Certificaatpolicy betreffende het Genormaliseerde E-Trust Code Signing Certificaat

Versie 1.0

Datum van publicatie : Januari 2004

Certificaatpolicy (Certificate Policy - CP) betreffende het Genormaliseerde E-Trust Code Signing Certificaat

Dit document beschrijft de toepasbaarheid van de certificaten van het type Genormaliseerd E-Trust Code Signing 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 het Genormaliseerd E-Trust Certificaat voor Code Signing die voldoet aan de volgende voorwaarden :

Deel		*Ref. RFC 2527*
A	***Overzicht van de Genormaliseerde E-Trust Code Signing Certificaatpolicy***	**1.1**
	Dit type van Certificaat verzekert op hoog niveau de elektronische identiteit van een Organisatie. Het garandeert een correcte authentificatie daar de Klant persoonlijk aanwezig moet zijn tijdens de registratie van zijn/haar aanvraag door een Lokale Registratie Autoriteit (LRA). De Klant is ofwel de wettelijke vertegenwoordiger van het Bedrijf (de Organisatie) dat verantwoordelijk is voor het electronisch handtekenen van Software Code ofwel zijn gemachtigde afvaardigde. De band tussen de Organisatie en zijn publieke sleutel wordt gecertifieerd. Dit Certificaat levert de hoogste zekerheidsgraad van een correcte authenticatie daar de kandidaat voor het bekomen van het Certificaat zich 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 Code Signing Certificaat door de Certificatiedienstverlener. De validering van de aanvraag vereist de voorlegging van het identiteitsbewijs van de aanvrager 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 het kader van de electronische ondertekening van Software Code door het Bedrijf (de Organisatie). Het Certificaat voldoet eveneens 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 gecertificeerd in overeenstemming hiermee (zie deel D1, § 5 van het onderhavige document).	
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	

Deel		Ref. RFC 2527
	toepasbaarheidsklasse met gemeenschappelijke vereisten inzake veiligheid. Het onderhavige document bevat en identificeert de **Genormaliseerde E-Trust Certificaatpolicy voor Code Signing.** Het Sleutelpaar wordt steeds gegenereerd door de houder van het Certificaat. Deze Certificaten zijn in overeenstemming met en voldoen aan de vereisten geformuleerd in de technische norm ETSI 102 042. De Certificaten uitgegeven in overeenstemming met de onderhavige CP "Genormaliseerd E-Trust Certificaat voor Code Signing" bevat een Certificaatpolicy identificatiefactor die door derden kan gebruikt worden om de toepasbaarheid en de betrouwbaarheid van het Certificaat ten opzichte van een bepaalde applicatie te bepalen. Deze identificatiefactor is 0.3.2062.7.1.1.2.1.	
C	***Toepasbaarheid***	**1.3.4**
	• Dit type van Certificaat verzekert de elektronische identiteit van een Organisatie. Het kan gebruikt worden voor het beveiligen van software code, zoals JAVA applets en ActiveX code. • 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 "het digitaal handtekenen van software code". • De Genormaliseerde Certificaten voor Code Signing, uitgegeven in het kader van deze CP voldoen aan de vereisten van de technische standaard ETSI 102 042.	
D	***Rechten, verantwoordelijkheden en verplichtingen***	***2***
D.1	***Rechten, verantwoordelijkheden en verplichtingen van de Certificatiedienstverlener***	**2.1**
	• De Certificatiedienstverlener zal Certificaten die voldoen aan de standaarden X.509v3 (ISO 9594-8) afleveren. • De Certificatiedienstverlener geeft de Genormaliseerde Certificaten uit onder het label "Normalised 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 Certificaatpolicies (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 : - **Certipost nv** 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	

