Certificaatpolicy betreffende het Gekwalificeerde

of Genormaliseerde Certipost E-Trust-certificaat

Versie 1.0

–

Datum van publicatie : Mei 2004

Certificaatpolicy (Certificate Policy - CP) betreffende het Gekwalificeerde of Genormaliseerde E-Trust-certificaat

Dit document beschrijft de toepasbaarheid van de certificaten van het type "Gekwalificeerd of Genormaliseerd E-Trust-Certificaat" (hierna het Certificaat genoemd), uitgegeven door de Certificatiedienstverlener (hierna de Certificatiedienstverlener – CSP genoemd) volgens de onderhavige CP, de te volgen procedures en de verantwoordelijkheden van de betrokken partijen, in overeenstemming met de geldende Verklaring van de Certificatie-Activiteiten (hierna het Certification Practices Statement - CPS genoemd) van de Certificatiedienstverlener. Het gaat om een Certificaatpolicy betreffende de Gekwalificeerde en Genormaliseerde Certificaten die voldoet aan de volgende voorwaarden :

Deel		*Ref. RFC 2527*
A	***Overzicht van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy***	**1.1**
	Zeer hoge graad van zekerheid inzake de persoonlijke en eventueel professionele elektronische identiteit ven de Certificaathouder. Het gaat om een Certificaat dat slechts wordt afgeleverd indien men zich persoonlijk aanbiedt tijdens het registratieproces. Dit Certificaat levert een zeer hoog zekerheidsniveau om de link te waarborgen tussen de persoonlijke identiteit van de houder van het Certificaat, een eventuele professionele hoedanigheid (niet-verplicht), een publieke sleutel en het toegestane gebruik ervan. Dit Certificaat levert de hoogste zekerheidsgraad van een correcte authenticatie daar de kandidaat voor het bekomen van het Certificaat : – zich ofwel persoonlijk bij een Lokale Registratie-autoriteit (hierna Local Registration Authority of LRA genoemd) moet aanbieden om correct te worden geregistreerd voor de uitgifte van zijn Certificaat door de Certificatiedienstverlener; – of vooraf moet beschikken over een Certificaat van een gelijkwaardig niveau om de aanvraag op een geldige manier te kunnen indienen. De validatie van de aanvraag vereist de voorlegging van het identiteitsbewijs van de kandidaat-houder voor het bekomen van het Certificaat alsook de verificatie van de stukken die zijn professionele hoedanigheid staven en de ermee overeenstemmende informatie die eventueel moet worden gecertificeerd. De aldus gecertificeerde publieke sleutel kan uitsluitend worden gebruikt in één van de volgende twee gevallen : – in het kader van een digitale handtekening; in dat geval beantwoordt het Certificaat aan het criterium van een **Gekwalificeerd Certificaat** in de zin van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (wet van 9 juli 2001) en de technische standaard ETSI 101 456, en kan het gebruikt worden voor een geavanceerde of een gekwalificeerde handtekening, waarbij deze laatste automatisch gelijkwaardig is aan een handgeschreven handtekening;of – in het kader van versleuteling en/of authenticatie en/of de genormaliseerde digitale handtekening (met uitsluiting van de gekwalificeerde handtekening); in dat geval beantwoordt het Certificaat aan het criterium van een **Genormaliseerd Certificaat** in de zin van de technische standaard ETSI 102 042. De Certificatiedienstverlener(s) gemachtigd om Certificaten af te leveren in overeenstemming met de onderhavige Certificaatpolicy specificeert (specificeren) of hij (zij) hieraan en aan de regelgevende documenten voldoet (voldoen) of of zij werden	

Deel		*Ref. RFC 2527*
	gecertificeerd in overeenstemming hiermee (zie deel D1, § 5 van het dit document). De Gekwalificeerde Certificaten (en de bijhorende Sleutelparen) die worden gebruikt voor de Gekwalificeerde Certificaten zijn steeds verschillend van de Genormaliseerde Certificaten.	
B	***Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy***	
	Een Certificaatpolicy (CP) is een welbepaald geheel van regels die de toepasbaarheid aangeven van een Certificaat op een specifieke gemeenschap en/of een toepasbaarheidsklasse met gemeenschappelijke vereisten inzake veiligheid. Dit document bevat en identificeert binnen dezelfde globale **Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy** verschillende Certificaatpolicies afhankelijk van het gebruik dat van het Certificaat mag worden gemaakt (digitale handtekening of versleuteling/authenticatie), afhankelijk van het feit of het Sleutelpaar werd gegenereerd door de houder van het Certificaat of door de Certificatiedienstleverancier, en afhankelijk van het feit of de Private Sleutel gegenereerd geweest is met en slechts mag worden gebruikt in een Veilig Middel voor het Aanmaken van een Handtekening (Secure Signature Creation Device – SSCD) of niet. Daaruit vloeien twee grote types Certificaten voort. Enerzijds, de **Gekwalificeerde Certificaten**, waarvan het gebruik strikt voorbehouden is voor de digitale handtekening, overeenkomstig de Europese Richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (. wet van 9 juli 2001). Anderzijds de **Genormaliseerde Certificaten**, waarvan het gebruik strikt is voorbehouden voor ofwel (i) de versleuteling, ofwel (ii) de authenticatie, ofwel (iii) de genormaliseerde digitale handtekening (met uitsluiting van de gekwalificeerde handtekening zoals hoger gedefinieerd in Deel A), ofwel (iv) een combinatie van deze gebruiken. Deze Certificaten zijn in overeenstemming met en voldoen aan de vereisten geformuleerd in de respectievelijke technische normen ETSI 101 456 en ETSI 102 042. De Certificaten uitgegeven in overeenstemming met deze CP “Gekwalificeerd of Genormaliseerd E-Trust-certificaat” bevatten een of meerdere Certificaatpolicy-identificatiefactoren die door derden kunnen worden gebruikt om de toepasbaarheid en de betrouwbaarheid van het Certificaat ten opzichte van een bepaalde applicatie te bepalen. De identificatiefactoren voor de Gekwalificeerde of Genormaliseerde E-Trust-certificaatpolicy’s gespecificeerd in dit document, zijn opgenomen in Tabel 1 hieronder.	

Deel		Ref. RFC 2527

Gekwalificeerd E-Trust-certificaat
enkel voor geavanceerde of gekwalificeerde handtekening

	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : **0.4.0.1456.1.2** Aanmaak van de sleutels door de houder : **0.3.2062.7.1.1.3.2.1**
Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : **0.4.0.1456.1.1** Aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.3.3.1**	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : **0.4.0.1456.1.2** Aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.3.4.1**

Genormaliseerd E-Trust-certificaat

	Genormaliseerd Certificaat zonder SSCD (OID ESTI 102 042) **0.4.0.2042.1.1** en aanmaak van de sleutels door de houder : **0.3.2062.7.1.1.3.6.1**
Genormaliseerd Certificaat met SSCD (OID ETSI 102 042) **0.4.0.2042.1.2** en aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.3.7.1**	Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) **0.4.0.2042.1.1** en aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.3.8.1**

Tabel 1. Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust-certificaatpolicy

