSP name" (clausule 5.4.1) wordt verleend, ◄ en die voorheen in overeenstemming was met criteria van de regeling, en eventueel ook de CDV zelf, voldoen niet meer aan Richtlijn 1999/93/EG.

Opmerking 3: Exact dezelfde statussen moeten worden gebruikt voor CDV's die KC's afgeven en voor CDV's die geen KC's afgeven (bv. verleners van tijdstempeldiensten die tijdstempeltokens afgeven, CDV's die niet-gekwalificeerde certificaten afgeven, enz.). ►C2 De „Service Type identifier" (clausule 5.5.1) wordt gebruikt om ◄ toepasselijke toezicht- en accreditatiesystemen te onderscheiden.

Opmerking 4: Bijkomende kwalificatie-informatie over statussen 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). ►C2 Uitvoerders van de regeling DIENEN de uitbreiding „additionalServiceInformation" (clausule 5.8.2) onder het veld „Service information extension" (clausule 5.5.9) te gebruiken om deze bijkomende kwalificatie-informatie te verstrekken. De uitvoerder van de regeling kan optioneel ook gebruikmaken van clausule 5.5.6 („Scheme service definition URI"). ◄

▼C2

Current status starting date and time (clausule 5.5.5)

▼C1

Dit veld is VERPLICHT en DIENT de datum en het uur te vermelden waarop de huidige goedkeuringsstatus van kracht werd (datum- en uurwaarde overeenkomstig clausule 5.1.4 van ETSI TS 102231).

▼C2

Scheme service definition URI (clausule 5.5.6)

▼C1

Dit veld is OPTIONEEL en DIENT, indien het wordt gebruikt, de URI('s) te vermelden waar gebruikers (derden) dienstspecifieke informatie kunnen verkrijgen die door de uitvoerder van de regeling wordt verstrekt, als een opeenvolging van meertalige verwijzingen (in EN als verplichte taal en eventueel in een of meer nationale talen).

Indien dit veld wordt gebruikt, MOETEN de URI('s) te leiden naar informatie over de door de regeling gespecificeerde dienst. Dit KAN, indien van toepassing, het volgende bevatten:

a) URI met de identiteit van de reserve-CDV in het geval van toezicht van een aflopende dienst waarbij een reserve-CDV is betrokken ►C2 (zie „Service current status" — clausule 5.5.4) ◄;

▼C1

b) URI die leidt naar documenten met bijkomende informatie over het gebruik van bepaalde nationaal bepaalde specifieke kwalificaties voor een onder toezicht staande of geaccrediteerde dienst die tokens voor vertrouwensdiensten afgeeft, overeenkomstig ►C2 het gebruik van het veld „Service information extension" (clausule 5.5.9) met een uitbreiding „additionalServiceInformation" zoals bepaald in clausule 5.8.2. ◄

▼C2

Service supply points (clausule 5.5.7)

▼C1

Dit veld is OPTIONEEL en DIENT, indien het wordt gebruikt, de URI('s) te vermelden waar derden toegang tot de dienst kunnen krijgen via een opeenvolging van tekenreeksen waarvan de opbouw in overeenstemming MOET zijn met RFC 3986.

▼C2

TSP service definition URI (clausule 5.5.8)

▼C1

Dit veld is OPTIONEEL en DIENT, indien het wordt gebruikt, de URI('s) te vermelden waar gebruikers (derden) dienstspecifieke informatie kunnen verkrijgen ►C2 die door de TSP wordt verstrekt ◄, als een opeenvolging van meertalige verwijzingen (in EN als verplichte taal en eventueel in een of meer nationale talen). De URI('s) MOETEN leiden naar informatie over ►C2 de door de TSP gespecificeerde dienst. ◄

▼C2

Service information extensions (clausule 5.5.9)

▼C1

In het kader van deze specificaties is dit veld OPTIONEEL, maar DIENT het wel gebruikt worden ►C2 indien de informatie in de „Service digital identity" (clausule 5.5.3) niet voldoende is ◄ om op ondubbelzinnige wijze de door deze dienst afgegeven gekwalificeerde certificaten te identificeren, en/of indien op basis van de informatie die in deze gekwalificeerde certificaten staat, niet op machinaal verwerkbare wijze kan worden nagegaan of het KC al dan niet door een VMAH wordt ondersteund ([1]).

