OID : 0.3.2062.7.1.1.6.0.1

Certificaatpolicy betreffende het

Gekwalificeerde E-Trust-certificaat voor de MyCertipost toepassing

Versie 1.0

–

Datum van publicatie : Mei 2004

Certificaatpolis (Certificate Policy - CP) betreffende het Gekwalificeerde Certificaat voor de MyCertipost-toepassing

Dit document beschrijft de toepasbaarheid van het certificaat van het type "Gekwalificeerd Certificaat voor de MyCertipost-toepassing" (hierna het Certificaat genoemd), uitgegeven door de Certificatiedienstverlener (hierna de Certificatiedienstverlener – CSP genoemd) volgens deze 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 Certificaatpolis betreffende de Gekwalificeerde Certificaten voor de MyCertipost-toepassing die voldoet aan de volgende voorwaarden en aan het document Controleprocedures van de Certificatiedienstverlener:

Deel		Ref. RFC 2527
A	***Overzicht van de Certificaatpolis betreffende het Gekwalificeerde E-Trust-certificaat voor de MyCertipost-toepassing***	**1.1**
	Zeer hoge graad van zekerheid inzake de persoonlijke en eventueel professionele elektronische identiteit van de Certificaathouder. Het gaat om een Certificaat dat slechts wordt afgeleverd indien men zich persoonlijk aanbiedt tijdens het registratieproces. Dit Certificaat biedt een zeer hoge zekerheidsgraad om de link te waarborgen tussen de persoonlijke identiteit van de Certificaathouder, een eventuele professionele hoedanigheid (niet verplicht), een Publieke Sleutel en het toegestane gebruik ervan. Dit Certificaat levert de hoogste zekerheidsgraad van een correcte authenticatie daar de kandidaat voor het bekomen van het Certificaat: – zich ofwel persoonlijk bij een Lokale Registratie-autoriteit (hierna Local Registration Authority of LRA genoemd) moet aanbieden om correct te worden geregistreerd voor de uitgifte van zijn Certificaat door de Certificatiedienstverlener; – of vooraf moet beschikken over een Certificaat van een gelijkwaardig niveau om de aanvraag op een geldige manier te kunnen indienen. De validatie van de aanvraag vereist de voorlegging van het identiteitsbewijs van de kandidaat-houder voor het bekomen van het Certificaat alsook de verificatie van de stukken die zijn professionele hoedanigheid staven en de ermee overeenstemmende informatie die eventueel moet worden gecertificeerd. De aldus gecertificeerde publieke sleutel kan uitsluitend worden gebruikt in het volgende geval: – een context van een *digitale handtekening* in het kader van de MyCertipost-toepassing; In dat geval beantwoordt het Certificaat aan het criterium van een **Gekwalificeerd Certificaat** in de zin van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001) en de technische standaard ETSI TS 101 456 en kan het gebruikt worden voor een geavanceerde of een gekwalificeerde handtekening, waarbij deze laatste automatisch gelijkwaardig is aan een handgeschreven handtekening. De Certificatiedienstverlener(s) gemachtigd om Certificaten uit te geven in overeenstemming met deze Certificaatpolicy specificeert (specificeren) of hij (zij) hieraan en aan de regelgevende documenten voldoet (voldoen), of werden gecertificeerd in overeenstemming hiermee (zie deel D1, § 5 van dit document).	
B	***Identificatie van de Certificaatpolicy van Gekwalificeerde E-Trust-Certificaat voor de MyCertipost-toepassing***	
	Een Certificaatpolicy (CP) is een welbepaald geheel van regels die de toepasbaarheid aangeven van een Certificaat op een specifieke gemeenschap en/of een toepasbaarheids-	