C *Toepasbaarheid* 1.3.4

- Dit type Certificaat biedt een zeer grote garantie van de persoonlijke of eventueel professionele elektronische identiteit, die kan worden gebruikt om sterk beveiligde applicaties te beschermen zoals bewerkingen van hetzij digitale handtekening, hetzij versleuteling/authenticatie.
- Het is echter de verantwoordelijkheid van de partijen de applicaties te kiezen waarvoor ze vertrouwen hebben in het Certificaat, rekening houdend met de aard van het Certificaat en het beveiligingsniveau van de procedures die werden gevolgd bij de uitgifte van het Certificaat (beschreven in delen B en F van de onderhavige CP).
- Het gebruik van de sleutel (key usage) en de toepasbaarheid van het Certificaat worden gecertificeerd (zie de beschrijving van de inhoud van het Certificaat in deel E van dit document). De aldus gecertificeerde publieke sleutel mag enkel worden gebruikt in een context van geavanceerde of gekwalificeerde digitale handtekening of (uitsluitend) ieder “genormaliseerd” gebruik (met uitsluiting van de gekwalificeerde digitale handtekening). De Certificaten (en de Sleutelparen) die worden gebruikt voor de digitale handtekening zijn steeds verschillend van de andere Certificaten van het genormaliseerde type.
- De Gekwalificeerde Certificaten uitgegeven in het kader van deze CP komen tegemoet aan de vereisten van bijlage I van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). Ze kunnen worden gebruikt om de elektronische handtekeningen te ondersteunen die voldoen aan de vereisten van een handtekening in verband met de gegevens onder elektronische vorm op dezelfde wijze als een handgeschreven handtekening voldoet aan de vereisten in verband met de gegevens op papier, zoals gespecificeerd in artikel 5.1 van de Europese richtlijn en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). In die context stemt deze CP overeen met en voldoet hij aan de vereisten beschreven in het document ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”, in overeenstemming met hoofdstuk 8 ervan zoals gepreciseerd in de clausules vervat

Deel		*Ref. RFC 2527*
	in dit document (zie delen B, C en D van het onderhavige document). Hiertoe publiceert de Certificatiedienstverlener de elementen die deze conformiteitsverklaring ondersteunen, zoals aangegeven in deel D van het onderhavige document. • De Genormaliseerde Certificaten uitgegeven in het kader van deze CP voldoen aan de vereisten van de technische standaard ETSI 102 042. • De Certificaten uitgegeven in het kader van deze CP worden uitgegeven door een Certificatie-autoriteit die voldoet aan de vereisten van bijlage II van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt betreffende het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). • De Certificaten uitgegeven in het kader van deze CP zijn niet uitsluitend bestemd voor het gebruik ervan samen met een Veilig Middel voor het Aanmaken van een Handtekening (SSCD) in de zin van de Europese richtlijn 1999/93/EC.	
D	***Rechten, verantwoordelijkheden en verplichtingen***	***2***
D.1	***Rechten, verantwoordelijkheden en verplichtingen van de Certificatiedienstverlener***	**2.1**
	• De Certificatiedienstverlener zal Certificaten afleveren die voldoen aan de standaarden X.509v3 (ISO 9594-8). • De Certificatiedienstverlener geeft de Gekwalificeerde Certificaten uit onder het label Qualified Certificate zoals bepaald in en in overeenstemming met de vereisten van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (wet van 9 juli 2001), en de technische standaard ETSI TS 101 456. Hiertoe publiceert de Certificatiedienstverlener de elementen die deze conformiteitsverklaring ondersteunen. • De Certificatiedienstverlener geeft de Genormaliseerde Certificaten uit onder het label Normalised Quality Certificate, zoals bepaald in en in overeenstemming met de vereisten van de technische standaard ETSI 102 042 . Hiertoe publiceert de Certificatiedienstverlener de elementen die deze conformiteitsverklaring ondersteunen. • De Certificatiedienstverlener waarborgt dat aan alle vereisten opgenomen in de toepasselijke Certificaatpolicy's (opgenomen in het Certificaat in overeenstemming met deel B van het onderhavige document) wordt voldaan, en waarborgt dat hij de verantwoordelijkheid op zich neemt voor deze conformiteit en dat hij deze diensten zal leveren in overeenstemming met zijn CPS. • Certificatiedienstverlener(s) gemachtigd om Certificaten uit te geven krachtens de onderhavige certificaatpolicy : - Het bedrijf Certipost nv via de **Certipost E-Trust** diensten via de **Certipost E-Trust Primary CA for Qualified Certificates** voor de uitgifte van Gekwalificeerde Certificaten en via de **Certipost E-Trust Primary CA for Normalised Certificates** voor de uitgifte van Genormaliseerde Certificaten: - *Bepalingen van de Certificatie-activiteiten (CPS) :* www.e-trust.be/CPS/QNcerts - *Openbaar Repertorium van de Digitale Certificaten en CRL :* www.e-trust.be/en/x500 - *Conformiteitsverklaring :* www.e-trust.be/CPS/QNcerts	

[1] De persoonsgegevens en de aangemaakte Certificaten die worden geleverd aan de Certificatiedienstverlener en aan de LRA, worden opgenomen in de bestanden van deze laatstgenoemden. Deze gegevens zullen alleen worden gebruikt voor de levering van Certificatiediensten. De titularis van deze gegevens heeft het recht deze te raadplegen en de rechtzetting of desgevallend de afschaffing ervan te vragen.

Deel		Ref. RFC 2527

- *Opschorting en revocatie authoriteit :* 078/15 24 70 (24h/24 beschikbaar en 7 dagen op 7), het formulier van suspensie en revocatie is beschikbaar op het volgende adres : www.e-trust.be/CPS/QNCerts

- Om over te gaan tot de registratie van de kandidaat-houders voor het bekomen van een Certificaat, gebruikt de Certificatiedienstverlener de volgende erkende Lokale Registratie-autoriteiten (Local Registration Authority - LRA) :
  - Personeelsleden van Belgacom en Certipost die door de voormelde Certificatiedienstverlener gemachtigd zijn als registratie-autoriteiten. De geauthenticeerde lijst van deze gemachtigde personeelsleden is beschikbaar op www.e-trust.be/CPS/QNcerts**.**
  - De postkantoren en andere lokale registratie authoriteiten dewelke geacrediteerd zijn om de registratie te kunnen vervullen van de myCertipost gebruikers. Deze lijst is beschikbaar op http://www.mycertipost.be.

- De Certificatiedienstverlener waarborgt enkel dat zijn procedures worden geïmplementeerd in overeenstemming met zijn CPS en met de geldende Controleprocedures en dat ieder Certificaat uitgegeven met aanduiding van het Object Identificatie Nummer (Object Identifier – OID) van een CP werd uitgegeven in overeenstemming met de bepalingen van deze CP, de procedurecontroles, de onderhavige CP en zijn geldende CPS.
- Zie delen 2.1, 2.2 en 2.3 van het CPS van de Certificatiedienstverlener die gelden voor de bijkomende rechten, verantwoordelijkheden en plichten van de Certificatiedienstverlener.
- In sommige gevallen die zijn beschreven in het geldende CPS (RFC 2527 - deel 4.4), heeft de Certificatiedienstverlener het recht het Certificaat te herroepen/schorsen (mits de Certificatiedienstverlener de Certificaathouder via de aangewezen kanalen verwittigt en op de hoogte stelt).
- Wanneer de Certificatiedienstverlener verantwoordelijk is voor de aanmaak van de Sleutels, waarborgt deze dat ieder door hem aangemaakt Sleutelpaar voor rekening van een houder van een Certificaat wordt aangemaakt op beveiligde wijze en dat het privé-karakter van de Private Sleutel van de houder van het Certificaat wordt gewaarborgd in overeenstemming met de vereisten van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (. wet van 9 juli 2001), en de technische standaard ETSI TS 101 456 en 102 042.
- Wanneer de Certificatiedienstverlener verantwoordelijk is voor de voorbereiding en de aflevering van een (Veilig) Middel voor het Aanmaken van een Handtekening ("SSCD"), waarborgt de Certificatiedienstverlener dat indien hij een dergelijk middel levert, dit op beveiligde wijze wordt geleverd in overeenstemming met de vereisten van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001), en met de technische standaard ETSI TS 101 456 en 102 042, en dat het Sleutelpaar zal worden aangemaakt via dit middel.
- In dit verband dient de Certificatiedienstverlener de persoonlijke levenssfeer van de betrokken personen te respecteren en bijgevolg een groot belang te hechten aan en heel behoedzaam te werk te gaan bij het verwerken van deze data. De persoonsgegevens die aan de Certificatiedienstverlener worden verstrekt, worden opgenomen in zijn bestanden. De gegevens zullen enkel worden gebruikt voor de levering van Certificatiediensten. De Certificaathouder van het Certificaat heeft het recht deze gegevens[1] te raadplegen en te wijzigen. De Certificatiedienstverlener verbindt zich ertoe op zijn inschrijvingscontracten voor de Certificaten duidelijk de rechten van de klant te vermelden in het kader van het respect voor de persoonlijke levenssfeer.

