

Certificaatpolicy betreffende het Gekwalificeerde of Genormaliseerde E-Trust-certificaat

Versie 4.0

—

OUTDATED

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 Certificaten die voldoet aan de volgende voorwaarden en aan het document "Controleprocedures van de Certificatiedienstverlener". Het gaat om een Certificaatpolicy betreffende de Gekwalificeerde of Genormaliseerde Certificaten die voldoet aan de volgende voorwaarden :

Deel		Ref. RFC 2527
A	Overzicht van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy	1.1
	<p>Zeer hoge graad van zekerheid inzake de persoonlijke en eventueel professionele elektronische identiteit van de houder van het Certificaat. Het gaat om een Certificaat dat slechts wordt afgeleverd indien men zich persoonlijk aanbiedt tijdens het registratieproces. Dit Certificaat levert een zeer hoog zekerheidsniveau in verband met de link tussen de persoonlijke identiteit van de houder van het Certificaat, een eventuele professionele hoedanigheid (niet-verplicht), een publieke sleutel en het toegestane gebruik ervan.</p> <p>Dit Certificaat levert de hoogste zekerheidsgraad van een correcte authenticatie daar de kandidaat voor het bekomen van het Certificaat :</p> <ul style="list-style-type: none"> – 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 voorafgaandelijk moet beschikken over een Certificaat van een gelijkwaardig niveau om de aanvraag op een geldige manier te kunnen indienen. <p>De validering 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.</p> <p>De aldus gecertificeerde publieke sleutel kan uitsluitend worden gebruikt in een van de volgende twee gevallen :</p> <ul style="list-style-type: none"> – in het kader van een gekwalificeerde 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 certificatediensten (cf. wet van 9 juli 2001) en de technische standaard ETSI 101 456, of (exclusief); – in het kader van versleuteling en/of authenticatie ; in dat geval beantwoordt het Certificaat aan het criterium van een Genormaliseerd Certificaat in de zin van de technische standaard ETSI 102 042. 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>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).</p> <p>De Certificaten (en de Sleutelparen) die worden gebruikt voor de digitale handtekening zijn steeds verschillend van de Genormaliseerde Certificaten ..</p>	
B	Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy	
	<p>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.</p> <p>Het onderhavige document bevat en identificeert binnen dezelfde globale Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy verschillende Certificaatpolicy's 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 is gegenereerd geweest en slechts mag worden gebruikt in een Veilig Middel voor het Aanmaken van een Handtekening (Secure Signature Creation Device – SSCD) of niet.</p> <p>Daaruit vloeien twee grote types Certificaten voort. Enerzijds, de Gekwalificeerde Certificaten, waarvan het gebruik strikt is voorbehouden voor de gekwalificeerde 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 (cf. wet van 9 juli 2001).</p> <p>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), 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.</p> <p>De Certificaten uitgegeven in overeenstemming met de onderhavige 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.</p> <p>De identificatiefactoren voor de Gekwalificeerde of Genormaliseerde E-Trust-certificaatpolicy's gespecificeerd in dit document, zijn opgenomen in Tabel 1 hieronder.</p>	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<div><div><div><div><div></div><div>Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.2.4</div></div><div><div>Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : 0.4.0.1456.1.1 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.3.4</div><div>Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.4.4</div></div></div><div><div><div></div><div>Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.6.4</div></div><div><div>Genormaliseerd Certificaat met SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.7.4</div><div>Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.8.4</div></div></div></div><div><div>Tabel 1. Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust-certificaatpolicy (CSP = Certification Service Provider)</div></div></div>	
C	Toepasbaarheid	1.3.4
	<div><div><ul style="list-style-type: none">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 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 certificatediensten (cf. 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 certificatediensten (cf. 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</div></div>	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>vervat 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.</p> <ul style="list-style-type: none"> 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 certificatediensten (cf. 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
	<ul style="list-style-type: none"> De Certificatiedienstverlener zal Certificaten die voldoen aan de standaarden X.509v3 (ISO 9594-8) afleveren. 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 certificatediensten (cf. wet van 9 juli 2001), en de technische standaard ETSI 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: <ul style="list-style-type: none"> Belgacom E-Trust via de Belgacom E-Trust Primary CA for Qualified Certificates voor de uitgifte van Gekwalificeerde Certificaten en via de Belgacom E-Trust Primary CA for Normalised Certificates voor de uitgifte van Genormaliseerde Certificaten: <i>Bepalingen van de Certificatie-activiteiten (CPS)</i> : www.e-trust.be/CPS/QNCerts <i>Openbaar Repertorium van de Digitale Certificaten en CRL</i> : www.e-trust.be/en/x500 <i>Conformiteitsverklaring</i> : www.e-trust.be/CPS/QNCerts <i>Opschorting en revocatie autoriteit</i> : 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) : 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<ul style="list-style-type: none"> - Het secretariaat van de Ordre français des avocats du barreau de Bruxelles vertegenwoordigd door de personen op de geauthenticeerde lijst beschikbaar op www.e-trust.be/CPS/Ofbb. - De advocaten die door de voormelde Certificatiedienstverlener gemachtigd zijn als registratie-autoriteiten en als afgevaardigden van de Ordre français des avocats du barreau de Bruxelles. De geauthenticeerde lijst van deze gemachtigde advocaten is beschikbaar op www.e-trust.be/CPS/Ofbb. - De Teleshops en personeelsleden van Belgacom die door de voormelde Certificatiedienstverlener gemachtigd zijn als registratie-autoriteiten. De geauthenticeerde lijst van deze gemachtigde Teleshops is beschikbaar op www.e-trust.be/CPS/QNcerts. - De postkantoren en andere lokale registratie autoriteiten dewelke geaccrediteerd zijn om de registratie te kunnen vervullen van de Certipost gebruikers. Deze lijst is beschikbaar op www.e-trust.be/CPS/QNcerts. <ul style="list-style-type: none"> • 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/schors (mits de Certificatiedienstverlener de advocaat-houder 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 certificatediensten (cf. 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 certificatediensten (cf. 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 bestanden. De gegevens zullen enkel worden gebruikt voor de levering van Certificatediensten. De klant-houder van het Certificaat heeft het recht deze 	

