

# **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**OUTDATED**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 :

OUTDATED

Deel		Ref. RFC 2527
A	<p><b>Overzicht van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy</b></p> <p>VALIDITY: 21/02/2003-</p> <p>0.3.2062.9.6.1.1.19.1.1</p>	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"> <li>– 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;</li> <li>– of voorafgaandelijk moet beschikken over een Certificaat van een gelijkwaardig niveau om de aanvraag op een geldige manier te kunnen indienen.</li> </ul> <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"> <li>– in het kader van een gekwalificeerde digitale handtekening; in dat geval beantwoordt het Certificaat aan het criterium van een <b>Gekwalificeerd Certificaat</b> 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 (cf. wet van 9 juli 2001) en de technische standaard ETSI 101 456, of (exclusief);</li> <li>– in het kader van versleuteling en/of authenticatie ; in dat geval beantwoordt het Certificaat aan het criterium van een <b>Genormaliseerd Certificaat</b> in de zin van de technische standaard ETSI 102 042.</li> </ul> <p>De Certificatiedienstverlener(s) gemachtigd om Certificaten af te leveren in overeenstemming met de onderhavige Certificaatpolicy specificceert (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	<p><b>Identificatie van de Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy</b></p>	
	<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 <b>Gekwalificeerde of Genormaliseerde E-Trust Certificaatpolicy</b> verschillende Certificaatpolities 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 <b>Gekwalificeerde Certificaten</b>, 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 <b>Genormaliseerde Certificaten</b>, 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</p>	<p>Pagina 3/4</p>

VALIDITY: 21/02/2003-

**OUTDATED**