Deel		Ref. RFC 2527
	• De Certificatiedienstverlener verbindt zich er eveneens toe de vertrouwelijkheid te waarborgen van de gegevens die niet in deze Certificaten zijn gepubliceerd.	
D.2	***Rechten, verantwoordelijkheden en plichten van de houder van het Certificaat***	**2.1.3**
	De Certificaathouder verklaart zich akkoord met het Certification Practice Statement (CPS) dat van kracht is en de Praktijken beschrijft die worden gebruikt om de Digitale Certificaten af te leveren, en dat is opgemaakt door de Certificatiedienstverlener. De houder van het Certificaat aanvaardt de onderhavige CP. In het bijzonder stemt de houder van het Certificaat in met het volgende : • Het contractuele akkoord met betrekking tot dit type van Certificaat wordt geregeld door het Belgische recht. • De kandidaat-Certificaathouder legt precieze, correcte en volledige informatie voor aan de Certificatiedienstverlener in overeenstemming met het type Certificaat en de Certificaatpolicy('s) opgenomen in deel B van dit document en inzonderheid in overeenstemming met de overeenstemmende registratieprocedures. De houder van het Certificaat is verantwoordelijk voor de nauwkeurigheid van de gegevens die naar de Certificatiedienstverlener worden gestuurd. • De Certificaathouder zal zijn Sleutelpaar enkel gebruiken in overeenstemming met de beperkingen die hem ter kennis werden gebracht in het Certificaat of via een contractueel akkoord. • Wanneer de Certificatiedienstverlener niet verantwoordelijk is voor de aanmaak van de Sleutels, is de kandidaat-Certificaathouder verantwoordelijk voor de aanmaak van zijn Sleutelpaar en zal hij dit aanmaken in overeenstemming met de Certificaatpolicy die werd gekozen uit die welke deel uitmaken van deel B van het onderhavige document, daarbij gebruik makend van een algoritme en een erkende Sleutellengte (minimaal 1024 bit) die voldoen aan de vereisten van de overeenstemmende Certificaatpolicy, in overeenstemming met de contractuele bepalingen overeengekomen met de Certificatiedienstverlener en inzonderheid, in het geval van een Gekwalificeerd Certificaat, in overeenstemming met de vereisten van een elektronische handtekening zoals bepaald in de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001) en in het document ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates". Bovendien waarborgt de Certificaathouder de enige te zijn die de Private Sleutel verbonden met de Publieke Sleutel die moet worden gecertificeerd, bezit. • Indien de toepasselijke CP het gebruik van een (veilig) middel voor het aanmaken van een handtekening vereist, zal het Sleutelpaar worden aangemaakt via dit middel en zal het Certificaat enkel worden gebruikt om deze handtekening uitsluitend via dit middel aan te maken. • De Certificaathouder is verplicht zijn Private Sleutel te allen tijde te beschermen tegen verlies, openbaarmaking aan een andere partij, niet-gewettigde wijziging en niet-gewettigd gebruik, overeenkomstig het geldende CPS en deze CP. Vanaf het ogenblik van de creatie van zijn paar Private en openbare Sleutels is de Certificaathouder persoonlijk aansprakelijk voor de vertrouwelijkheid en de integriteit van zijn Private Sleutel. Elk gebruik van de Private Sleutel wordt geacht het werk te zijn van de eigenaar ervan. De PIN-code (Personal Identity Number) of het paswoord gebruikt om het niet-toegelaten gebruik van de Private Sleutel te vermijden, mag nooit onbeveiligd op dezelfde plaats als de Private Sleutel, noch naast de drager ervan worden opgeslagen, en dient voldoende te zijn beveiligd. De houder van het Certificaat mag zijn Private Sleutel niet onbewaakt in een onvergrendelde staat	

Deel		Ref. RFC 2527

	achterlaten (bv. zonder bewaking in een werkstation wanneer de PIN-code of het paswoord werd ingevoerd). De houder van het Certificaat is als enige verantwoordelijk voor het gebruik van zijn Private Sleutel, de Certificatiedienstverlener is niet verantwoordelijk voor het gebruik van het Sleutelpaar van deCertificaathouder.
	• De Certificaathouder dient de Certificatiedienstverlener te verzoeken zijn Certificaat te schorsen of te herroepen telkens wanneer dit in het geldende CPS wordt vereist (deel 4.4), meer bepaald wanneer :
	  • de Private Sleutel van de houder van het Certificaat werd verloren, gestolen of potentieel gecompromitteerd; of
	  • de Certificaathouder het toezicht over zijn Private Sleutel kwijt is omdat de activeringsgegevens ervan gecompromitteerd werden (bv. de PIN-code) of om een andere reden; en/of
	  • de gecertificeerde gegevens onjuist zijn geworden of zijn veranderd.
	• Zijn Certificaat zal in dat geval onmiddellijk worden herroepen. De schorsings- en herroepingsprocedures worden beschreven in deel J van het onderhavige document.
	• De Certificaathouder dient de Certificatiediensten van de Certificatiedienstverlener onmiddellijk op de hoogte te stellen van elke wijziging in de informatie die in zijn Certificaat is vervat. Zijn certificaat zal in dat geval onmiddellijk worden herroepen.
	• De klant-Certificaathouder dient de Certificatiedienstverlener in kennis te stellen van iedere wijziging van de informatie die niet voorkomt in het Certificaat, maar die bij de registratie naar de Certificatiedienstverlener werd gestuurd. De Certificatiedienstverlener zal de geregistreerde gegevens rechtzetten.
	• De Certificaathouder dient op eigen initiatief de herroeping van zijn Certificaat te vragen indien de aan de Certificatiedienstverlener gestuurde informatie ter staving van een professionele hoedanigheid geheel of gedeeltelijk verouderd zou zijn.
	• De Certificaathouder aanvaardt dat zijn Certificaat onmiddellijk na de creatie ervan in het Certificate Public Registry (Openbaar Certificatieregister) van de Certificatiedienstverlener wordt gepubliceerd.
	• Het Certificaat wordt geacht aanvaard te zijn door de houder van het Certificaat zodra het eerste van de volgende gebeurtenissen zich voordoet, hetzij de 8e dag na de publicatie ervan in het Openbaar Certificatieregister (Certificate Public Registry) van de Certificatiedienstverlener, hetzij vanaf het ogenblik van het eerste gebruik ervan door de Certificaathouder. Tijdens de voormelde periode is de Certificaathouder verantwoordelijk voor de controle van de juistheid van de inhoud van zijn gepubliceerde Certificaat. Indien de Certificaathouder enige incoherentie vaststelt tussen de informatie van het contractuele akkoord en de inhoud van zijn Certificaat, dient hij de Certificatiedienstverlener daarvan onverwijld op de hoogte te stellen. De Certificatiedienstverlener zal in dat geval het Certificaat herroepen en de gepaste maatregelen nemen om een nieuw Certificaat uit te geven. Dit is de enige beroepsmogelijkheid van de Klant m.b.t. de niet-aanvaarding van het Certificaat.
	• De Certificaathouder aanvaardt de bewaring gedurende een periode van 30 jaar na het verstrijken van de geldigheidsduur van het laatste certificaat dat gerelateerd is aan deze registratie door de Certificatiedienstverlener en de Lokale Registratie-autoriteit van alle informatie gebruikt voor de registratie, voor de eventuele levering van een (Veilig) Middel voor het Aanmaken van een Handtekening, om het Certificaat te schorsen of te herroepen en om deze informatie naar derden te sturen onder dezelfde voorwaarden als die vooropgesteld in deze CP ingeval van stopzetting van de activiteiten van de Certificatiedienstverlener.
	• De Certificaathouder aanvaardt de rechten, plichten en verantwoordelijkheden	