In het kader van de onderhavige specificaties, DIENT, indien VERPLICHT, bv. voor CA/KC-diensten, een optioneel informatieveld „Uitbreidingen dienstinformatie" („Udi") te worden gebruikt en gestructureerd als een opeenvolging van een of meer tupels, overeenkomstig de uitbreiding „Kwalificaties" die omschreven wordt in bijlage L.3.1 van ETSI TS 102231, waarbij elke tupel de volgende informatie bevat:

— (filters) informatie die kan worden gebruikt om de onder de in het Ddi-veld geïdentificeerde certificatiedienst de exacte dienst (de reeks van gekwalificeerde certificaten) waarvoor bijkomende informatie nodig is of wordt versterkt over de ondersteuning of niet door een VMAH (en/of de afgifte aan een rechtspersoon), verder te identificeren; en

— aanvullende informatie („kwalificeerders") over het al dan niet ondersteund zijn van deze verder geïdentificeerde dienstenreeks van gekwalificeerde certificaten door een VMAH (indien deze informatie „KCVMAHStatusZoalsInCert" is, impliceert dit dat deze informatie een onderdeel is van het KC in een door ETSI-gestandaardiseerde, machinaal verwerkbare versie ([2]), 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).

— ►C2 **QCWithSSCD** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): impliceert dat het door de CDV is verzekerd en door de lidstaat (de toezichthoudende instantie of de accrediterende instantie van de lidstaat) is gecontroleerd of geauditeerd (respectievelijke het toezichtmodel of accreditatiemodel) dat alle KC's onder de dienst ►C2 die wordt geïdentificeerd in „Service digital identity" (clausule 5.5.3) ◄ en verder wordt geïdentificeerd door de bovenvermelde informatie (filters) die wordt gebruikt om de onder ►C2 de in het „Sdi"-veld geïdentificeerde certificatiedienst ◄ de exacte reeks van gekwalificeerde certificaten waarvoor bijkomende informatie nodig is over de aanwezigheid of afwezigheid van VMAH-ondersteuning, verder te identificeren, **WORDEN** ondersteund door een VMAH (dus dat de privésleutel die gelinkt is aan de openbare sleutel in het certificaat is opgeslagen in een veilig middel voor het aanmaken van handtekeningen overeenkomstig bijlage III bij Richtlijn 1999/93/EG);

([1]) Zie punt 2.2 van dit document.

([2]) Dit verwijst naar een passende combinatie van de door ETSI bepaalde vermeldingen KcCompliantie, KcVMAH [ETSI TS 101 862] of een KCP/KCP + OID van ETSI [ETSI TS 101 456].

▼C1

— ►C2 **QCNoSSCD** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): impliceert dat het door de CDV is verzekerd en door de lidstaat (de toezichthoudende instantie of de accrediterende instantie van de lidstaat) is gecontroleerd of geauditeerd (respectievelijke het toezichtmodel of accreditatiemodel) dat alle KC's onder de dienst (root-CA/KC of CA/KC) ►C2 die wordt geïdentificeerd in „Service digital identity" (clausule 5.5.3) ◄ en verder wordt geïdentificeerd door de bovenvermelde informatie (filters) die wordt gebruikt om de onder ►C2 de in het „Sdi"-veld geïdentificeerde certificatiedienst ◄ de exacte reeks van gekwalificeerde certificaten waarvoor bijkomende informatie nodig is over de aanwezigheid of afwezigheid van VMAH-ondersteuning, verder te identificeren, **NIET WORDEN** ondersteund door een VMAH (dus dat de privésleutel die gelinkt is aan de openbare sleutel **niet** in het certificaat is opgeslagen in een veilig middel voor het aanmaken van handtekeningen overeenkomstig bijlage III bij Richtlijn 1999/93/EG);