Deel		Ref. RFC 2527
	klasse met gemeenschappelijke vereisten inzake veiligheid. Dit document bevat en identificeert binnen dezelfde globale **Certificaatpolicy** verschillende Certificaatpolicies afhankelijk van het gebruik dat van het Certificaat mag worden gemaakt (digitale handtekening of versleuteling/authenticatie), afhankelijk van het feit of het Sleutelpaar werd gegenereerd door de houder van het Certificaat of door de Certificatiedienstleverancier, en afhankelijk van het feit of de Private Sleutel gegenereerd geweest is met en slechts mag worden gebruikt in een Veilig Middel voor het Aanmaken van een Handtekening (Secure Signature Creation Device – SSCD) of niet. Voor de **Gekwalificeerde Certificaten voor de MyCertipost-toepassing**, is het gebruik strikt voorbehouden voor de ondersteuning van de digitale handtekening, die ondersteund moet worden door een gekwalificeerd certificaat, in overeenstemming met de Europese richtlijn 1999/93/EG en de omzetting ervan in de Belgische wet houdende vaststelling van bepaalde regels in verband met het juridische kader voor elektronische handtekeningen en Certificatiediensten (cf. Wet van 9 juli 2001). Bovendien is het gebruik van het certificaat strikt beperkt in het kader van de diensten die aangeboden worden via de MyCertipost-toepassing. De Certificaten uitgegeven in overeenstemming met deze globale CP “Gekwalificeerd E-Trust-certificaat voor de MyCertipost-toepassing” bevatten een Certificaatpolicy-identificatiefactoor, die door derden kan worden gebruikt om de toepasbaarheid en de betrouwbaarheid van het Certificaat ten opzichte van een bepaalde toepassing te bepalen. De identificatiefactoren voor de Gekwalificeerde E-Trust Certificaatpolicy voor de MyCertipost-toepassing gespecificeerd in dit document, zijn opgenomen in Tabel 1 hieronder. Gekwalificeerd E-Trust-certificaat voor gekwalificeerde en geavanceerde handtekening in de MyCertipost toepassing |	
---	---
	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : **0.4.0.1456.1.2** Aanmaak van de sleutels door de houder : **0.3.2062.7.1.1.6.2.1**
Gekwalificeerd Certificaat met SSCD (OID ETSI 101 456) : **0.4.0.1456.1.1** Aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.6.3.1**	Gekwalificeerd Certificaat zonder SSCD (OID ETSI 101 456) : **0.4.0.1456.1.2** Aanmaak van de sleutels door het CSP : **0.3.2062.7.1.1.6.4.1** | Tabel 1. Identificatie van de Gekwalificeerde Certipost E-Trust-certificaatpolicy voor MyCertipost applicatie	
C	***Toepasbaarheid***	**1.3.4**
	• Dit type Certificaat biedt een zeer grote garantie van de persoonlijke of eventueel professionele elektronische identiteit, die kan worden gebruikt om diensten in het kader van de MyCertipost-toepassing te beveiligen.	

Deel		Ref. RFC 2527
	• Het is echter aan de partijen om de toepassingen 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 deze CP). • Het gebruik van de sleutel (key usage) en de toepasbaarheid van het Certificaat worden gecertificeerd (zie de beschrijving van de inhoud van het Certificaat in deel E van dit document). De aldus gecertificeerde publieke sleutel mag enkel worden gebruikt in een context van geavanceerde of gekwalificeerde handtekening die ondersteund moet worden door een gekwalificeerd certificaat in het kader van de diensten van de MyCertipost-toepassing. • De Gekwalificeerde Certificaten uitgegeven in het kader van deze CP komen tegemoet aan de vereisten van bijlage I van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). Ze kunnen worden gebruikt om de elektronische handtekeningen te ondersteunen die voldoen aan de vereisten van een handtekening in verband met de gegevens in elektronische vorm op dezelfde wijze als een handgeschreven handtekening voldoet aan de vereisten in verband met de gegevens op papier, zoals gespecificeerd in artikel 5.1 van de Europese richtlijn en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). In die context stemt deze CP overeen met en voldoet aan de vereisten beschreven in het document ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”, in overeenstemming met hoofdstuk 8 ervan zoals gepreciseerd in de clausules vervat in dit document (zie delen B, C en D van dit document). Hiertoe publiceert de Certificatiedienstverlener de elementen die deze conformiteitsverklaring ondersteunen, zoals aangegeven in deel D van dit document. • De Certificaten uitgegeven in het kader van deze CP zijn uitgegeven door een Certificatie-autoriteit die beantwoordt 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 met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001). • De Certificaten uitgegeven in het kader van deze CP zijn niet 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. • De MyCertipost-toepassing waartoe het gebruik van het certificaat is beperkt, omvat (niet-limitatief) de dienst “registered electronic mail”. Het Gekwalificeerde E-Trust-Certificaat voor de MyCertipost-toepassing kan worden gebruikt voor de ondersteuning van elektronische handtekeningen in het kader van de “registered electronic mail” die voldoen aan de vereisten van een handtekening in verband met de gegevens in elektronische vorm op dezelfde wijze als een handgeschreven handtekening voldoet aan de vereisten in verband met de gegevens op papier, zoals gespecificeerd in artikel 5.1 van de Europese richtlijn en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot de elektronische handtekeningen en de certificatiediensten (cf. wet van 9 juli 2001).	
D	***Rechten, verantwoordelijkheden en verplichtingen***	**2**
D.1	***Rechten, verantwoordelijkheden en verplichtingen van de Certificatiedienstverlener***	**2.1**
	• De Certificatiedienstverlener zal Certificaten afleveren die voldoen aan de standaarden X.509v3 (ISO 9594-8). • De Certificatiedienstverlener geeft de Gekwalificeerde Certificaten uit onder het label “Qualified Certificate for Certipost application”, zoals bepaald in en in overeenstemming	