Deel		Ref. RFC 2527
	van de Certificatiedienstverlener. Ze worden beschreven in het geldende CPS, de bestelbon, de desbetreffende algemene voorwaarden en de onderhavige CP (deel D1).	
D.3	***Rechten, verantwoordelijkheden en verplichtingen van de Lokale Registratie-autoriteit (LRA)***	
	De Lokale Registratie-autoriteit (LRA) is contractueel verplicht de bepalingen van de Certificatiepraktijken (CPS) van de Certificatiedienstverlener strikt na te leven (zie deel D.1, § 5). De LRA waarborgt : – dat de Certificaathouders correct worden geïdentificeerd en geauthenticeerd, zowel op het niveau van de persoonlijke identiteit van de Certificaathouder als natuurlijke persoon als op het niveau van de eventuele vermeldingen betreffende de beroepshoedanigheid van deze houder ; – dat in voorkomend geval de Certificaataanvragen die naar de Certificatiedienstverlener worden gestuurd ingevuld, correct, geldig en degelijk toegestaan zijn. Meer bepaald : – De registratie-officier informeert de Certificaathouder over de voorwaarden betreffende het gebruik van het Certificaat. Deze zijn opgenomen in de Bestelbon en de Algemene Voorwaarden die moeten worden ondertekend door de advocaat-titularis van het Certificaat (papieren of elektronisch genotariseerd formaat). – De registratie-officier verifieert de identiteit van de Certificaathouder op basis van het (de) door de Belgische wetgeving gevalideerde en erkende identiteitsdocument(en). Dit (deze) document(en) bevat(ten) meer bepaald de volledige naam (familienaam en voornamen), de geboortedatum en –plaats, het fysieke adres van de houder van het Certificaat, zodat contact kan worden opgenomen met de houder. – De registratie-officier verifieert, met het oog op hun Certificatie zoals vermeld in deel E van dit document, de eventuele vermeldingen betreffende de professionele hoedanigheid van de houder van het Certificaat. – Indien de Certificaathouder verenigd is met een rechtspersoon, dient een bewijs van deze vereniging te worden gevalideerd door de registratie-officier. – De registratie-officier zal een kopie van de informatie die bij de registratieprocedure werd verstrekt door de Certificaathouder en die volledig naar de Certificatiedienstverlener werd gestuurd, archiveren, inzonderheid : – een kopie van alle informatie die werd gebruikt om de identiteit en de eventuele vermeldingen inzake de professionele hoedanigheid van de kandidaat-Certificaathouder te verifiëren, met inbegrip van alle referentienummers op de documentatie gebruikt voor de verificatie en alle beperkingen inzake de geldigheid ervan; – een kopie van het contractuele akkoord ondertekend door de Certificaathouder, met inbegrip van zijn akkoord met al zijn verplichtingen. Deze informatie wordt gedurende een periode van 30 jaar bewaard na het verstrijken van de geldigheidsduur van het laatste certificaat dat gerelateerd is aan deze registratie. – Indien het Sleutelpaar niet wordt aangemaakt door de Certificatiedienstverlener of de Lokale Registratie-autoriteit, waarborgt de door de registratieofficier gebruikte valideringsprocedure voor de elektronische aanvraag van het Certificaat dat de houder van het Certificaat in het bezit is van de Private Sleutel die verbonden is met de Publieke Sleutel die moet worden gecertificeerd. – Het respecteren van de vereisten betreffende de bescherming van de persoonsgegevens in het kader van de registratieverrichtingen. De LRA is contractueel verplicht de precieze en geschikte maatregelen te treffen aangaande :	

Deel		*Ref. RFC 2527*
	• de materiële beveiliging van de informatie en, desgevallend, van de systemen; • de logische toegang tot de eventuele software; • het personeel dat belast is met de registratie. De klassering van de gegevens en de verantwoordelijkheid voor deze gegevens zijn van essentieel belang. Worden hier bedoeld : • de gegevens zelf, op papier (registratiegegevens, richtlijnen en procedures, …) en, desgevallend, in elektronische vorm; • de gebruikte software en de configuratie ervan; • de uitrustingen (hardware, telecommunicatiemiddelen, …) en de configuratie ervan; • de materiële toegang tot de gegevens (gebouwen, kluizen, toegangscontrole en voorwaardelijke toegang tot de software, …). De LRA waarborgt dat deze elementen worden beheerd en geklasseerd om een mogelijke impact wegens een gebrek aan vertrouwelijkheid, integriteit of zelfs beschikbaarheid van deze elementen, te vermijden.	
D.4	**Rechten, verantwoordelijkheden en verplichtingen van de Certificaathouder als zelfstandige (indien van toepassing)**	
	De Certificaathouder , als zelfstandige : • stemt in met de verplichtingen, rechten en verantwoordelijkheden van de Certificaathouder zoals hierboven vermeld (deel D.2) respecteren; • is verantwoordelijk voor de voorlegging van het bewijs van zijn statuut van zelfstandige aan de LRA op het ogenblik van de registratie; • waarborgt dat het bewijs van zijn situatie als zelfstandige geldig en correct is.	
D.5	***Rechten, verantwoordelijkheden en verplichtingen van de Onderneming (of de Organisatie) van de houder van het Certificaat (indien van toepassing)***	
	De Onderneming (of de Organisatie), vertegenwoordigd door zijn wettelijke vertegenwoordiger, keurt de registratie van de Certificaathouder goed in het kader van de verkrijging van het Certificaat, waarbij een professionele hoedanigheid moet worden gecertificeerd waarbij de Onderneming (of de Organisatie) betrokken is. De Onderneming (of Organisatie) gaat akkoord met : • het geldende Certification Practice Statement (CPS) dat werd opgesteld door de Certificatiedienstverlener en een beschrijving geeft van de Praktijken die worden gebruikt om de Certificaten af te leveren; • de onderhavige Certificate Policy (CP) van het Gekwalificeerde of Genormaliseerde E-Trust-certificaat. De Onderneming (of Organisatie) gaat akkoord met het volgende : • De Overeenkomst tussen de Onderneming (of de Organisatie), de Certificaathouder en de Certificatiedienstverlener wordt geregeld naar Belgisch recht. • De Onderneming (of Organisatie) stemt in met alle verantwoordelijkheden van de Klant die zijn beschreven in het contract met de Klant. • De Onderneming (of Organisatie) is verantwoordelijk voor de juistheid van de gegevens die door de Onderneming (of de Organisatie) naar de Certificatiedienstverlener worden gestuurd in het kader van de registratie van de Certificaathouder. Ingeval van wijziging van deze informatie dient de Onderneming (of Organisatie) er onmiddellijk de diensten van de Certificatiedienstverlener van in kennis te stellen, die overeenkomstig zullen reageren. • In sommige gevallen die zijn beschreven in het geldende CPS (deel 4.4), heeft de Certificatiedienstverlener het recht het Certificaat te herroepen/schorsen (mits de	