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 Certificatediensten. De titularis van deze gegevens heeft het recht deze te raadplegen en de rechtzetting of

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>gegevens 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.</p> <ul style="list-style-type: none"> 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
	<p>De houder van het Certificaat 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.</p> <p>In het bijzonder stemt de houder van het Certificaat in met het volgende :</p> <ul style="list-style-type: none"> Het contractuele akkoord met betrekking tot dit type van Certificaat wordt geregeld door het Belgische recht. De kandidaat-houder van het Certificaat 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 het onderhavige 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 houder van het Certificaat 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-houder van het Certificaat 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 certificatie-diensten (cf. wet van 9 juli 2001), en in het document ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates". Bovendien waarborgt de houder van het Certificaat 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 houder van het Certificaat 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 	

desgevallend de afschaffing ervan te vragen.

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>houder van het Certificaat 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 het voorwerp te zijn van een voldoende beveiliging. 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 de houder van het Certificaat.</p> <ul style="list-style-type: none"> De houder van het Certificaat 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 : <ul style="list-style-type: none"> de Private Sleutel van de houder van het Certificaat werd verloren, gestolen of potentieel gecompromitteerd; of de houder van het Certificaat 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 houder van het Certificaat 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-houder van het Certificaat 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 houder van het Certificaat 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 houder van het Certificaat 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 vanaf de 7e 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 houder van het Certificaat. Tijdens de voormede periode is de houder van het Certificaat verantwoordelijk voor de controle van de juistheid van de inhoud van zijn gepubliceerde Certificaat. Indien de houder van het Certificaat 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. De houder van het Certificaat aanvaardt hierdoor volledig vergoed te zijn voor de niet-aanvaarding. De houder van het Certificaat aanvaardt de bewaring gedurende een periode van 30 jaar 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 houder van het Certificaat aanvaardt de rechten, plichten en verantwoordelijkheden 	