[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
	- *Openbaar Repertorium van de Digitale Certificaten en CRL :* www.e-trust.be/en/x500 - *Conformiteitsverklaring :* www.e-trust.be/CPS/QNcerts - *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) : - De 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 aanvaard zijn om de registratie te kunnen vervullen van de MyCertipost gebruikers. Deze lijst is beschikbaar op www.e-trust.be/CPS/QNcerts. • 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 kandidaat-houder via de aangewezen kanalen verwittigt en op de hoogte stelt). • 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 bestanden. De gegevens zullen enkel worden gebruikt voor de levering van Certificatiediensten. Het bedrijf/de organisatie, verantwoordelijk voor 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. 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	

Deel		Ref. RFC 2527

	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.
	• De Certificaathouder is verantwoordelijk voor de aanmaak van de Sleutelpaar en zal dit aanmaken in overeenstemming met de Certificaatpolicy, 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. 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 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.	

Deel		Ref. RFC 2527
	• 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 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 in 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	

Deel		Ref. RFC 2527
	(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. – De door de registratieofficier gebruikte valideringsprocedure voor de elektronische aanvraag van het Certificaat waarborgt 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 : • 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 Onderneming (of de Organisatie) van de houder van het Certificaat***	
	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.	

<table>
<tr><td>Deel</td><td></td><td>Ref. RFC 2527</td></tr>
<tr><td></td><td>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 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><td>Attribuut</td><td>Verplicht /Optioneel/Vast</td><td>Waarde</td></tr>
<tr><td colspan="3">Distinguished Name :</td></tr>
<tr><td>Country (C)</td><td>Verplicht</td><td>Land van de sociale zetel van het bedrijf (zoals vermeld in de statuten)</td></tr>
</table></td><td></td></tr>
</table>

Deel				Ref. RFC 2527
	Locality (L)	Verplicht	Plaats van de sociale zetel van het bedrijf (zoals vermeld in de statuten)	
	Organisation (O)	Verplicht	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.	
	Organisational Unit (OU)	Optioneel	Organisatie-eenheid of departement	
	Common Name (CN)	Verplicht	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.	
	Rfc822Name	Verplicht	E-mailadres van de Certificaathouder	
	Extensies :(non-critical behalve indien anders vermeld)			
	KeyUsage	Vast/Critical	"Digital Signature"	
	SubjectPublicKey	Verplicht	Publieke sleutel: 1024 bits of 2048 bits (RSA); publieke exponent: Fermat-4 (=010001)	
	CertificatePolicies-policyIdentifier	Vast	0.3.2062.7.1.1.2.1	
	CertificatePolicies-policyQualifier-userNotice	Vast	"E-Trust Certificate for Code Signing Certificate. General conditions O.I.D.: 0.3.2062.7.1.2.2.1"	
	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	Code Signing	
	Other information:			
	Issuer	Vast	"CN = Certipost E-Trust Primary CA for Normalised certificates O = Certipost C = BE"	
	Validity	Vast	1 jaar, 2 jaar of 3 jaar (zoals vermeld op de bestelbon)	
	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 dient 1024 of 2048 bits te zijn. ***Aanmaak van de Sleutels door de houder van het Certificaat*** De kandidaat-houder van het Certificaat maakt zelf zijn Sleutelpaar aan. In dat geval dient hij :			