Deel		Ref. RFC 2527

met de vereisten van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (wet van 9 juli 2001), en de technische standaard ETSI TS 101 456. Hiertoe publiceert de Certificatiedienstverlener de elementen die deze conformiteitsverklaring ondersteunen.

- De Certificatiedienstverlener waarborgt dat aan alle vereisten opgenomen in de toepasselijke Certificaatpolicy's (opgenomen in het Certificaat in overeenstemming met deel B van dit document) wordt voldaan, en waarborgt dat hij de verantwoordelijkheid voor deze conformiteit op zich neemt en dat hij deze diensten zal leveren in overeenstemming met zijn CPS.
- Informatie m.b.t. de Certificatiedienstverlener die gemachtigd is Certificaten onder deze CP uit te geven:
  - Uitsluitend de onderstaande CA's zijn hiertoe gemachtigd: Certipost nv via haar Certipost E-Trust diensten en via de **Certipost E-Trust Primary CA for Qualified Certificates** voor de uitgifte van Gekwalificeerde Certificaten voor de MyCertipost-toepassing.
  - *Bepalingen van de Certificatiepraktijken (CPS):* www.e-trust.be/CPS/QNcerts
  - *Openbaar Repertorium van Certificaten en CRL:* www.e-trust.be/en/x500
  - *Conformiteitsverklaring:* www.e-trust.be/CPS/QNcerts
  - *Opschorting/Revocatie-autoriteit:* 078/15 24 70 (beschikbaar 24u/24 en 7d/7), opschorting/revocatieformulier beschikbaar op het volgende adres www.e-trust.be/CPS/QNcerts

- Om over te gaan tot de registratie van de kandidaat-Certificaathouders, gebruikt de Certificatiedienstverlener de volgende erkende Lokale Registratie-autoriteiten (Local Registration Authority - LRA):
  - De postkantoren en andere lokale registratie-authoriteiten die aanvaard zijn om de registratie uit te voeren van de MyCertipost-gebruikers, zoals bepaald in de lijst die beschikbaar is op: www.mycertipost.be
  - De lokale registratie-authoriteiten die aanvaard zijn om de registratie uit te voeren, zoals gespecifieerd 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 Certificaathouder via de aangewezen kanalen verwittigt en op de hoogte stelt).
- Wanneer de Certificatiedienstverlener verantwoordelijk is voor de aanmaak van de Sleutels, waarborgt deze dat ieder door hem aangemaakt Sleutelpaar voor rekening van een houder van een Certificaat wordt aangemaakt op beveiligde wijze en dat het privé-karakter van de Private Sleutel van de houder van het Certificaat wordt gewaarborgd in overeenstemming met de vereisten van de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (. wet van 9 juli 2001), en de technische standaard ETSI TS 101 456.
- 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