— ►C2 **QCSSCDStatusAsInCert** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): impliceert dat het door de CDV is verzekerd en door de lidstaat (de toezichthoudende instantie of de accrediterende instantie van de lidstaat) is gecontroleerd of geauditeerd (respectievelijk het toezichtmodel of accreditatiemodel) dat alle KC's onder de dienst (CA/KC) ►C2 die wordt geïdentificeerd in „Service digital identity" (clausule 5.5.3) ◄ en verder wordt geïdentificeerd door de bovenvermelde informatie (filters) die wordt gebruikt om de onder ►C2 de in het „Sdi"-veld geïdentificeerde certificatiedienst ◄ de exacte reeks van gekwalificeerde certificaten waarvoor bijkomende informatie nodig is over de aanwezigheid of afwezigheid van VMAH-ondersteuning, verder te identificeren, de machinaal verwerkbare informatie DIENT te bevatten die aangeeft of het KC door een VMAH wordt ondersteund;

— ►C2 **QCForLegalPerson** ◄ (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): impliceert dat het door de CDV is verzekerd en door de lidstaat (de toezichthoudende instantie of de accrediterende instantie van de lidstaat) is gecontroleerd of geauditeerd (respectievelijke het toezichtmodel of accreditatiemodel) dat alle KC's onder de dienst ►C2 die wordt geïdentificeerd in „Service digital identity" (clausule 5.5.3) ◄ en verder wordt geïdentificeerd door de bovenvermelde informatie (filters) die wordt gebruikt om de onder ►C2 de in het „Sdi"-veld geïdentificeerde certificatiedienst ◄ de exacte reeks van gekwalificeerde certificaten waarvoor bijkomende informatie nodig is over de afgifte aan rechtspersonen, verder te identificeren, **WORDEN** afgegeven aan rechtspersonen.

Deze kwalificeerders mogen slechts worden gebruikt als uitbreiding en als het diensttype http://uri.etsi.org/TrstSvc/Svctype/CA/QC is.

Dit veld is implementatiespecifiek (ASN.1 of XML) en MOET voldoen aan de specificaties in bijlage L.3.1 bij ETSI TS 102231.

▼M1

Voor een XML-implementatie moet de specifieke inhoud van deze bijkomende informatie worden gecodeerd aan de hand van de xsd-bestanden in bijlage C bij ETSI TS 102 231.

▼C2

Service Approval History

▼C1

Dit veld is OPTIONEEL, maar MOET worden gebruikt ►C2 indien informatie staat in „Historical information period" (clausule 5.3.12). ◄ In de context van deze specificaties MOET de regeling dus historische informatie bevatten. Indien historische informatie moet worden bijgehouden, maar de dienst geen geschiedenis heeft vóór de huidige status (dus bij een eerste status of indien de uitvoerder van de regeling geen historische informatie heeft bijgehouden), DIENT dit veld leeg te zijn. Anderzijds DIENT voor elke verandering van de huidige status van de VVD-dienst die binnen de historische informatieperiode gebeurde zoals omschreven in clausule 5.3.12 van ETSI TS 102231, informatie over de vorige goedkeuringsstatus te worden gegeven in een aflopende volgorde van datum en uur van de statusverandering (d.w.z. de datum en het uur waarop de volgende goedkeuringsstatus van kracht werd).

▼C1

Dit DIENT een opeenvolging te zijn van historische informatie zoals hierna wordt bepaald.

▼C2

TSP(1) Service(1) History(1)

Service type identifier (clausule 5.6.1)

▼C1

Dit veld is VERPLICHT en DIENT de identificator van het diensttype te vermelden met ►C2 het formaat en de betekenis van „TSP Service Information — Service type identifier" (clausule 5.5.1) ◄.