<table>
<tr><td>Deel</td><td></td><td>Ref. RFC 2527</td></tr>
<tr><td></td><td>Certificatiedienstverlener de Certificaathouder en de Onderneming (Organisatie) via de aangewezen kanelen verwittigt en op de hoogte stelt).
• De Onderneming (of Organisatie) dient de Certificatiedienstverlener te verzoeken het Certificaat te schorsen of in te trekken telkens dit in het geldende CPS wordt vereist (deel 4.4). De procedures voor schorsing en herroeping worden beschreven in het geldende CPS (deel 4.4).
• De Onderneming (of Organisatie) verklaart zich akkoord met de rechten, verplichtingen en verantwoordelijkheden van de Certificatiedienstverlener. Deze staan beschreven in het geldende CPS, het contract en deze CP (deel D).</td><td></td></tr>
<tr><td>D.6</td><td>Rechten, verantwoordelijkheden en verplichtingen van derden</td><td></td></tr>
<tr><td></td><td>De derden die zich baseren op de Certificaten die werden uitgegeven krachtens de onderhavige CP :
• zullen de geldigheid van het Certificaat verifiëren door de controle van de inhoud en de handtekening van de Certificatiedienstverlener op het Certificaat en, desgevallend, van de bijbehorende Certificatieketen, de toestand van eventuele schorsing of herroeping van het Certificaat, het Certificaat van de Certificatiedienstverlener die het Certificaat heeft uitgegeven of van een Certificaat van de Certificatieketen die er eventueel mee verbonden is, door zich te baseren op de Lijsten met de Herroepingen van de Certificaten (CRL's) van de Certificatiedienstverlener (zie deel D.1, § 5 van het onderhavige document);
• zullen rekening houden met alle beperkingen op het gebruik van het Certificaat beschreven in het Certificaat, de contractuele documenten en deze CP;
• zullen alle andere voorzorgen nemen zoals voorgeschreven in de onderhavige CP of elders, betreffende het gebruik van het Certificaat.</td><td></td></tr>
<tr><td>E</td><td>Identificatie en Authenticatie – gecertificeerde informatie</td><td>3.1</td></tr>
<tr><td></td><td>De volgende informatie wordt geverifieerd (zie deel E : "Procedure voor aanvraag van een Certificaat" in de onderhavige CP) en gecertificeerd in het Gekwalificeerde of Genormaliseerde E-Trust-certificaat in de volgorde als aangegeven :
<table>
<tr><th>Attribuut</th><th>Verplicht /Optioneel/Vast</th><th>Waarde</th></tr>
<tr><td colspan="3">Distinguished Name :</td></tr>
<tr><td>Country (C)</td><td>Verplicht</td><td>Nationaliteit van de Certificaathouder (Land)</td></tr>
<tr><td>Locality (L)</td><td>Verplicht</td><td>Geboorteplaats van de Certificaathouder (Plaats)</td></tr>
<tr><td>Organisation (O)</td><td>Verplicht</td><td>De officiële naam van de Onderneming (of Organisatie) waartoe de Certificaathouder behoort, zoals gepubliceerd in de statuten van de Onderneming (of Organisatie), met inbegrip van de rechtsvorm of
Voor privé personen wordt de vermelding "Private Person" ingevuld.</td></tr>
<tr><td>Organisational Unit (OU)</td><td>Optioneel</td><td>Organisatie-eenheid of departement (enkel voor "werknemers")</td></tr>
<tr><td>Organisational Unit (OU)</td><td>Verplicht voor kandidaat Certificaathouders, die hun professionele hoedanigheid wensen te specifiëren.</td><td>"Professional status: <…>" Dit kan zijn :
- Self-employed person
- Administrator
- C.E.O.
- Manager
- Employee
of
een andere professionele status, indien de noodzakelijke bewijzen hiervoor geleverd worden tijdens de registratie.)</td></tr>
</table></td><td></td></tr>
</table>

Deel				Ref. RFC 2527
	Organisational Unit (OU)	Verplicht	"Date of birth: <dd/mm/jjjj>" (geboortedatum van de Certificaathouder (dd/mm/jjjj))	
	Common Name (CN)	Verplicht	Naam en voorna(a)m(en) van de Certificaathouder zoals vermeld op de identiteitskaart of gelijkwaardig document.	
	Rfc822Name	Verplicht	E-mailadres van de Certificaathouder	
	Extensies :(non-critical behalve indien anders vermeld)			
	KeyUsage	Vast/Critical	Gekwalificeerd Certificaat : "DigitalSignature, non-repudation" Genormaliseerd Certificaat : "Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment" of een combinatie van deze, zoals aangegeven op de bestelbon.	
	SubjectPublicKey	Verplicht	Publieke sleutel: lengte van de sleutel: 1024 bit; publieke exponent: Fermat-4 (=010001)	
	CertificatePolicies-policyIdentifier	Vast	Zie tabel 1.	
	CertificatePolicies-policyQualifier-userNotice	Vast	"<Qualified or Normalised> E-Trust certificate for digital signature; <Qualified or Normalised> certificate <with or without> SSCD; Key generation by <the owner or the CSP>. General conditions O.I.D.: 0.3.2062.7.1.2.3.1"	
	CertificatePolicies-policyQualifier-CPS	Vast	http://www.e-trust.be/CPS/QNcerts	
	subjectKeyIdentifier	Vast	De keyIdentifier is samengesteld uit een 4 bit type veld met de value 0100, gevolgd door de minst significante 60 bits van de SHA-1 hash van de waarde of subjectPublicKey bit string (tag, lengte en het aantal niet gebruikte bit string bits niet inbegrepen).	
	Authority Info Access	Vast	Access Method=On line Certificate Status Protocol(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.e-trust.be	
	Netscape extension	Vast	SSL client authentication, S/MIME client	
	QcStatement (only for Qualified)	Vast	0.4.1862.1.1 { id-etsi-qcs 1 }	
	Other information:			
	Issuer	Vast	"CN = Certipost E-Trust Primary CA for <Qualified or Normalised>certificates O = Certipost C = BE"	
	Validity	Vast	1 jaar	
	SerialNumber	Verplicht	Volgnummer van het certificaat	
	Algorithm	Vast	"Sha1withRSAEncryption"	
	Versie	Vast	2 (conform met v3)	
	Aan deze gecertificeerde informatie wordt de handtekening van de Certificatie-autoriteit gehecht, die slaat op alle gecertificeerde informatie.			
F	***Procedure voor de aanmaak van de Sleutels***			
	De lengte van de Sleutels moet minstens 1024 bits zijn. ***Aanmaak van de Sleutels door de houder van het Certificaat***			

Deel		Ref. RFC 2527
	De kandidaat-houder van het Certificaat kan zelf zijn Sleutelpaar aanmaken. In dat geval dient hij : • ofwel, in overeenkomst met de Bestelbon op het ogenblik van de registratie bij de officier van de Lokale Registratie-autoriteit een diskette te verstrekken met de PKCS#10-aanvraag van het Certificaat. • ofwel, en dit in het kader van een registratie, uitgevoerd tijdens de inschrijving op de dienst MyCertipost, zijn sleutelpaar en zijn beveiligde electronische aanvraag aan te maken, binnen zijn beveiligde MyCertipost omgeving. ***Aanmaak van de Sleutels door de Certificatiedienstverlener of de Lokale Registratie-autoriteit*** Indien de kandidaat-Certificaathouder de PKCS#10-aanvraag van het Certificaat niet verstrekt op het ogenblik van de registratie bij de officier van de Lokale Registratie-autoriteit en in contractuele overeenstemming met de kandidaat-houder, kunnen drie gevallen zich voordoen: 1. Indien de Lokale Registratie Autoriteit beschikt over de software voor sleutelpaargeneratie en certificaatsaanvraag : • maakt de LRA-operator (LRAO) de Sleutels aan : • de LRAO vraagt de kandidaat-houder van het Certificaat het paswoord (of de PIN-code) in te voeren dat zijn Sleutels zal beschermen; • de LRAO genereert de Sleutels onder standaard-PKCS-formaat op de gekozen drager (bijvoorbeeld diskette of SSCD). De Sleutels hebben de vorm van een bestand dat wordt beschermd door het paswoord (of PIN-code) dat door de kandidaat-houder van het Certificaat werd gekozen; • de LRAO creëert de PKCS#10-aanvraag; • de LRAO wist in zijn software- en hardwareomgeving ieder spoor van de Sleutels van de kandidaat-houder van het Certificaat uit. De Sleutels zijn enkel aanwezig op de drager die aan de houder van het Certificaat wordt bezorgd. 2. Indien de Lokale Registratie Autoriteit niet beschikt over de software voor sleutelpaargeneratie en certificaatsaanvraag : • Maakt de CRA-operator (CRAO) de Sleutels aan, • Creëert de CRAO de PKCS#10-aanvraag. 3. In het kader van een registratie, uitgevoerd tijdens de inschrijvingsprocedure voor de dienst MyCertipost bij een voor dit doeleinde geaccrediteerde LRA, zal de kandidaat-houder van het Certificaat, voor zoverre de dienst beschikbaar zal zijn aan de Certificatiedienstverlener en dit in het kader van zijn beveiligde MyCertipost omgeving, kunnen vragen om zijn sleutelpaar aan te maken. Dit kan gebeuren in en door middel van een SSCD. Deze SSCD zal hem persoonlijk via een aangetekende zending met ontvangstbewijs worden opgezonden. Het paswoord (of PIN code) dat deze SSCD beveiligt, zal hem op een beveiligde wijze via een ander kanaal worden bezorgd. Indien het sleutelpaar niet in en door middel van een SSCD zal worden aangemaakt, zal Certipost de private sleutel geëncrypteerd opsturen binnen zijn beveiligde MyCertipost account. De code om de private sleutel te decrypteren zal worden meegedeeld aan de Klant via een verschillend beveiligd kanaal.	
G	***Procedure voor de aanvraag van het Certificaat***	
	<u>In het geval van de aanvraag via een beveiligde MyCertipost account :</u> 1. De kandidaat-Certificaathouder dient op voorhand een MyCertipost account verkregen hebben waarbij hij de procedures en de voorwaarden tot het verkrijgen van dit account dient te respecteren. Hiervoor dient de kandidaat-Certificaathouder zich on-line te preregistreren op de website http://www.mycertipost.be. Hij dient hierbij zijn MyCertipost contract af te drukken en te ondertekenen, en zich persoonlijk aan te melden bij een geaccrediteerd MyCertipost registratiekantoor. Als alternatief hiervoor kan hij zich electronisch registreren op basis van een electronische handtekening die hem overhandigd geweest is op basis van van een registratie dewelke een	