VALIDITY: 21/02/2003-31/10/2003

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)	
	<p>De Lokale Registratie-autoriteit (LRA) is contractueel verplicht strikt de registratieprocedures beschreven in de Bepalingen van de Certificatie-activiteiten (CPS) van de Certificatiedienstverlener te respecteren (zie deel D.1, § 5).</p> <p>De LRA waarborgt :</p> <ul style="list-style-type: none"> – dat de houders van een Certificaat correct worden geïdentificeerd en geauthenticeerd, zowel wat de persoonlijke identiteit van de houder van het Certificaat als natuurlijk persoon betreft als wat de eventuele vermeldingen betreffende de beroepshoedanigheid van deze betreft ; – dat de Certificaataanvragen die naar de Certificatiedienstverlener worden gestuurd ingevuld, correct, geldig en degelijk toegestaan zijn. <p>Meer bepaald :</p> <ul style="list-style-type: none"> – De registratieofficier informeert de houder van het Certificaat over de algemene 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 registratieofficier verifieert de identiteit van de houder van het Certificaat 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 registratieofficier 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 houder van het Certificaat verenigd is met een rechtspersoon, dient een bewijs van deze vereniging te worden gevalideerd door de registratieofficier. – De registratieofficier zal een kopie van de informatie die bij de registratieprocedure werd verstrekt door de houder van het Certificaat en die volledig naar de Certificatiedienstverlener werd gestuurd, archiveren, inzonderheid : <ul style="list-style-type: none"> – een kopie van alle informatie die werd gebruikt om de identiteit en de eventuele vermeldingen inzake de professionele hoedanigheid van de titularis van het Certificaat 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 houder van het Certificaat, met inbegrip van zijn akkoord met het geheel van zijn verplichtingen. <p>Deze informatie wordt gedurende een periode van 30 jaar bewaard.</p> <ul style="list-style-type: none"> – 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. <p>De LRA is contractueel verplicht de precieze en geschikte maatregelen te treffen aangaande :</p> <ul style="list-style-type: none"> • de fysieke beveiliging van de informatie en, desgevallend, van de systemen; 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<ul style="list-style-type: none"> • de logische toegang tot de eventuele software; • het personeel dat belast is met de registratie. <p>De klassering van de gegevens en de verantwoordelijkheid voor deze gegevens zijn van essentieel belang. Worden hier bedoeld :</p> <ul style="list-style-type: none"> • 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 fysieke toegang tot de gegevens (gebouwen, kluizen, toegangscontrole en voorwaardelijke toegang tot de software, ...). <p>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.</p>	
D.4	Rechten, verantwoordelijkheden en verplichtingen van de houder van het Certificaat als zelfstandige (indien van toepassing)	
	<p>De houder van het Certificaat zal, als zelfstandige :</p> <ul style="list-style-type: none"> • de verplichtingen, rechten en verantwoordelijkheden van de houder van het Certificaat zoals hierboven vermeld (deel D.2) respecteren; • verantwoordelijk zijn voor de voorlegging van het bewijs van zijn statuut van zelfstandige of zijn beroepsstatuut aan de LRA op het ogenblik van de registratie; • waarborgen dat het bewijs van zijn situatie als zelfstandige of van zijn beroepsstatuut 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)	
	<p>De Onderneming (of de Organisatie), vertegenwoordigd door zijn wettelijke vertegenwoordiger, keurt de registratie van de houder van het Certificaat goed in het kader van de bekoming van het Certificaat, waarbij een professionele hoedanigheid moet worden gecertificeerd waarbij de Onderneming (of de Organisatie) betrokken is.</p> <p>De Onderneming (of Organisatie) gaat akkoord met :</p> <ul style="list-style-type: none"> • het geldende <u>Certification Practice Statement</u> (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 <u>Certificate Policy</u> (CP) van het Gekwalificeerde of Genormaliseerde E-Trust-certificaat. <p>De Onderneming (of Organisatie) gaat met name akkoord met het volgende :</p> <ul style="list-style-type: none"> • De Overeenkomst tussen de Onderneming (of de Organisatie), de houder van het Certificaat en de Certificatiedienstverlener wordt geregeld door het 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 nauwkeurigheid van de gegevens die door de Onderneming (of de Organisatie) naar de Certificatiedienstverlener worden gestuurd in het kader van de registratie van de houder van het Certificaat. 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 van een houder te 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527																								
	<p>herroepen/schorsen.</p> <ul style="list-style-type: none"> 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). 																									
D.6	Rechten, verantwoordelijkheden en verplichtingen van derden																									
	<p>De derden die zich baseren op de Certificaten die werden uitgegeven krachtens de onderhavige CP zullen :</p> <ul style="list-style-type: none"> 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); rekening houden met alle beperkingen op het gebruik van het Certificaat beschreven in het Certificaat, de contractuele documenten en de onderhavige CP; alle andere voorzorgen nemen zoals voorgeschreven in de onderhavige CP of elders, betreffende het gebruik van het Certificaat. 																									
E	Identificatie en Authenticatie – gecertificeerde informatie	3.1																								
	<p>De volgende informatie wordt geverifieerd (zie deel E : "Procedure voor aanvraag van een Certificaat" in de onderhavige CP) en gecertificeerd in het Gekwalificeerde Belgacom E-Trust-certificaat in de orde als aangegeven :</p> <table border="1"> <thead> <tr> <th>Attribuut</th><th>Verplicht/Optioneel/Vast</th><th>Waarde</th></tr> </thead> <tbody> <tr> <td colspan="3">Informatie betreffende de houder van het certificaat</td></tr> <tr> <td>Country (C)</td><td>Verplicht</td><td>Nationaliteit van de houder van het Certificaat</td></tr> <tr> <td>Locality (L)</td><td>Verplicht</td><td>Geboorteplaats van de houder van het Certificaat (gemeente)</td></tr> <tr> <td>Organisation (O)</td><td>Optioneel, maar verplicht voor de werknemers</td><td>De officiële naam van de Onderneming (of Organisatie) waartoe de houder van het certificaat behoort, zoals gepubliceerd in de statuten van de Onderneming (of Organisatie).</td></tr> <tr> <td>OrganisationalUnit (OU)</td><td>Optioneel</td><td>Organisatie-eenheid of departement</td></tr> <tr> <td>OrganisationalUnit (OU)</td><td>Obligatoire</td><td>Limitation on transaction value : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde « Not applicable » ingevuld></td></tr> <tr> <td>OrganisationalUnit (OU)</td><td>Obligatoire</td><td>Limitation on certificate usage : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde</td></tr> </tbody> </table>	Attribuut	Verplicht/Optioneel/Vast	Waarde	Informatie betreffende de houder van het certificaat			Country (C)	Verplicht	Nationaliteit van de houder van het Certificaat	Locality (L)	Verplicht	Geboorteplaats van de houder van het Certificaat (gemeente)	Organisation (O)	Optioneel, maar verplicht voor de werknemers	De officiële naam van de Onderneming (of Organisatie) waartoe de houder van het certificaat behoort, zoals gepubliceerd in de statuten van de Onderneming (of Organisatie).	OrganisationalUnit (OU)	Optioneel	Organisatie-eenheid of departement	OrganisationalUnit (OU)	Obligatoire	Limitation on transaction value : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde « Not applicable » ingevuld>	OrganisationalUnit (OU)	Obligatoire	Limitation on certificate usage : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde	
Attribuut	Verplicht/Optioneel/Vast	Waarde																								
Informatie betreffende de houder van het certificaat																										
Country (C)	Verplicht	Nationaliteit van de houder van het Certificaat																								
Locality (L)	Verplicht	Geboorteplaats van de houder van het Certificaat (gemeente)																								
Organisation (O)	Optioneel, maar verplicht voor de werknemers	De officiële naam van de Onderneming (of Organisatie) waartoe de houder van het certificaat behoort, zoals gepubliceerd in de statuten van de Onderneming (of Organisatie).																								
OrganisationalUnit (OU)	Optioneel	Organisatie-eenheid of departement																								
OrganisationalUnit (OU)	Obligatoire	Limitation on transaction value : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde « Not applicable » ingevuld>																								
OrganisationalUnit (OU)	Obligatoire	Limitation on certificate usage : <waarde, ingevuld door de klant om een beperking te plaatsen op de waarde van de transactie, indien niet gespecificeerd, wordt de waarde																								