▼C2

Service name (clausule 5.6.2)

▼C1

Dit veld is VERPLICHT en DIENT de naam te vermelden waaronder de CDV de dienst verleende ►C2 die is vermeld in „TSP Service Information — Service type identifier" (clausule 5.5.1), met het formaat en de betekenis van „TSP Service Information — Service name" (clausule 5.5.2) ◄. Deze clausule vereist niet dat de naam dezelfde is als de naam in clausule 5.5.2. Een naamsverandering KAN een van de redenen voor een nieuwe status zijn.

▼M1

Service digital identity (clausule 5.6.3)

Dit veld is VERPLICHT en DIENT ten minste één voorstelling van de digitale identificator (d.w.z. het X.509v3-certificaat) te vermelden die in „TSP Service Information — Service digital identity" (clausule 5.5.3) wordt gebruikt en het formaat en de betekenis heeft als omschreven in ETSI TS 102 231, clausule 5.5.3.

Opmerking: In een vertrouwenslijst mag er voor een in de „Sdi" (clausule 5.5.3) van een dienst gebruikte waarde van het X.509v3-certificaat slechts één enkel dienstenartikel per „Sti:Sie/additionalServiceInformation"-waarde voorkomen. De informatie in de „Sdi" (clausule 5.6.3) waarvan wordt gebruikgemaakt in de informatie over de geschiedenis van de goedkeuring van de dienst welke bij een dienstenartikel hoort, en de informatie in de „Sdi" (clausule 5.5.3) waarvan in het dienstenartikel wordt gebruikgemaakt, MOETEN op dezelfde waarde van het X.509v3-certificaat betrekking hebben. Wanneer de „Sdi" van een dienst op de lijst wijzigt (d.w.z. vernieuwing of heruitgifte van een X.509v3-certificaat voor bijvoorbeeld een CA/PKC of CA/QC) of er een nieuwe „Sdi" voor een dergelijke dienst wordt aangemaakt, zelfs met identieke waarden voor de gelinkte „Sti", „Sn" en [„Sie"], dan houdt dat in dat de Scheme Operator een dienstenartikel MOET aanmaken dat verschilt van het vorige.

▼C2

Service previous status (clausule 5.6.4)

▼C1

Dit veld is VERPLICHT en DIENT de identificator van de vorige status van de dienst te vermelden met ►C2 het formaat en de betekenis van „TSP Service Information — Service current status" (clausule 5.5.4) ◄.

▼C2

Previous status starting date and time (clausule 5.6.5)

▼C1

Dit veld is VERPLICHT en DIENT de datum en het uur te vermelden waarop de vorige status in kwestie van kracht werd, met ►C2 het formaat en de betekenis van „TSP Service Information — Service current status starting date and time" (clausule 5.5.5). ◄

▼C2

Service information extensions (clausule 5.6.6)

▼C1

Dit veld is OPTIONEEL en KAN door uitvoerders van regelingen worden gebruikt om specifieke informatie over diensten te geven met ►C2 het formaat en de betekenis van „TSP Service Information — Service information extensions" (clausule 5.5.9) ◄.

▼C2

TSP(1) Service(1) History(2)

Idem voor TSP(1) Service(1) History(2) (vóór History 1)

▼C1

…

▼C2

TSP(1) Service(2)

Idem voor TSP(1) Service 2 (indien van toepassing)

TSP(1)Service(2)History(1).

▼C1

…

▼C2

TSP(2) Information

Idem voor TSP 2 (indien van toepassing)

Idem voor TSP 2 Service 1

Idem voor TSP 2 Service 1 History 1.