Deel		Ref. RFC 2527

persoonlijke aanmelding vereist van de kandidaat-Certificaathouder. Door het myCertipost contract te ondertekenen, aanvaardt de kandidaat-Certificatiehouder de Algemene Voorwaarden, de CP en het CPS van kracht in het kader van een on-line aanvraag voor een Gekwalificeerd of Genormaliseerd Certificaat.

2. De kandidaat-Certificaathouder kan binnen zijn beveiligde MyCertipost omgeving toegang verkrijgen tot een dienst die het mogelijk maakt om on-line een certificaat aan te vragen. Hiervoor dient hij on-line een bestelbon in te vullen. Deze bestelbon zal enkel de certificatie mogelijk maken van die gegevens dewelke geverifieerd geweest zijn tijdens de registratie voor een MyCertipost account met uitzondering van het e-mail adres, wat vrij kan ingevuld worden. Overeenkomstig de algemene voorwaarden van het MyCertipost platform heeft het on-line versturen van een electronische certificaatsaanvraag binnen MyCertipost dezelfde contractuele waarde als deze van een handgeschreven handtekening. Tijdens deze procedure aanvaardt de kandidaat-Certificaathouder de Algemene Voorwaarden, de CP het CPS van kracht. Deze documenten en de on-line bestelbon vormen samen de Conventie.
3. De kandidaat-Certificaathouder neemt kennis van de Bestelbon en de Algemene Voorwaarden betreffende de Gekwalificeerde en Genormaliseerde E-Trust-certificaten (hierna de "Bestelbon" en de "Algemene Voorwaarden" genoemd) bij Certipost (www.mycertipost.be). Samen met de CP en het CPS vormen deze de Overeenkomst.
4. De kandidaat-Certificaathouder moet de Bestelbon online invullen en ondertekenen.

Door de Bestelbon te tekenen, aanvaarden de kandidaat-Certificaathouder en de Onderneming (of Organisatie) de Algemene Voorwaarden, de CP en de CPS.

Validatie

In het geval van de elektronische aanvraag via de bestelbon, on line beschikbaar in de persoonlijke beveiligde Certipost-omgeving, zal de tweede verificatie uitgevoerd worden door de Auditor van de Certificatie-Authoriteit (Certification Authority Auditor – CAA), die de coherentie nagaat tussen de uitgegeven Certificaten en de dossiers ontvangen van de LRA's.

In alle andere gevallen :

1. De kandidaat-Certificaathouder verschaft zich de Bestelbon en de Algemene Voorwaarden betreffende de Gekwalificeerde of Genormaliseerde E-Trust-certificaten (hierna de "Bestelbon" en de "Algemene Voorwaarden" genoemd) bij de Certificatiedienstverlener (zie deel D.1, § 5). Samen met de CP en het CPS vormen deze de Overeenkomst. De kandidaat-Certificaathouder kan eveneens aan de Certificatiedienstverlener vragen een kopie van deze documenten te krijgen via de post of deze documenten te bekomen van een Lokale Registratie-autoriteit (Local Registration Authority – LRA) die werd erkend door de Certificatiedienstverlener. Er zijn drie types Bestelbons en Algemene Voorwaarden beschikbaar :

   a. **Bestelbon en Algemene Voorwaarden voor werknemers** : voor de medewerkers of de leden van een Onderneming (of Organisatie)
   b. **Bestelbon en Algemene Voorwaarden voor zelfstandigen/privé-personen** : voor de zelfstandigen en de privé-personen
   c. **Bestelbon en Algemene Voorwaarden voor bestuurders/zaakvoerders** : voor de bestuurders en zaakvoerders van bedrijven

2. De kandidaat-Certificaathouder dient de Bestelbon behoorlijk in te vullen en te ondertekenen. De versies *zelfstandigen/privé-personen* en *bestuurders/zaakvoerders* van de Bestelbon bevatten slechts een enkel gedeelte, het gedeelte Klant. De versie *werknemers* van de Bestelbon bestaat uit twee delen :
   a. Het gedeelte Klant dient behoorlijk te worden ingevuld en ondertekend door de kandidaat-houder van het Certificaat;
   b. Het gedeelte Organisatie dient behoorlijk te worden ingevuld en ondertekend door

Deel		Ref. RFC 2527

een wettelijke vertegenwoordiger (of zijn gemachtigde afgevaardigde) van de Onderneming (of Organisatie) waar de kandidaat-houder van het Certificaat deel van uitmaakt op het ogenblik dat hij deze informatie betreffende zijn professionele hoedanigheid in het Certificaat wil laten certificeren, in overeenstemming met zijn Onderneming (of Organisatie).

Door de ondertekening van de Bestelbon aanvaarden de kandidaat-Certificaathouder en de Onderneming (of Organisatie) de Algemene Voorwaarden.

3. De kandidaat-houder van het Certificaat dient zich persoonlijk aan te bieden bij een in de context van deze CP goedgekeurde LRA (zie deel D.1, § 5). De kandidaat-Certificaathouder maakt een afspraak met een officier van de LRA (LRAO) en gaat bij de LRA langs met alle onderstaande documenten.

a. Voor de werknemers of de leden van een Onderneming (of Organisatie) :

- de behoorlijk ingevulde en ondertekende Bestelbon;
- een kopie (recto/verso) van de geldige en officiële identiteitskaart van de kandidaat-houder van het Certificaat, zijn paspoort of ieder gelijkwaardig officieel document. De kopie moet worden ondertekend door de kandidaat-Certificaathouder;
- de elektronische aanvraag van het Certificaat op diskette (optie indien de Sleutels niet worden aangemaakt door de Certificatiedienstverlener).
- een kopie (recto/verso) van de geldige en officiële identiteitskaart van de wettelijke vertegenwoordiger van de Onderneming (of Organisatie) of van zijn gemachtigde afgevaardigde, van zijn paspoort of van ieder gelijkwaardig officieel document. De kopie dient ondertekend te zijn door de wettelijke vertegenwoordiger van de Onderneming (of Organisatie) of door zijn gemachtigde afgevaardigde;
- een kopie van de officiële huidige statuten van de Onderneming (of Organisatie);
- indien een gemachtigde afgevaardigde van een wettelijke vertegenwoordiger de bestelbon heeft ondertekend (versie Werknemers), dient de kandidaat-houder van het Certificaat het bewijs te leveren dat deze persoon gemachtigd is te ondertekenen voor de wettelijke vertegenwoordiger.

b. Voor de zelfstandigen/privé-personen :

- De behoorlijk ingevulde en ondertekende Bestelbon;
- een kopie (recto/verso) van de geldige en officiële identiteitskaart van de kandidaat-Certificaathouder, zijn paspoort of ieder gelijkwaardig officieel document. De kopie moet worden ondertekend door de kandidaat-Certificaathouder;
- de elektronische aanvraag van het Certificaat op diskette (optie indien de Sleutels niet worden aangemaakt door de CSP).