Deel		Ref. RFC 2527
	richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001), en met de technische standaard ETSI TS 101 456, en dat het Sleutelpaar zal worden aangemaakt via dit middel. • In dit verband dient de Certificatiedienstverlener de persoonlijke levenssfeer van de betrokken personen te respecteren en bijgevolg een groot belang te hechten aan en heel behoedzaam te werk te gaan bij het verwerken van deze data. De persoonsgegevens die aan de Certificatiedienstverlener worden verstrekt, worden opgenomen in zijn bestanden. De gegevens zullen enkel worden gebruikt voor de levering van Certificatiediensten. De Certificaathouder heeft het recht deze gegevens te raadplegen en te wijzigen.[1] De Certificatiedienstverlener verbindt zich ertoe op zijn inschrijvingscontracten voor de Certificaten duidelijk de rechten van de klant te vermelden in het kader van de bescherming van 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 verplichtingen van de Certificaathouder***	**2.1.3**
	De Certificaathouder verklaart zich akkoord met het geldende Certification Practice Statement (CPS) dat de Praktijken beschrijft die worden gebruikt om de Digitale Certificaten af te leveren en is opgemaakt door de Certificatiedienstverlener. De Certificaathouder aanvaardt deze CP. In het bijzonder stemt de Certificaathouder in met het volgende: • Het contractuele akkoord met betrekking tot dit type van Certificaat wordt geregeld naar Belgisch recht. • De kandidaat-Certificaathouder legt precieze, correcte en volledige informatie voor aan de Certificatiedienstverlener in overeenstemming met het type Certificaat en de Certificaatpolicy('s) opgenomen in deel B van dit document en inzonderheid in overeenstemming met de overeenstemmende registratieprocedures. De Certificaathouder is verantwoordelijk voor de nauwkeurigheid van de gegevens die naar de Certificatiedienstverlener worden gestuurd. • De Certificaathouder zal zijn Sleutelpaar enkel gebruiken in overeenstemming met de beperkingen die hem ter kennis werden gebracht in het Certificaat of via een contractueel akkoord. • Wanneer de Certificatiedienstverlener niet verantwoordelijk is voor de aanmaak van de Sleutels,is de kandidaat-Certificaathouder verantwoordelijk voor de aanmaak van zijn Sleutelpaar en zal hij dit aanmaken in overeenstemming met de Certificaatpolicy die werd gekozen uit die welke deel uitmaken van deel B van dit document, daarbij gebruik makend van een algoritme en een Sleutellengte (minimaal 1024 bit) die voldoen aan de vereisten van de overeenstemmende Certificaatpolicy, in overeenstemming met de contractuele bepalingen overeengekomen met de Certificatiedienstverlener en inzonderheid, in het geval van een Gekwalificeerd Certificaat, in overeenstemming met de vereisten van een elektronische handtekening zoals bepaald in de Europese richtlijn 1999/93/EC en de omzetting ervan in de Belgische wet die bepaalde regels vastlegt met betrekking tot het juridische kader voor de elektronische handtekeningen en de certificatiediensten (Wet van 9 juli 2001) en in het document ETSI TS 101 456 "Policy requirements for certification authorities issuing qualified certificates". Bovendien waarborgt de Certificaathouder de enige te zijn die de Private Sleutel verbonden met de Publieke Sleutel die moet worden gecertificeerd, bezit. • Indien de toepasselijke CP het gebruik van een (veilig) middel voor het aanmaken van een handtekening vereist, zal het Sleutelpaar worden aangemaakt via dit middel en zal	

[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

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 aanmaak 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. Het wachtwoord 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 Certificaathouder mag zijn Private Sleutel niet onbewaakt in een onvergrendelde staat achterlaten (bv. zonder bewaking in een werkstation wanneer het wachtwoord werd ingevoerd). De Certificaathouder is als enige verantwoordelijk voor het gebruik van zijn Private Sleutel, de Certificatiedienstverlener is niet verantwoordelijk voor het gebruik van het Sleutelpaar van de Certificaathouder.
- 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 Certificaathouder werd verloren, gestolen of potentieel gecompromitteerd; of
  - de Certificaathouder het toezicht over zijn Private Sleutel kwijt is omdat de activeringsgegevens ervan gecompromitteerd werden (bv. het wachtwoord) 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 dit 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 elke wijziging van de informatie die niet voorkomt in het Certificaat, maar die bij de registratie naar de Certificatiedienstverlener werd gestuurd. De Certificatiedienstverlener zal de geregistreerde gegevens rechtzetten.
- De Certificaathouder dient op eigen initiatief de herroeping van zijn Certificaat te vragen indien de aan de Certificatiedienstverlener gestuurde informatie ter staving van een professionele hoedanigheid geheel of gedeeltelijk verouderd zou zijn.
- De Certificaathouder aanvaardt dat zijn Digitaal Certificaat onmiddellijk na de aanmaak ervan in het Certificate Public Registry (Openbaar Certificatieregister) van de Certificatiedienstverlener wordt gepubliceerd.
- Het Certificaat wordt geacht aanvaard te zijn door de Certificaathouder zodra de eerste van de volgende gebeurtenissen zich voordoet, hetzij de 8e dag na de publicatie ervan in het Openbaar Certificatieregister (Certificate Public Registry) van Certificatiedienstverlener, hetzij bij het eerste gebruik ervan door de Certificaathouder. Tijdens de voornoemde 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 brengen. 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 – 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