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527																		
	<table><tr><td></td><td></td><td>« Not applicable » ingevuld></td></tr><tr><td>OrganisationalUnit (OU)</td><td>Optioneel, maar verplicht voor de klanten die hun professioneel deel willen certificeren.</td><td>« Professional status: <...> » voor de zelfstandigen gaat het om de vermelding « Independant » of om de naam van het beroep , voor de Bestuurders-beheerders gaat het om de vermelding “Manager” voor de bestuurders of « Chief Executive Officer» voor de afgevaardigde bestuurder of « Manager» voor de beheerder, voor de werknemer gaat het over de vermelding «Employer».</td></tr><tr><td>OrganisationalUnit (OU)</td><td>Optionnel</td><td>« Role in the organisation : <Rol in de onderneming> » (uitsluitend voor werknemers)</td></tr><tr><td>OrganisationalUnit (OU)</td><td>Verplicht</td><td>“Date of Birth: “ : geboortedatum van de houder van het certificaat (dd/mm/jjjj)</td></tr><tr><td>CommonName (CN)</td><td>Verplicht</td><td>Naam en voornamen van de houder van het Certificaat, zoals weergegeven op zijn identiteitskaart of evenwaardig document.</td></tr><tr><td>Rfc822Name</td><td>Verplicht</td><td>E-mailadres van de houder van het Certificaat</td></tr></table>			« Not applicable » ingevuld>	OrganisationalUnit (OU)	Optioneel, maar verplicht voor de klanten die hun professioneel deel willen certificeren.	« Professional status: <...> » voor de zelfstandigen gaat het om de vermelding « Independant » of om de naam van het beroep , voor de Bestuurders-beheerders gaat het om de vermelding “Manager” voor de bestuurders of « Chief Executive Officer» voor de afgevaardigde bestuurder of « Manager» voor de beheerder, voor de werknemer gaat het over de vermelding «Employer».	OrganisationalUnit (OU)	Optionnel	« Role in the organisation : <Rol in de onderneming> » (uitsluitend voor werknemers)	OrganisationalUnit (OU)	Verplicht	“Date of Birth: “ : geboortedatum van de houder van het certificaat (dd/mm/jjjj)	CommonName (CN)	Verplicht	Naam en voornamen van de houder van het Certificaat, zoals weergegeven op zijn identiteitskaart of evenwaardig document.	Rfc822Name	Verplicht	E-mailadres van de houder van het Certificaat	
		« Not applicable » ingevuld>																		
OrganisationalUnit (OU)	Optioneel, maar verplicht voor de klanten die hun professioneel deel willen certificeren.	« Professional status: <...> » voor de zelfstandigen gaat het om de vermelding « Independant » of om de naam van het beroep , voor de Bestuurders-beheerders gaat het om de vermelding “Manager” voor de bestuurders of « Chief Executive Officer» voor de afgevaardigde bestuurder of « Manager» voor de beheerder, voor de werknemer gaat het over de vermelding «Employer».																		
OrganisationalUnit (OU)	Optionnel	« Role in the organisation : <Rol in de onderneming> » (uitsluitend voor werknemers)																		
OrganisationalUnit (OU)	Verplicht	“Date of Birth: “ : geboortedatum van de houder van het certificaat (dd/mm/jjjj)																		
CommonName (CN)	Verplicht	Naam en voornamen van de houder van het Certificaat, zoals weergegeven op zijn identiteitskaart of evenwaardig document.																		
Rfc822Name	Verplicht	E-mailadres van de houder van het Certificaat																		
Extensions :																				
KeyUsage	Verplicht	<ul style="list-style-type: none">Gekwalificeerd Certificaat : “DigitalSignature, non repudation”Genormaliseerd Certificaat : zoals aangegeven op de bestelbon																		
subjectPublicKey	Vast	Publieke sleutel : lengte van de sleutel : minimaal 1024 bit Clé publique: longueur de clé: minimum 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.: 0.3.2062.9.6.2.13.4.4”																		
CertificatePolicies-policyQualifier-CPS	Vast	www.e-trust.belgium.be/CPS/QNcerts																		
Andere informatie :																				