Wanneer de kandidaat-Certificaathouder het professionele gedeelte van het Certificaat wil laten certificeren als zelfstandige :

- een bewijs van zijn beroepsstatuut : namelijk een uittreksel uit het Handelsregister of iedere ander gelijkwaardig officieel document alsook de desbetreffende uittreksels van de bijlagen bij het Belgisch Staatsblad of ieder ander gelijkwaardig document, of een bewijs dat hij behoort tot een welbepaalde organisatie of een bewijs van de uitoefening van een beroep.

c. Bestuurder/zaakvoerders :

- De behoorlijk ingevulde en ondertekende Bestelbon
- een kopie (recto/verso) van de geldige en officiële identiteitskaart van de kandidaat-Certificaathouder, zijn paspoort of ieder gelijkwaardig officieel document. De kopie moet worden ondertekend door de kandidaat-Certificaathouder;
- de elektronische aanvraag van het Certificaat op diskette (optie indien de Sleutels niet worden aangemaakt door de LRAO).

Deel		Ref. RFC 2527
	– een kopie van de huidige officiële statuten van de Onderneming/Organisatie of, bij gebrek aan statuten, een uittreksel uit het Handelsregister of ieder ander gelijkwaardig officieel document alsook de desbetreffende uittreksels van de bijlagen bij het Belgisch Staatsblad of ieder ander gelijkwaardig document. 4. Indien de klant beschikt over een MyCertipost account, faxt hij zijn dossier naar +32 2 209 99 02. 5. Indien de klant niet beschikt over een MyCertipost account, maakt hij een afspraak met de LRA operator bij de LRA van zijn keuze, geaccrediteerd in de context van deze CP. (zie sectie D.1§5). 6. Indien de klant niet beschikt over een MyCertipost account, gebeurt een registratie en validatie bij de Lokale Registratie-autoriteit (LRA). De klant biedt zich aan in persoon bij de LRA, met wie hij een afspraak maakt, met de documenten, zoals gespecificeerd hierboven. De LRA-operator (LRAO) controleert de ontvangen documenten en gaat over tot de verificatie : • van de identiteit van de kandidaat-Certificaathouder op basis van het origineel van zijn geldige identiteitsbewijs; • op basis van de door de kandidaat-Certificaathouder verstrekte stukken, van de vermeldingen die moeten worden gecertificeerd met betrekking tot de professionele hoedanigheid van de vooraf geïdentificeerde kandidaat-Certificaathouder. Indien de aanvraag gevalideerd is, dient de LRAO de ingewonnen documenten te verzamelen om het Registratiedossier van de Certificaathouder samen te stellen, er op veilige wijze een kopie van te archiveren en het origineel ervan voor te bereiden om veilig te worden gestuurd naar en gearchiveerd bij de Certificatiedienstverlener. 7. Validatie Indien de LRA niet rechtstreeks in verbinding staat met de Certificatiediensten van de Certificatiedienstverlener, bij het verzamelen van enerzijds het Registratiedossier van de Kandidaathouder van het Certificaat ontvangen van de LRAO, en desgevallend, anderzijds van de door de Klant verstuurde elektronische aanvraag van het Certificaat, voert de officier van de Centrale Registratie-autoriteit (Central Registration Authority – CRA) een definitieve verificatie van de validatie uit : nauwkeurigheid van de informatie verstrekt in het Registratiedossier van de Klant dat van de LRAO werd ontvangen, telefonisch contact met de kandidaat-houder van het Certificaat. Wanneer ze door de CRAO wordt aanvaard, wordt de elektronische aanvraag van het Certificaat naar de Certificatie-autoriteit van de Certificatiedienstverlener gestuurd voor de uitgifte van het Certificaat. Wanneer de aanvraag voor het Certificaat wordt verworpen door de CRAO, dient deze laatste de kandidaat-houder van het Certificaat hierover te informeren en de motieven ervoor te melden. 8. Verificatie a posteriori Een tweede verificatie van het dossier wordt a posteriori uitgevoerd door de Certification Authority Auditor (CAA) van de Certificatiedienstverlener, die de samenhang tussen de uitgegeven Certificaten en de van de LRA's ontvangen dossiers verifieert.	

Deel		*Ref. RFC 2527*
H	***Uitgifte van het Certificaat en levering***	**4.2**
	In het geval van de aanvraag via een beveiligde myCertipost account : Bij ontvangst van een door het myCertipost platform gevalideerde certificaat-aanvraag, zal de certificatie-authoriteit van de Certificatiedienstverlener het digitale Certificaat uitgeven en aan de Certificaathouder bezorgen. Het Certificaat wordt gepubliceerd in overeenstemming met deel I van dit document. ***In alle andere gevallen :*** Bij ontvangst van de aanvraag voor een Certificaat via fax, zal de Certificatie-autoriteit van de Certificatiedienstverlener het Certificaat aanmaken. Het Certificaat wordt gepubliceerd in overeenstemming met deel I van het onderhavige document. De houder van het Certificaat zal zijn Certificaat of de nodige informatie om zijn Certificaat te bekomen, ontvangen, evenals het benodigde paswoord om toegang te krijgen tot zijn private sleutel. Het Certificaat, met private sleutel, wordt op beveiligde manier aan de LRA bezorgd, of aan de kandidaatCertificaathouder, indien deze over een MyCertipost account beschikt, via zijn beveiligde MyCertipost account. Wanneer de sleutels op een gecentraliseerde wijze aangemaakt worden door de CRAO wordt het certificaat onmiddellijk opgeschort tot dat de procedure voor persoonlijke overhandiging van het Sleutelpaar door de LRA en het bijhorende Certificaat met bijhorende validatie beëindigd is en bevestigd is aan de CRA door de LRA, via een ontvangstbewijs, getekend door de titularis van het Certificaat. Op dat moment wordt het Certificaat weer hersteld door de CRA.	
I	***Aanvaarding van het Certificaat en Publicatie van het Certificaat***	**4.3**
	Publicatie van het Certificaat in het Openbaar Certificatenregister van de Certificatiedienstverlener. Eens het Certificaat is uitgegeven door de Certificatiedienstverlener, wordt het onmiddellijk gepubliceerd in het Openbaar Certificatenregister van de Certificatiedienstverlener. Dit Register is openbaar en permanent toegankelijk. *Aanvaarding* • De Certificaathouder aanvaardt dat zijn Digitale Certificaat onmiddellijk na de creatie ervan in het Openbaar Certificatieregister (Certificate Public Registry) van de Certificatiedienstverlener wordt gepubliceerd. • Het Certificaat wordt geacht aanvaard te zijn door de houder van het Certificaat zodra het eerste van van de volgende gebeurtenissen zich voordoet: hetzij vanaf de 8e dag na de publicatie ervan in het Openbaar Certificatieregister van de Certificatiedienstverlener, hetzij vanaf het ogenblik van het eerste gebruik ervan door de houder van het Certificaat. Tijdens de voormelde periode is de houder van het Certificaat verantwoordelijk voor de controle van de juistheid van de inhoud van zijn gepubliceerde Certificaat. Indien de Certificaathouder enige incoherentie vaststelt tussen de informatie van het contractuele akkoord en de inhoud van zijn Certificaat, dient hij de Certificatiedienstverlener daarvan onverwijld op de hoogte te stellen. De Certificatiedienstverlener zal in dat geval het Certificaat herroepen en de gepaste maatregelen nemen om een nieuw Certificaat uit te geven. Dit is de enige mogelijkheid m.b.t. de niet-aanvaarding van het Certificaat.	
J	**Procedure voor Schorsing/Herstel na schorsing/Herroeping**	**4.4**
	De Certificaathouder, de wettelijke vertegenwoordiger (of zijn gemachtigde afgevaardigde)	