Deel		Ref. RFC 2527
	• 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 beveiligde electronische aanvraag door te sturen, binnen zijn beveiligde myCertipost omgeving.	
G	***Procedure voor de aanvraag van het Certificaat***	
	In het geval van de aanvraag via een beveiligde MyCertipost account : 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 zich hierbij te registreren als zelfstandige of rechtspersoon. Hij dient hierbij zijn MyCertipost contract af te drukken en te ondertekenen, en zich persoonlijk aan te melden bij een aanvaard MyCertipost registratiekantoor. Door het myCertipost contract te ondertekenen, aanvaardt de onderneming (of organisatie) 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. Hiervoor dient hij de bestelbon (de correcte up-to-date versie van deze bestelbon bevindt zich steeds op http://www.e-trust.be/CPS/QNCerts) correct in te vullen en correct te handtekenen. Deze bestelbon zal de certificatie mogelijk maken van die gegevens dewelke geverifieerd worden, zowel tijdens de registratie voor een myCertipost account met uitzondering van het e-mail adres, wat vrij kan ingevuld worden, als na ontvangst van de electronische certificaatsaanvraag (cfr stap 3)(er wordt met name geverifieerd door de Centrale Registratie Authoriteit of de URL('s) toebehoren aan het bedrijf dat de aanvraag heeft ingediend). Tijdens deze procedure, aanvaardt de kandidaat-Certificaathouder de Algemene Voorwaarden, de CP en het CPS van kracht. Deze documenten en de electronische certificaatsaanvraag vormen samen de Conventie. 3. De kandidaat-Certificaathouder faxt of stuurt per post de correct ingevulde en ondertekende bestelbon naar de Certipost E-Trust Centrale Registratie Authoriteit. De coordinaten van de Centrale Registratie Autoriteit zijn beschikbaar via http://www.e-trust.be/CPS/QNCerts. 4. De kandidaat-Certificaathouder stuurt binnen zijn beveiligde MyCertipost omgeving zijn electronische certificaatsaanvraag in pkcs#10 formaat naar de Certipost E-Trust Centrale Registratie Authoriteit. 5. De Certipost E-Trust Centrale Registratie Authoriteit verifieert de electronische certificaatsaanvraag en de bestelbon. De Certipost E-Trust Centrale Registratie Authoriteit verifieert of de URL's die aangevraagd worden ter certificatie wel degelijk toebehoren aan het bedrijf/de organisatie die deze aanvraagt. **Validatie** Een validatie wordt uitgevoerd 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 en van de de CRA's. ***In alle andere gevallen :*** 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	

Deel		Ref. RFC 2527
	post of deze documenten te bekomen van een Lokale Registratie-autoriteit (Local Registration Authority – LRA) die werd erkend door de Certificatiedienstverlener. De correcte versie van deze documenten bevindt zich op http://www.e-trust.be/CPS/QNCerts De kandidaat-Certificaathouder dient de Bestelbon behoorlijk in te vullen en te ondertekenen. De Bestelbon bestaat uit twee delen : a. Het gedeelte "Requestor" dient behoorlijk te worden ingevuld en ondertekend door de aanvrager van het Code Signing Certificaat; b. Het gedeelte "Organisation" dient behoorlijk te worden ingevuld en ondertekend door 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. 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. • 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 • 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, dient de kandidaat-houder van het Certificaat het bewijs te leveren dat deze persoon gemachtigd is te ondertekenen voor de wettelijke vertegenwoordiger. De klant maakt een afspraak met de LRA operator bij de LRA van zijn keuze, geaccrediteerd in de context van deze CP. (zie sectie D.1§5). **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 volgende documenten : 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 ownership van de te certificeren URL's.	

Deel		Ref. RFC 2527
	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. **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 enerzijds, en van de door de Klant verstuurde elektronische aanvraag van het Certificaat anderzijds, 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. Indien de LRA rechtstreeks in verbinding staat met de Certificatiediensten gebeurt de tweede verificatie van het dossier a posteriori door de Auditeur van de Certificatie-autoriteit (Certification Authority Auditor -- CAA) van de Certificatiedienstverlener, die de samenhang tussen de uitgegeven Certificaten en de van de LRA ontvangen dossiers verifieert. **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.	
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 :*** De CRA zal het Certificaat sturen via e-mail naar de Certificaathouder. Indien de LRA rechtstreeks in verbinding staat met de Certificatiediensten, zal de LRA het Certificaat bezorgen aan de Certificaathouder op een diskette. Het Certificaat wordt gepubliceerd in overeenstemming met deel I van dit document.	
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	

Deel		Ref. RFC 2527
	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 de Certificaathouder terug te betalen of 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) 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** :	

Deel		Ref. RFC 2527
	• 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; • 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	

Deel		Ref. RFC 2527
	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, worden opgenomen in een bestand van Certipost N.V. (Muntcentrum, 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 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.	