Deel		Ref. RFC 2527
	deze informatie naar derden te sturen onder dezelfde voorwaarden als die vooropgesteld in deze CP in geval 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 bepalingen van de Certificatiepraktijken (CPS) van de Certificatiedienstverlener beschreven registratieporcedures strikt na te leven (zie deel D.1, § 5). De LRA waarborgt: • dat de Certificaathouders correct worden geïdentificeerd en geauthentificeerd, 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 Certificaathouder (papieren of elektronisch genotariseerd formaat). • De registratie-officier verifieert de identiteit van de Certificaathouder op basis van het (de) door de Belgische wetgeving gevalideerde en erkende identiteitsdocument(en). Dit (deze) document(en) bevat(ten) meer bepaald de volledige naam (familienaam en voornamen), de geboortedatum en –plaats, het fysieke adres van de Certificaathouder, 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 Certificaathouder. • Indien de Certificaathouder verbonden is aan een rechtspersoon, dient een bewijs van deze vereniging te worden gevalideerd door de registratie-officier. • De registratie-officier zal een kopie archiveren van de informatie die bij de registratieprocedure werd verstrekt door de Certificaathouder en die volledig naar de Certificatiedienstverlener werd gestuurd, 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 die gebruikt wordt 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. • 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	

Deel		Ref. RFC 2527
	essentieel belang: • 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 Organisatie) van de Certificaathouder (indien van toepassing)***	
	De Onderneming (of 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 Organisatie) betrokken is. De Onderneming (of Organisatie) gaat akkoord met: • het geldende Certification Practice Statement (CPS) dat werd opgesteld door de Certificatiedienstverlener en een beschrijving geeft van de Praktijken die worden gebruikt om de Certificaten af te leveren. • deze Certificate Policy (CP) van het Gekwalificeerde E-Trust-certificaat voor de Certipost-toepasing. 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. In geval van wijziging van deze informatie dient de Onderneming (of Organisatie) er onmiddellijk de diensten van de Certificatiedienstverlener van in kennis te stellen, die dienovereenkomstig 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 (of Organisatie) via de aangewezen kanalen 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).	
D.5	***Rechten, verantwoordelijkheden en verplichtingen van derden***	
	De derden die zich baseren op de Certificaten die werden uitgegeven volgens deze 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	

Deel		Ref. RFC 2527
	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 dit 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 deze CP of elders, betreffende het gebruik van het Certificaat.	
E	***Identificatie en Authenticatie – gecertificeerde informatie***	**3.1**

De volgende informatie wordt geverifieerd (zie deel G: "Procedure voor aanvraag van een Certificaat" in deze CP) en gecertificeerd in het Gekwalificeerde E-Trust-certificaat voor de Certipost-toepassing in de volgorde als aangegeven:

Attribuut	**Verplicht /Optioneel/Vast**	**Waarde**
	Distinguished Name	
Country (C)	Verplicht	Nationaliteit van de Certificaathouder (Land)
Locality (L)	Verplicht	Geboorteplaats van de Certificaathouder (Plaats)
Organisatie (O)	Verplicht	Voor natuurlijke personen gaat het om de vermelding "Private Person", voor organisaties gaat het om de officiële naam van de Onderneming (of organisatie) die de Certificaathouder tewerkstelt (zoals gepubliceerd in de statuten van de Onderneming (of organisatie))
OrganisationalUnit (OU)	Vast	"Limitation on transaction value: Not applicable"
OrganisationalUnit (OU)	Vast	"Limitation on certificate usage: for use within MyCertipost application only"
OrganisationalUnit (OU)	Verplicht	"Date of birth: <dd/mm/jjjj>" (geboortedatum van de Certificaathouder)
CommonName (CN)	Verplicht	Naam en voorna(a)m(en) van de Certificaathouder zoals vermeld op de identiteitskaart of gelijkwaardig document.
	Extensions:	
KeyUsage	Vast	NonRepudation
subjectPublicKey	Vast	Publieke sleutel: lengte van de sleutel: minimum 1024 bit; pulieke exponent: Fermat-4 (=010001)
CertificatePolicies-policyIdentifier	Vast	Zie tabel 1.
CertificatePolicies-policyQualifier-userNotice	Vast	"E-Trust Qualified Certificate for Use within MyCertipost application only. General conditions O.I.D.: 0.3.2062.7.1.2.7.1»
CertificatePolicies-policyQualifier-CPS	Vast	http://www.e-trust.be/CPS/QNcerts
0.3.2062.7.1.5.1.1	Vast	"E-Trust Qualified Certificate for Use within MyCertipost application only"