Deel		Ref. RFC 2527
	van de Organisatie in het geval van werknemers, de LRA of Certipost kunnen de schorsing, het herstel na schorsing of de herroeping van het Certificaat aanvragen. De houder van een Certificaat, en indien toepasselijk de wettelijke vertegenwoordiger (of zijn gemachtigde afgevaardigde) dienen van de schorsing, het herstel na schorsing of de herroeping van het Certificaat op de hoogte te worden gesteld. De informatie betreffende de status van de schorsing of herroeping van een Certificaat wordt ten allen tijde ter beschikking van allen gesteld door de Certificatiedienstverlener, zoals aangegeven in deel D1, § 5 van het onderhavige document. Een formulier van schorsing/herstel na schorsing/herroeping wordt ter beschikking van de partijen gesteld door de Certificatiedienstverlener. De aanvragen en verslagen betreffende een schorsing, een herstel na schorsing of een herroeping zullen worden behandeld zodra ze worden ontvangen en zullen als volgt worden geauthenticeerd en bevestigd : Ingeval van **schorsing** : • De aanvrager dient de Schorsings- en Herroepingsautoriteit (Suspension Revocation Authority – SRA) van de Certificatiedienstverlener die het Certificaat waarop de aanvraag slaat, heeft uitgegeven, op de hoogte te brengen. • De SRA zal overgaan tot een call back om de bevestiging te bekomen van de vraag om schorsing. • De SRA zal het Certificaat daadwerkelijk schorsen vanaf de ontvangst van de aanvraag. Het formulier dient binnen de 14 werkdagen per fax of met de post naar de Certificatiedienstverlener te worden gestuurd, zoniet zal het Certificaat worden hersteld. • De schorsing van een Certificaat zal een termijn van één (1) maand hebben. Na deze periode dient een nieuwe aanvraag om schorsing te worden ingediend om de schorsingsperiode met één (1) maand te verlengen. Zoniet zal het Certificaat automatisch worden herroepen. Ingeval van **herstel na schorsing** : • De aanvrager dient contact op te nemen met de Schorsings- en Herroepingsautoriteit (Suspension Revocation Authority – SRA) van de Certificatiedienstverlener die het Certificaat waarop de aanvraag slaat, heeft uitgegeven om te vragen een formulier te ontvangen voor de aanvraag van een herstel na schorsing van een Certificaat of het formulier in bijlage bij de Algemene Voorwaarden te gebruiken. • De aanvrager dient een afspraak te maken met een door de Certificatiedienstverlener erkende Lokale Registratie-autoriteit en zich met het behoorlijk ingevulde formulier en het ondertekende afschrift (recto/verso) van zijn identiteitskaart aan te melden. • De Officier van de Lokale Registratie-autoriteit zal de verstrekte documenten en de identiteit van de aanvrager verifiëren. Indien het verzoek wordt gevalideerd, zal de Officier de aanvraag naar de SRA doorsturen. • De SRA zal het Certificaat binnen de 24 uur, te rekenen vanaf de ontvangst van de aanvraag, herstellen. Ingeval van een **herroeping** moet : • de aanvrager de schorsing van het Certificaat (zie hierboven) aanvragen; • de aanvrager contact opnemen met de SRA om een aanvraagformulier voor herroeping van het Certificaat te bekomen of het formulier in bijlage bij de Algemene Voorwaarden gebruiken. • de aanvrager een afspraak maken met een door de Certificatiedienstverlener erkende Lokale Registratie-autoriteit en zich met het behoorlijk ingevulde formulier en het ondertekende afschrift (recto/verso) van zijn identiteitskaart aanmelden;	

Deel		Ref. RFC 2527
	• de Officier van de Lokale Registratie-autoriteit de verstrekte documenten en de identiteit van de aanvrager verifiëren; indien het verzoek wordt gevalideerd, moet de Officier de aanvraag naar de SRA doorsturen; De SRA herroept het Certificaat bij ontvangst van de aanvraag tot herroeping. • Het certificaat moet worden herroepen (of hersteld) na een onderzoeksperiode van maximum 10 werkdagen ; • **De herroeping van een certificaat is definitief.**	
K	***Procedure voor de vernieuwing van de Sleutels en van het Certificaat***	
	De Certificatiedienstverlener vergewist zich ervan dat de aanvragen ingediend door de houder van een Certificaat dat reeds eerder geldig werd geregistreerd volledig, geldig en toegestaan zijn. Dit houdt de vernieuwing van het Certificaat en/of de Sleutels in na een herroeping of ten gevolge van de naderende vervaldag of ten gevolge van een wijziging in de gecertificeerde gegevens. De Certificatiedienstverlener vergewist zich ervan dat : • de informatie die wordt gebruikt om de identiteit van de klant-houder van het Certificaat te verifiëren nog steeds geldig is en daartoe : – wordt dezelfde procedure als voor de aanvankelijke registratie voorzien (cf. punt G van de onderhavige CP) OF – dient, ingeval van een vernieuwing en voor zover de Sleutels en het Certificaat van de houder van het Certificaat nog steeds geldig zijn (niet herroepen, geschorst of vervallen), de Certificatiedienstverlener een aanvraag te aanvaarden die elektronisch is ondertekend aan de hand van een Private Sleutel waarvan de Publieke Sleutel is gecertificeerd en vergezeld van een tekst, die eveneens behoorlijk elektronisch ondertekend is, waarin wordt bepaald dat geen enkele informatie van het dossier gewijzigd is sinds de vorige aanvraag, voor zover de key usage van het betreffende certificaat de handtekening toestaat. • Indien de algemene voorwaarden van de Certificatiedienstverlener gewijzigd zijn, zal de Certificatiedienstverlener dit meedelen aan de klant-houder van het Certificaat. • De Certificatiedienstverlener zal slechts een Certificaat uitgeven voor een eerder gecertificeerde Sleutel indien de beveiliging van de cryptografische parameters betreffende deze Sleutel nog steeds voldoende is en de Sleutel in kwestie niet werd gecompromitteerd.	
L	***Bescherming van de persoonlijke levenssfeer en van de persoonsgegevens***	
	De persoonsgegevens die door de aanvrager meegedeeld worden aan Certipost of Belgacom, worden opgenomen in een bestand van Certipost N.V. (Willebroekkaai, 22, B-1000 Brussel) en indien nodig in het bestand van de betrokken LRA. De gegevens worden uitsluitend gebruikt om de Certipost-diensten te kunnen leveren. De klant beschikt over een recht van toegang en verbetering.	
M	***Klachten en regeling van geschillen***	
	• In geval van technische problemen die betrekking hebben op het Certificaat en in geval van klachten die betrekking hebben op de diensten geleverd op basis van de onderhavige Certificaatpolicy, kan de Certificaathouder contact opnemen met de helpdesk van de Certificatiedienstverlener: - Certipost E-Trust: - Telefoonnummer : 070/22 55 33 - Faxnummer : 070/22 55 01 - E-mail : feedback.nl@contact.certipost.be	

Deel		*Ref. RFC 2527*
	De Certificatiedienstverlener en de Certificaathouder verbinden zich ertoe alles in het werk te stellen om een minnelijke schikking te vinden voor alle geschillen betreffende de geldigheid, de interpretatie of de uitvoering van de overeenkomst die hen bindt. Indien geen minnelijke schikking kan worden gevonden, zal het geschil betreffende de geldigheid, de interpretatie of de uitvoering van de overeenkomst die hen bindt, voor de rechtbanken van Brussel worden gebracht.	