VALIDITY: 21/02/2003-31/10/2003

Deel				Ref. RFC 2527								
	Issuer	Vast	"CN = Belgacom E-Trust Primary CA for <normalised or qualified> certificates OU = E-Trust O = Belgacom C = BE"									
	Validity	Vast	1 jaar									
	serialNumber	Vast	Serienummer van het certificaat									
	Algorithm	Vast	"Sha1withRSAEncryption"									
	Version	Vast	2 (overeenkomend met v3)									
<div><div><p>Gekwalificeerd E-Trust-certificaat enkel voor gekwalificeerde handtekening</p><table><tr><td></td><td>Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.2.4</td></tr><tr><td>Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : 0.4.0.1456.1.1 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.3.4</td><td>Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.4.4</td></tr></table></div><div><p>Genormaliseerd E-Trust-certificaat</p><table><tr><td></td><td>Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.6.4</td></tr><tr><td>Genormaliseerd Certificaat met SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.7.4</td><td>Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.8.4</td></tr></table></div></div> <p>Tabel 1. Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust-certificaatpolicy (CSP = Certification Service Provider)</p> <p>Aan deze gecertificeerde informatie wordt de handtekening van de Certificatie-autoriteit gehecht, die slaat op alle gecertificeerde informatie.</p>						Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.2.4	Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : 0.4.0.1456.1.1 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.3.4	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.4.4		Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.6.4	Genormaliseerd Certificaat met SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.7.4	Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.8.4
	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.2.4											
Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : 0.4.0.1456.1.1 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.3.4	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : 0.4.0.1456.1.2 Aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.4.4											
	Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de houder : 0.3.2062.9.6.1.19.6.4											
Genormaliseerd Certificaat met SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.7.4	Genormaliseerd Certificaat zonder SSCD (OID ETSI 102 042) 0.4.0.2042.1.1 en aanmaak van de sleutels door de CSP : 0.3.2062.9.6.1.19.8.4											
F	Procedure voor de aanmaak van de Sleutels											
	<p>De lengte van de Sleutels moet minstens 1024 bits zijn.</p> <p>Aanmaak van de Sleutels door de houder van het Certificaat De kandidaat-houder van het Certificaat mag zelf zijn Sleutelpaar aanmaken. In dat geval dient hij :</p> <ul style="list-style-type: none">• 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											