Deel		Ref. RFC 2527

subjectKeyIdentifier	Vast	The keyIdentifier is composed of a four bit type field with the value 0100 followed by the least significant 60 bits of the SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bit string bits).
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
QcStatement	Vast	0.4.1862.1.1 { id-etsi-qcs 1 }
Other information:		
Issuer	Vast	"CN = Certipost E-Trust Primary CA for qualified certificates O = Certipost C = BE"
Validity	Vast	1 jaar
SerialNumber	Vast	Volgnummer van het certificaat
Algorithm	Vast	"Sha1withRSAEncryption"
Versie	Vast	2 (conform met v3)

Merk op dat de extensie "0.3.2062.7.1.5.1.1" een privé-extensie van E-Trust is, met als doel duidelijk aan te geven dat dit certificaat alleen kan worden gebruikt in het kader van de diensten die worden aangeboden door de MyCertipost-toepassing.
Aan deze gecertificeerde informatie wordt de handtekening van de Certificatie-autoriteit gehecht, die slaat op alle gecertificeerde informatie.

F *Procedure voor de aanmaak van sleutels*

De lengte van de Sleutels moet minstens 1024 bits zijn.

Aanmaak van sleutels door de Certificaathouder

De kandidaat-Certificaathouder maakt zelf zijn Sleutelpaar aan.
In het kader van een registratie – uitgevoerd tijdens de inschrijving op de dienst Certipost bij een erkende LRA, maakt de kandidaat-Certificaathouder het sleutelpaar en de beveiligde elektronische aanvraag aan, binnen zijn beveiligde MyCertipost-omgeving.

Aanmaak van de Sleutels door de Certificatiedienstverlener of de Lokale Registratie-autoriteit

Indien de kandidaat-Certificaathouder de PKCS#10-aanvraag van het Certificaat niet verstrekt op het ogenblik van de registratie bij de officier van de Lokale Registratie-autoriteit en in contractuele overeenstemming met de kandidaat-houder, kunnen drie gevallen zich voordoen:
1. Indien de Lokale Registratie Autoriteit beschikt over de software voor sleutelpaargeneratie en certificaatsaanvraag :

- maakt de LRA-operator (LRAO) de Sleutels aan :
  - de LRAO vraagt de kandidaat-houder van het Certificaat het paswoord (of de PIN-code) in te voeren dat zijn Sleutels zal beschermen;
  - de LRAO genereert de Sleutels onder standaard-PKCS-formaat op de gekozen drager (bijvoorbeeld diskette of SSCD). De Sleutels hebben de vorm van een bestand dat wordt beschermd door het paswoord (of PIN-code) dat door de kandidaat-houder van het Certificaat werd gekozen;
- de LRAO creëert de PKCS#10-aanvraag;
- de LRAO wist in zijn software- en hardwareomgeving ieder spoor van de Sleutels van de kandidaat-houder van het Certificaat uit. De Sleutels zijn enkel aanwezig op de drager