▼C1

…

▼M1

Signed TSL

De menselijk leesbare TSL-implementatie van de vertrouwenslijst, die onder deze specificaties, en met name hoofdstuk IV, wordt opgesteld, DIENT door de „Scheme operator name" (clausule 5.3.4) te worden ondertekend om de authenticiteit en de integriteit ervan te verzekeren ([1]). Het formaat van de handtekening ZOU PAdES part 3 (ETSI TS 102 778-3 ([2])) MOETEN ZIJN maar MAG ook PAdES part 2 (ETSI TS 102 778-2 ([3])) zijn in de context van het specifieke model dat is opgesteld via de publicatie van de certificaten waarvan voor de ondertekening van de vertrouwenslijsten is gebruikgemaakt.

De machinaal verwerkbare TSL-implementatie van de vertrouwenslijst, die volgens deze specificaties wordt opgesteld, MOET door de „Scheme operator name" (clausule 5.3.4) worden ondertekend om de authenticiteit en de integriteit ervan te verzekeren. Het formaat van de machinaal verwerkbare TSL-implementatie van de vertrouwenslijst die volgens deze specificaties wordt opgesteld, MOET XML zijn en tevens in overeenstemming zijn met de specificaties die in de bijlagen B en C bij ETSI TS 102 231 zijn vermeld.

Het formaat van de handtekening MOET XAdES BES of EPES zijn, als omschreven in de specificaties van ETSI TS 101 903 voor XML-implementaties. Deze implementatie voor elektronische handtekening MOET voldoen aan de vereisten van bijlage B bij ETSI TS 102 231 ([4]). Aanvullende algemene vereisten voor deze handtekening worden in de volgende afdelingen besproken.

▼C2

Scheme identification (clausule 5.7.2)

▼C1

Dit veld is VERPLICHT en DIENT een door de uitvoerder van de regeling toegewezen referentie te vermelden die op een unieke wijze de regeling die beschreven staat in de onderhavige specificaties en SLV, identificeert. Deze referentie MOET worden opgenomen in de berekening van de handtekening, die wellicht zal bestaan uit een tekenreeks of een reeks van bits.

([1]) Ingeval de menselijk leesbare TSL-implementatie van de vertrouwenslijst niet is ondertekend, MOETEN de authenticiteit en de integriteit ervan worden verzekerd via een passend communicatiekanaal met een evenwaardig veiligheidsniveau. Aanbevolen wordt daartoe gebruik te maken van TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2"), en de vingerafdruk van het certificaat van het TLS-kanaal MOET buiten de band aan de TSL-gebruikers beschikbaar worden gesteld door de lidstaat.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic — Profile based on ISO 32000-1.

([4]) Het ondertekeningscertificaat van de Scheme Operator met de handtekening moet worden beschermd op een van de in ETSI TS 101 903 beschreven manieren en de ds:keyInfo DIENT, indien toepasselijk, de desbetreffende certificaatketen te bevatten.

▼M1

In het kader van de onderhavige specificaties DIENT de referentie het volgende te omvatten: het „TSL type” (clausule 5.3.3), de „Scheme name” (clausule 5.3.6) en de waarde van de uitbreiding SubjectKeyIdentifier van het certificaat dat door de Scheme operator wordt gebruikt om de TSL elektronisch te ondertekenen.

▼C2

Signature algorithm identifier (clausule 5.7.3)

▼C1

Dit veld is VERPLICHT en DIENT het cryptografisch algoritme te vermelden dat werd gebruikt om de handtekening aan te maken. Afhankelijk van het gebruikte algoritme, KUNNEN voor dit veld bijkomende parameters nodig zijn. Dit veld MOET worden opgenomen in de berekening van de handtekening.

▼C2

Signature value (clausule 5.7.4)

▼C1

Dit veld is VERPLICHT en DIENT de huidige waarde van de digitale handtekening te bevatten. Alle SLV-velden (behalve de waarde van handtekening zelf) MOETEN in de berekening van de handtekening worden opgenomen.