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>PKCS#10-aanvraag van het Certificaat.</p> <ul style="list-style-type: none"> • ofwel, en dit in het kader van een registratie, uitgevoerd tijdens de inschrijving op de dienst Certipost, zijn sleutelpaar en zijn beveiligde elektronische aanvraag aan te maken, binnen zijn beveiligde Certipost omgeving <p>Aanmaak van de Sleutels door de Certificatiedienstverlener of de Lokale Registratie-autoriteit</p> <p>Indien de kandidaat-houder van het Certificaat 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 twee gevallen zich voordoen:</p> <ol style="list-style-type: none"> 1. Indien de Lokale Registratie Autoriteit beschikt over de software voor sleutelpaargeneratie en certificaatsaanvraag : <ul style="list-style-type: none"> • maakt de LRA-operator (LRAO) de Sleutels aan : <ul style="list-style-type: none"> • 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 kopieert 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 : <ul style="list-style-type: none"> • 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 bij de dienst Certipost 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 Certipost omgeving, kunnen vragen om zijn sleutelpaar en zijn elektronische aanvraag in en door middel van een SSCD aan te maken. Deze SSCD zal hem persoonlijk via een aangetekende zending met ontvangstbewijs worden opgezonden. Het paswoord (of PIN code) dat deze SSCD beveiligd, zal hem op een beveiligde wijze via een ander kanaal worden bezorgd. 	
G	<i>Procedure voor de aanvraag van het Certificaat</i>	
	<ol style="list-style-type: none"> 1. De kandidaat-houder van het Certificaat verschaft zich de Bestelbon en de Algemene Voorwaarden betreffende de <u>Gekwalificeerde of Genormaliseerde E-Trust-certificaten</u> (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-houder van het Certificaat 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 : <ol style="list-style-type: none"> 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 <p>Deze bestelbonnen kunnen in een zogenaamde “volledige” versie verkregen</p> 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>worden, waarbij de kandidaat-houder zelf de mogelijke opties kiest, of in een vereenvoudigde versie, of in een geïntegreerde vorm met het contract dat betrekking heeft op de Certipost dienst in het kader van een registratie, uitgevoerd bij de inschrijvingsprocedure bij de Certipost dienst.</p> <p>2. De kandidaat-houder van het Certificaat dient de Bestelbon behoorlijk in te vullen en te ondertekenen. De versies <i>zelfstandigen/privé-personen</i> en <i>bestuurders/zaakvoerders</i> van de Bestelbon bevatten slechts een enkel gedeelte, het gedeelte Klant. De versie <i>werknemers</i> van de Bestelbon bestaat uit twee delen :</p> <ol style="list-style-type: none"> Het gedeelte Klant dient behoorlijk te worden ingevuld en ondertekend door de kandidaat-houder van het Certificaat; Het gedeelte Organisatie 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). <p>Door de ondertekening van de Bestelbon aanvaarden de kandidaat-houder van het Certificaat en de Onderneming (of Organisatie) de Algemene Voorwaarden, paraferen ze deze en hechten ze aan de Bestelbon.</p> <p>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-houder van het Certificaat maakt een afspraak met een officier van de LRA (LRAO) en gaat bij de LRA langs met alle onderstaande documenten.</p> <p>a. Voor de werknemers of de leden van een Onderneming (of Organisatie) :</p> <ul style="list-style-type: none"> de behoorlijk ingevulde en ondertekende Bestelbon; de erbij gevoegde en geparafeerde Algemene Voorwaarden; 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-houder van het Certificaat; 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. <p>b. Voor de zelfstandigen/privé-personen :</p> <ul style="list-style-type: none"> De behoorlijk ingevulde en ondertekende Bestelbon; de erbij gevoegde en geparafeerde Algemene Voorwaarden; 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-houder van het Certificaat; de elektronische aanvraag van het Certificaat op diskette (optie indien de Sleutels niet worden aangemaakt door de CSP). 	