Deel		Ref. RFC 2527
	die aan de houder van het Certificaat wordt bezorgd. 2. Indien de Lokale Registratie Autoriteit niet beschikt over de software voor sleutelpaargeneratie en certificaatsaanvraag : • Maakt de CRA-operator (CRAO) de Sleutels aan, • Creëert de CRAO de PKCS#10-aanvraag. 3. In het kader van een registratie, uitgevoerd tijdens de inschrijvingsprocedure voor de dienst MyCertipost bij een voor dit doeleinde geaccrediteerde LRA, zal de kandidaat-houder van het Certificaat, voor zoverre de dienst beschikbaar zal zijn aan de Certificatiedienstverlener en dit in het kader van zijn beveiligde MyCertipost omgeving, kunnen vragen om zijn sleutelpaar aan te maken. Dit kan gebeuren in en door middel van een SSCD. Deze SSCD zal hem persoonlijk via een aangetekende zending met ontvangstbewijs worden opgezonden. Het paswoord (of PIN code) dat deze SSCD beveiligt, zal hem op een beveiligde wijze via een ander kanaal worden bezorgd. Indien het sleutelpaar niet in en door middel van een SSCD zal worden aangemaakt, zal Certipost de private sleutel geëncrypteerd opsturen binnen zijn beveiligde MyCertipost account. De code om de private sleutel te decrypteren zal worden meegedeeld aan de Klant via een verschillend beveiligd kanaal.	
G	***Procedure en aanvraag van het Certificaat***	
	– De klant bezit steeds voorafgaandelijk een **MyCertipost account**. – Indien de Klant zelf zijn sleutelpaar wenst te genereren (enkel voor *privé*-gebruik) : De Klant vult, in zijn persoonlijke en beveiligde Certipost-omgeving die hij met behulp van zijn toegangscodes kan bereiken, de bestelbon in van het type Gekwalificeerd Certificaat voor privépersoon. – Indien de Klant wenst dat Certipost zijn sleutelpaar genereert (enkel mogelijk voor *werknemers*) : De Klant wenst een Certificaat te bekomen voor professioneel gebruik. Hiertoe vult hij de bestelbon in van het type Gekwalificeerd Certificaat voor uitsluitend gebruik in MyCertipost toepassing voor werknemers. De bestelbon is on-line beschikbaar op het volgende internet-adres : http://www.e-trust.be/CPS/QNCerts. De Klant vult deze bestelbon in en tekent deze. De Klant faxt deze bestelbon door naar de Certipost E-Trust Registratiediensten. De coördinaten hiervoor zijn beschikbaar op het volgende internet-adres : http://www.e-trust.be/CPS/QNCerts. – Door de Bestelbon in te vullen en te ondertekenen aanvaardt de Klant de onderhavige Algemene Voorwaarden, alsook de “Certificate Policy” (hierna de “CP”) en het “Certification Practice Statement of Qualified or Normalised Certificates” (hierna het “CPS”) met betrekking tot de Gekwalificeerde of Genormaliseerde E-Trust-certificaten, zoals deze documenten on line beschikbaar zijn op het volgende internetadres : http://www.e-trust.be/CPS/QNcerts, en waarvan de Klant erkent kennis te hebben genomen. Voornoemde documenten vormen, met de Bestelbon, de overeenkomst tussen de Partijen (hierna de “Overeenkomst”). **Validatie** : : In het geval van de elektronische aanvraag via de bestelbon, on line beschikbaar in zijn persoonlijke beveiligde MyCertipost-omgeving, zal de tweede verificatie uitgevoerd worden door de Auditor van de Certificatie-Authoriteit (Certification Authority Auditor – CAA), die de coherentie nagaat tussen de uitgegeven Certificaten en de dossiers ontvangen van de LRA’s.	

Deel		Ref. RFC 2527
H	***Uitgifte van het Certificaat***	**4.2**
	– Indien de Klant zelf zijn sleutelpaar gegenereerd heeft (enkel voor *privé*-gebruik) zal de uitgifte van het Certificaat online gebeuren tijdens de bestelprocedure van certificaten binnen de MyCertipost toepassing, – Indien Certipost het sleutelpaar voor de klant gegenereert heeft, zal Certipost zijn private sleutel geëncrypteerd opsturen binnen zijn beveiligde MyCertipost omgeving. De code om de private sleutel te decrypteren zal worden meegedeeld aan de Klant via een verschillend beveiligd kanaal. Indien Certipost het sleutelpaar voor de klant op een SSCD gegenereert heeft, zal Certipost de PIN code via zijn beveiligde MyCertipost omgeving opsturen . De SSCD zal worden opgestuurd via een apart beveiligd kanaal.	
I	***Aanvaarding van het Certificaat en Publicatie van het Certificaat***	**4.3**
	Publicatie van het Certificaat in het Openbaar Certificatenregister van de Certificatiedienstverlener. Eens het Certificaat is uitgegeven door de Certificatiedienstverlener, wordt het onmiddellijk gepubliceerd in het Openbaar Certificatenregister van de Certificatiedienstverlener. Dit Register is openbaar en permanent toegankelijk. *Aanvaarding* • De Certificaathouder, en in voorkomend geval de Organisatie, aanvaardt dat zijn Digitale Certificaat onmiddellijk na aanmaak in het Openbaar Certificatieregister van de Certificatiedienstverlener wordt gepubliceerd. • Het Certificaat wordt geacht aanvaard te zijn door de Certificaathouder, en in voorkomend geval de Organisatie, zodra de 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 het eerste gebruik ervan door de Certificaathouder. Tijdens de voornoemde periode is de Certificaathouder, en eventueel de Organisatie, verantwoordelijk voor de controle van de juistheid van de inhoud van zijn gepubliceerde Certificaat. Indien de Certificaathouder, of eventueel de Organisatie, enige incoherentie vaststelt tussen de informatie van het contractuele akkoord en de inhoud van zijn Certificaat, dient hij/zij de Certificatiedienstverlener daarvan onverwijld op de hoogte te brengen. De Certificatiedienstverlener zal in dat geval het Certificaat herroepen en de gepaste maatregelen nemen om een nieuw Certificaat uit te geven. Dit is de enige mogelijkheid m.b.t. de niet-aanvaarding van het Certificaat.	
J	***Procedure voor Schorsing/Herstel na Schorsing/Herroeping***	**4.4**
	De Certificaathouder, de wettelijke vertegenwoordiger (of zijn gemachtigde afgevaardigde) van de Organisatie in het geval van Werknemers-certificaten, de LRA of E-Trust kunnen de schorsing, het herstel na schorsing of de herroeping van het Certificaat vragen. 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 te allen tijde ter beschikking van allen gesteld door de Certificatiedienstverlener, zoals aangegeven in deel D1, § 5 van dit document. Een formulier van schorsing/herstel na schorsing/herroeping wordt ter beschikking van de partijen gesteld door de Certificatiedienstverlener op het volgende adres: http://www.e-trust.be/CPS/QNcerts). 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	