▼C2

TSL extensions (clausule 5.8)

ExpiredCertsRevocationInfo (clausule 5.8.1)

▼C1

Deze uitbreiding is OPTIONEEL. Bij gebruik ervan MOET worden voldaan aan clausule 5.8.1 van ETSI TS 102231.

▼C2

AdditionalServiceInformation (clausule 5.8.2)

▼C1

Indien deze OPTIONELE uitbreiding wordt gebruikt, MAG het enkel op dienstniveau worden gebruikt en enkel in ►C2 het veld in clausule 5.5.9 („Service information extension”) ◄. Deze uitbreiding wordt gebruikt om bijkomende informatie over een dienst te geven en DIENT een opeenvolging te zijn van meerdere tupels, waarbij elke tupel de volgende informatie bevat:

a) een URI met aanvullende informatie, zoals:

— een URI met bepaalde nationale specifieke kwalificaties voor een onder toezicht staande of geaccrediteerde vertrouwensdienst die tokens afgeeft, bv.

— een specifiek niveau van onderverdeling op het gebied van veiligheid/kwaliteit van nationale toezicht- of accreditatieregelingen voor CDV's die geen KC's afgeven (bv. RGS */**/*** in FR, specifieke „toezichtstatus” die door de nationale wetgeving is bepaald voor specifieke CDV's die KC's afgeven in DE), zie opmerking 4 van „Huidige status van de dienst” — clausule 5.5.4;

— of een specifieke juridische status voor een onder toezicht staande of geaccrediteerde vertrouwensdienst die tokens afgeeft (bv. een nationale „gekwalificeerde TST's” zoals in DE of HU);

▼C2

— een specifieke beleidsidentificator in het „Sdi”-veld van een X.509v3-certificaat;

▼C1

— of een geregistreerde URI ►C2 zoals bepaald in „Service type identifier”, clausule 5.5.1, om de deelname verder te specificeren van de in het „Sti”-veld geïdentificeerde dienst ◄ als een van de diensten van een certificatiedienstverlener die KC's afgeeft (bc. OCSP-KC, LIC-KC en root-CA-KC);

b) een optionele reeks met de waarde dienstInformatie zoals bepaald in de regeling (bv. *, ** of ***);

c) optionele, bijkomende informatie in een specifiek formaat voor de regeling.

▼**M1**

Het volgen van de URI DIENT te leiden naar menselijk leesbare informatie (ten minste in het EN en eventueel in een of meer nationale talen) die passend en voldoende wordt geacht voor derden om de uitbreiding te begrijpen, en in het bijzonder om de betekenis van alle URI's te verduidelijken en de mogelijke waarden voor serviceInformation en de betekenis van elke waarde te specificeren.

Qualifications Extension (clausule L.3.1)

Omschrijving: Dit veld is FACULTATIEF, maar DIENT te worden gebruikt indien dit VERPLICHT is, bv. voor RootCA/QC- of CA/QC-diensten en indien

— de informatie in „Service digital identity" niet toereikend is om de gekwalificeerde certificaten die door deze dienst worden afgegeven, ondubbelzinnig te identificeren;

— op basis van de informatie die in deze gekwalificeerde certificaten staat, niet op een machinaal verwerkbare manier kan worden nagegaan of het QC al dan niet door een SSCD wordt ondersteund.

Indien van deze uitbreiding op dienstniveau wordt gebruikgemaakt, MAG dat alleen in het veld dat is omschreven in „Service information extension" (clausule 5.5.9) en MOET worden voldaan aan de specificaties die zijn vastgelegd in bijlage L.3.1 bij ETSI TS 102 231.