Deel		Ref. RFC 2527
	<p><i>Wanneer de kandidaat-houder van het Certificaat het professionele gedeelte van het Certificaat wil laten certificeren :</i></p> <ul style="list-style-type: none"> – 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. <p>c. Bestuurder/zaakvoerders :</p> <ul style="list-style-type: none"> – De behoorlijk ingevulde en ondertekende Bestelbon; de erbij gevoegde en geparafeerde Algemene Voorwaarden; – een kopie (recto/verso) van de geldige en officiële identiteitskaart van de kandidaat-houder van het Certificaat, zijn paspoort of ieder ander gelijkwaardig officieel document. De kopie moet worden ondertekend door de kandidaat-houder van het Certificaat; – de elektronische aanvraag van het Certificaat op diskette (optie indien de Sleutels niet worden aangemaakt door de LRAO). – 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. <p>4. - In het geval van de vereenvoudigde procedure (overeenkomend met de vereenvoudigde bestelbon), faxt de klant zijn dossier naar 0800 933 16 en 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)</p> <ul style="list-style-type: none"> - In het geval van de normale procedure, maakt de kandidaat-houder van het Certificaat een afspraak met een LRA operator (LRAO) bij de LRA van zijn keuze, die geaccrediteerd is in de context van deze CP. (zie sectie D.1§5) - In het geval van de Certipost procedure, zal de kandidaat-houder van het Certificaat de bestelbon invullen, die on-line beschikbaar is, in zijn beveiligde Certipost omgeving. Het verkrijgen van en de toegang tot deze beveiligde, persoonlijke Certipost omgeving is onderworpen aan de persoonlijke fysische presentatie van de kandidaat-houder van het certificaat bij een Certipost geaccrediteerde LRA (zie sectie D.1 §5) en aan de handtekening van een Certipost contract, die eveneens alle verbintenissen inhoud met betrekking tot de Algemene Voorwaarden, de huidige CP en de CPS. Tijdens deze face-to-face registratie zal de LRAO de validaties uitvoeren, zoals hierna beschreven. Om deze face-to-face registratie geldig uit te voeren, zal de klant zich naar een lokale registratie autoriteit (LRA) begeven, die gemandateerd is door Certipost en door Belgacom E-Trust voor de registratie van Certificaten van het Gekwalificeerde en Genormaliseerde Type, beschikbaar via de on-line Certipost bestelbon. Tijdens de face-to face, zal de klant zich aanbieden met de documenten, zoals vermeld in (3) (uitgenome de elektronische aanvraag van het Certificaat op diskette). De bestelbon, on-line beschikbaar in zijn persoonlijke en beveiligde Certipost omgeving, zal enkel de certificatie toelaten van gegevens die geverifieerd en gevalideerd zijn bij de LRAO, met uitzondering van het e-mail adres te certificeren en de vermeldingen van de eventuele beperkingen op het gebruik. Deze gegevens zullen geleverd worden tijdens het invullen van de on-line bestelbon en vallen onder de verantwoordelijkheid en garantie van de kandidaat-houder van het certificaat, in overeenstemming met de algemene voorwaarden. Het invullen en het doorsturen van de on-line bestelbon, beschikbaar in de persoonlijke en beveiligde Certipost omgeving, wordt gelijkwaardig beschouwd ald een geschreven en ondertekende bestelbon. De klant aanvaardt, door het invullen en het tekenen van het Certipost Contract, met in annex de huidige algemene voorwaarden, met referentie naar de CP en CPS, de huidige algemene voorwaarden, alsook de CP en CPS, met betrekking tot de Gekwalificeerde en Genormaliseerde Certificaten. Deze documenten zijn on-line beschikbaar op het volgende Internet adres : http://www.e-trust.be/CPS/QNCerts. De klant erkent van deze documenten kennis te 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>hebben genomen. Deze documenten, vormen, samen met de bestelbon, de overeenkomst van de Partijen (hierna de "Overeenkomst" genoemd).</p> <p>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 :</p> <p>De LRA-operator (LRAO) controleert de ontvangen documenten en gaat over tot de verificatie :</p> <ul style="list-style-type: none"> • van de identiteit van de kandidaat-houder van het Certificaat op basis van het origineel van zijn geldige identiteitsbewijs; • op basis van de door de kandidaat-houder van het Certificaat verstrekte stukken, van de vermeldingen die moeten worden gecertificeerd met betrekking tot de professionele hoedanigheid van de vooraf geïdentificeerde kandidaat-houder. <p>Indien de aanvraag gevalideerd is, dient de LRAO de ingewonnen documenten te verzamelen om het Registratiedossier van de houder van het Certificaat 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 gearhiveerd bij de Certificatiedienstverlener.</p> <p>5. Validatie</p> <p>Indien de LRA niet rechtstreeks in verbinding staat met de Certificatiediensten van de Certificatiedienstverlener, bij het verzamelen van enerzijds het Registratiedossier van de kandidaat-houder van het Certificaat ontvangen van de LRAO, en desgevallend, anderzijds van de door de Klant verstuurd 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.</p> <p>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.</p> <p>In het geval van de elektronische aanvraag via de bestelbon, on-line beschikbaar in zijn persoonlijke beveiligde Certipost omgeving, zal de tweede verificatie uitgevoerd worden a posteriori door de Auditor van de Certificatie Autoriteit (Certification Authority Auditor), die de coherentie nagaat tussen de uitgegeven Certificaten en de dossiers ontvangen van de LRA's.</p> <p>6. Verificatie a posteriori</p> <p>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.</p>	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
H	<i>Uitgifte van het Certificaat en levering</i>	4.2
	<p>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.</p> <p>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.</p>	
I	<i>Aanvaarding van het Certificaat en Publicatie van het Certificaat</i>	4.3
	<p><i>Publicatie van het Certificaat in het Openbaar Certificatenregister van de Certificatiedienstverlener.</i></p> <p>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.</p> <p><i>Aanvaarding</i></p> <ul style="list-style-type: none"> De houder van het Certificaat 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 7e 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 houder van het Certificaat 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 houder van het Certificaat terug te betalen of een nieuw Certificaat uit te geven. De houder van het Certificaat aanvaardt dat hij hierdoor volledig vergoed is voor de niet-aanvaarding. 	
J	<i>Procedure voor Schorsing/Herstel na schorsing/Herroeping</i>	4.4
	<p>De houder van een Certificaat, de wettelijke vertegenwoordiger (of zijn gemachtigde afgevaardigde) van de Organisatie wanneer de klant-houder van het Certificaat het professionele gedeelte van het Certificaat heeft laten certificeren, de LRA of Belgacom 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.</p> <p>De informatie betreffende de status van de schorsing of herroeping van een Certificaat wordt te allen tijde ter beschikking van allen gesteld door de Certificatiedienstverlener, zoals aangegeven in deel D1, § 5 van het onderhavige document.</p>	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
	<p>Een formulier van schorsing/herstel na schorsing/herroeping wordt ter beschikking van de partijen gesteld door de Certificatiedienstverlener.</p> <p>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 :</p> <p>Ingeval van schorsing :</p> <ul style="list-style-type: none"> • 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. <p>Ingeval van herstel na schorsing :</p> <ul style="list-style-type: none"> • 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. <p>Ingeval van een herroeping moet :</p> <ul style="list-style-type: none"> • 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. 	