Deel		Ref. RFC 2527
	geauthentificeerd en bevestigd: In geval van **schorsing:** • De aanvrager neemt contact op met de Schorsings- en Herroepingsautoriteit (Suspension Revocation Authority – SRA) van de Certificatiedienstverlener die het Certificaat in kwestie, heeft uitgegeven, om een formulier voor de aanvraag om schorsing van het Certificaat te vragen, of gebruikt het formulier dat beschikbaar is op het volgende adres: http://www.e-trust.be/CPS/QNcerts. • 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 14 werkdagen per fax of per brief 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, anders zal het certificaat automatisch worden herroepen. In geval van **herstel na schorsing**: • De aanvrager neemt contact op met de Schorsings- en Herroepingsautoriteit (Suspension Revocation Authority – SRA) van de Certificatiedienstverlener die het Certificaat in kwestie, heeft uitgegeven om een formulier voor de aanvraag van herstel na schorsing van een Certificaat te vragen, of gebruikt het formulier dat beschikbaar is op het volgende adres: http://www.e-trust.be/CPS/QNcerts. • 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 (beide zijden) van zijn identiteitskaart aan te melden. • De Officier van de Lokale Registratie-autoriteit zal de verstrekte documenten en de identiteit van de aanvrager verifiëren. Als het verzoek is gevalideerd, zal de Officier de aanvraag naar de SRA doorsturen. • De SRA zal het Certificaat binnen 24 uur, te rekenen vanaf de ontvangst van de aanvraag, herstellen. In geval van een **herroeping**: • De aanvrager vraagt de schorsing van het Certificaat (zie hierboven) aan. • De aanvrager neemt contact op met de SRA om een formulier voor de aanvraag om herroeping van het Certificaat te vragen of gebruikt het formulier dat beschikbaar is op het volgende adres: http://www.e-trust.be/CPS/QNcerts. • 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 (beide zijden) van zijn identiteitskaart aan te melden. • De Officier van de Lokale Registratie-autoriteit zal de verstrekte documenten en de identiteit van de aanvrager verifiëren. Als het verzoek is gevalideerd, zal de Officier de aanvraag naar de SRA doorsturen. De SRA herroept het Certificaat vanaf de datum van ontvangst van de aanvraag om herroeping. • Het certificaat wordt 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 het Certificaat en voor updates***	
	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	

Deel		Ref. RFC 2527
	herroeping of ten gevolge van de naderende vervaldag. De Certificatiedienstverlener vergewist zich ervan dat : - de informatie die wordt gebruikt om de identiteit van de klant-Certificaathouder 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, in geval van een vernieuwing en voor zover de Sleutels en het Certificaat van de Certificaathouder 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, moet de Certificatiedienstverlener dit meedelen aan de klant-Certificaathouder. • De Certificatiedienstverlener zal slechts een Certificaat uitgeven voor een eerder gecertificeerde Sleutel indien de beveiliging van de cryptografische parameters betreffende deze Sleutel nog steeds voldoende is en de Sleutel in kwestie niet werd gecompromitteerd.	
L	***Bescherming van de persoonlijke levenssfeer en van de persoonsgegevens***	
	De gegevens die door E-Trust of door de Registratie-autoriteit worden verzameld (papieren document en elektronische informatie) en die door de Certificaathouder worden 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 levenssfeer[2] (cf. de instructie betreffende dit punt in de algemene voorwaarden).	
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.fr@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.	

[2] Om haar taken efficiënt te kunnen uitvoeren, gebruikt Certipost databanken met deze persoonsgegevens. Certipost 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 Certipost verstrekte persoonsgegevens worden opgenomen in de bestanden van CERTIPOST NV, Willebroekkaai, 22, 1000 Brussel. De gegevens worden enkel gebruikt voor de levering van Certipost E-Trust-diensten. U hebt het recht deze gegevens te raadplegen en te wijzigen.