TakenOverBy Extension (clausule L.3.2)

Omschrijving: Deze uitbreiding is FACULTATIEF maar MOET aanwezig zijn wanneer een dienst die eerder onder de juridische verantwoordelijkheid van een CSP viel, door een andere TSP is overgenomen, en is bedoeld voor de formele mededeling van de juridische verantwoordelijkheid voor een dienst en om de verificatiesoftware in staat te stellen enige juridische bijzonderheden weer te geven ten behoeve van de gebruiker. De in deze uitbreiding verstrekte informatie MOET in overeenstemming zijn met het gerelateerde gebruik van clausule 5.5.6 en MOET voldoen aan de specificaties in bijlage L.3.2 bij ETSI TS 102 231.

▼**M1**

HOOFDSTUK II

Bij het opstellen van hun vertrouwenslijsten maken de lidstaten gebruik van:

taalcodes in kleine letters en landencodes in hoofdletters;

de taal- en landencodes die in onderstaande tabel zijn vermeld;

wanneer een Latijnse schrijfwijze (met een eigen taalcode) bestaat, wordt in onderstaande tabel de transcriptie in Latijns schrift met de bijbehorende taalcodes toegevoegd.

Courante benaming (in de oorspronkelijke taal/talen)	Courante benaming (in het Engels)	Landencode	Taalcode	Opmerkingen	Transcriptie (in Latijns schrift)
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Door de EU aanbevolen landencode	el-Latn
España	Spain	ES	es	ook Catalaans (ca), Baskisch (eu), Galicisch (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Courante benaming (in de oorspronkelijke taal/talen)	Courante benaming (in het Engels)	Landencode	Taalcode	Opmerkingen	Transcriptie (in Latijns schrift)
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Door de EU aanbevolen landencode	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) In Latijns schrift: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

HOOFDSTUK IV

SPECIFICATIES VOOR DE MENSELIJK LEESBARE VERSIE VAN DE SLV-IMPLEMENTATIE VAN DE VERTROUWENSLIJST

Een menselijk leesbare versie van de SLV-implementatie van de vertrouwenslijst MOET op elektronische wijze voor het publiek beschikbaar en toegankelijk zijn. Het ZOU moeten worden verstrekt als een Portable Document Format (PDF)-document overeenkomstig ISO 32000 en MOET worden geformatteerd volgens het PDF/A-profiel (ISO 19005).

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

▼M1

— De titel van de menselijk leesbare versie van vertrouwenslijsten is opgebouwd als een aaneenschakeling van de volgende elementen:

  — facultatieve afbeelding van de nationale vlag van de lidstaat;

  — blanco spatie;

  — courante benaming van het land in de oorspronkelijke taal/talen (als vermeld in de eerste kolom van de tabel in hoofdstuk II);

  — blanco spatie;

  — „(”;

  — courante benaming van het land in het Engels (als vermeld in de tweede kolom van de tabel in hoofdstuk II) binnen de haakjes;

  — „):” als sluitend haakje en scheidingsteken;

  — blanco spatie;

  — „Trusted List”;

  — facultatief logo van de Scheme Operator van de lidstaat.

▼C1

— De structuur van de menselijke leesbare versie ZOU het logische model uit onderdeel 5.1.2 van ETSI TS 102231 moeten weergeven.

— Elk veld ZOU 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 en met name zoals bepaald in bijlage D bij ETSI TS 102231 of in deze specificaties voor geregistreerde URI's (bv. „Een certificatie-autoriteit die certificaten met openbare sleutel afgeeft”);

  — indien van toepassing, meerdere versies in natuurlijke talen zoals bepaald in de SLV-implementatie van de vertrouwenslijst.

— De volgende velden en overeenkomstige waarden van de digitale certificaten in het veld „Digitale dienstidentiteit” ZOUDEN minstens in de menselijk leesbare versie moeten worden vermeld:

  — Versie

  — Volgnummer

  — Algoritme van de handtekening

  — Emittent

  — Geldig vanaf

  — Geldig tot

▼C1

— 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 KAN elektronisch worden ondertekend. Indien deze wordt ondertekend, MOET de uitvoerder van de regeling dit doen volgens dezelfde handtekeningspecificaties als voor de SLV-implementatie van de vertrouwenslijst.