VALIDITY: 21/02/2003-31/10/2003

Deel		Ref. RFC 2527
K	<i>Procedure voor de vernieuwing van de Sleutels en van het Certificaat</i>	
	<p>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 :</p> <ul style="list-style-type: none"> • de informatie die wordt gebruikt om de identiteit van de klant-houder van het Certificaat te verifiëren nog steeds geldig is en daartoe : <ul style="list-style-type: none"> – 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	<i>Bescherming van de persoonlijke levenssfeer en van de persoonsgegevens</i>	
	<p>De gegevens die door Belgacom of door de Registratie-autoriteit werden verzameld (papieren document en elektronische informatie) en die door de houder van het Certificaat werden verstrekt in het kader van de aanvraag van een Certificaat en de levering ervan, worden behoorlijk gearchiveerd en beschermd volgens de Belgische wet op de bescherming van de persoonlijke levenssfeer² (cf. de instructie betreffende dit punt in de algemene voorwaarden).</p>	
M	<i>Klachten en regeling van geschillen</i>	
	<ul style="list-style-type: none"> • Ingeval van technische problemen die betrekking hebben op het Certificaat en ingeval van klachten die betrekking hebben op de diensten geleverd op basis van de onderhavige Certificaatpolicy, kan de advocaat-houder van het Certificaat contact opnemen met de helpdesk van de Certificatiedienstverlener : <ul style="list-style-type: none"> - Belgacom E-Trust (Qualified en Normalised CAs) : <ul style="list-style-type: none"> - Telefoonnummer : 0800 91 157 (NL), 0800 91 158 (FR) - Faxnummer : 0800 933 16 - E-mail : info@e-trust.be. 	

² Om haar taken efficiënt te kunnen uitvoeren, gebruikt Belgacom databanken met deze persoonsgegevens. Belgacom dient terzake de persoonlijke levenssfeer van de betrokken personen te respecteren en dus het grootst mogelijke belang te hechten aan en de grootst mogelijke omzichtigheid aan de dag te leggen bij de behandeling van deze gegevens. Deze aan Belgacom verstrekte persoonsgegevens worden opgenomen in de bestanden van Belgacom NV van Publiek recht, Koning Albert II-laan 27, 1030 Brussel. De gegevens worden enkel gebruikt voor de levering van Belgacom E-Trust-diensten. U hebt het recht deze gegevens te raadplegen en te wijzigen.

VALIDITY: 21/02/2003-31/10/2003

<i>Deel</i>		<i>Ref. RFC 2527</i>
	<ul style="list-style-type: none">De Certificatiedienstverlener en de houder van het Certificaat verbinden zich ertoe alles in het werk te stellen om een minnelijke schikking te vinden voor alle conflicten betreffende de geldigheid, de interpretatie of de uitvoering van de overeenkomst die hen bindt. Indien geen minnelijke schikking kan worden gevonden, zal het conflict betreffende de geldigheid, de interpretatie of de uitvoering van de overeenkomst die hen bindt, voor de rechtbanken van Brussel worden gebracht.	

OUTDATED