OID : 0.3.2062.7.1.1.6.0.1

Politique de Certificat relative au

Certificat Qualifié E-Trust pour application MyCertipost

Version 1.0

–

Date de publication : Mai 2004

Politique de Certificat (Certificate Policy - CP) relative au Certificat Qualifié pour application MyCertipost

Ce document décrit l'applicabilité du certificat de type « Certificat Qualifié pour application MyCertipost» (ci-après le Certificat) émis par le Prestataire de Services de Certification (ci-après le Prestataire de Services de Certification – CSP) selon la présente CP, les procédures à suivre et les responsabilités des parties impliquées, conformément aux déclarations de pratiques de certification en vigueur (ci-après le CPS) du Prestataire de Services de Certification. Il s'agit d'une politique de Certification relative à des Certificats Qualifiés pour application MyCertipost qui satisfait aux conditions suivantes :

Section		Réf. RFC 2527
A	***Aperçu de la Politique de Certificat Qualifié E-Trust pour application Certipost***	**1.1**
	Très haut niveau d'assurance quant à l'identité électronique personnelle et éventuellement professionnelle du titulaire du Certificat. Il s'agit d'un Certificat dont la délivrance est conditionnée à une présentation personnelle durant le processus d'enregistrement. Ce Certificat fournit un niveau très élevé de garantie pour assurer le lien entre l'identité personnelle du titulaire du Certificat, une qualité professionnelle éventuelle (non obligatoire), une clé publique et son usage autorisé. Ce Certificat fournit le degré le plus élevé de garantie d'authentification correcte puisque le candidat titulaire à l'obtention du Certificat doit : – soit se rendre en personne auprès d'une Autorité d'Enregistrement Locale (ci-après Local Registration Authority ou LRA) afin d'être enregistré correctement avant l'émission de son Certificat par le Prestataire de Services de Certification, – soit disposer au préalable d'un Certificat de niveau équivalent pour procéder valablement à cette demande. La validation de la demande nécessitera la fourniture de la preuve de l'identité du candidat titulaire à l'obtention du Certificat et la vérification des pièces apportant la preuve de sa qualité professionnelle et des informations correspondantes devant éventuellement être certifiées. La clé publique ainsi certifiée ne peut être utilisée exclusivement que dans le cas suivant : – un contexte de *signature digitale qualifiée* dans le cadre de l'application MyCertipost, auquel cas le Certificat répondra au critère de **Certificat Qualifié** au sens de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001), et du standard technique ETSI TS 101 456 et peut être utilisé dans un contexte de signature avancée ou qualifiée, étant automatiquement équivalente à la signature manuscrite. Le(s) Prestataire(s) de Services de Certification autorisé(s) à délivrer des Certificats selon la présente Politique de Certificat spécifie(nt) s'il(s) déclare(nt) leur conformité à celle-ci et aux documents régulateurs ou s'ils ont été certifiés comme conformes à ceux-ci (voir section D1 §5 du présent document).	
B	***Identification de la Politique de Certificat Qualifié E-Trust pour application MyCertipost***	
	Une Politique de Certificat (CP) est un ensemble déterminé de règles qui indiquent l'applicabilité d'un Certificat à une communauté particulière et/ou une classe d'application ayant des exigences communes en matière de sécurité. Pour les **Certificats Qualifiés pour application MyCertipost**, l'usage est strictement	

Section		Réf. RFC 2527
	réservé au support de la signature digitale devant être supportée par un certificat qualifié, conformément à la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de Certification (Loi du 9 juillet 2001). En plus l'usage du certificat est limité à l'usage strictement dans le cadre des services qui sont offerts via l'application MyCertipost. Les Certificats émis en accord avec la présente CP globale « Certificat Qualifié E-Trust pour application Certipost» incluent l'identifiant de Politique de Certificat qui peut être utilisé par les parties tierces afin de déterminer l'applicabilité et la fiabilité du Certificat en rapport à une application particulière. Les identifiants pour la Politique de Certificat Qualifié E-Trust pour application MyCertipost spécifiées dans le présent document sont repris dans le Tableau 1 ci-dessous. Certificat Qualifié E-Trust pour la Signature Qualifiée et Avancée, dans le cadre de l'application MyCertipost **Tableau 1. Identification de la Politique de Certificat Qualifié E-Trust pour MyCertipost**	

	Certificat Qualifié sans SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** Génération des clés par le titulaire: **0.3.2062.7.1.1.6.2.1**
Certificat Qualifié avec SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** Génération des clés par le CSP: **0.3.2062.7.1.1.6.3.1**	Certificat Qualifié sans SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** Génération des clés par le CSP: **0.3.2062.7.1.1.6.4.1**

C	***Applicabilité***	**1.3.4**
	• Ce type de Certificat constitue une très haute garantie d'identité électronique personnelle ou éventuellement professionnelle pouvant être utilisée pour sécuriser des services dans le cadre de l'application MyCertipost. • Il incombe toutefois aux parties de choisir les applications pour lesquelles elles ont confiance dans le Certificat en fonction de la nature du Certificat et du niveau de sécurité des procédures suivies pour l'émission du Certificat (décrits aux sections B et F de la présente CP). • L'utilisation de la clé (key usage) et l'applicabilité du Certificat sont certifiées (voir la description du contenu du Certificat en section E du présent document). La clé publique ainsi certifiée ne peut être utilisée que dans un contexte de signature avancée ou qualifiée devant être supportée par un certificat qualifié dans le cadre des services de l'application MyCertipost. • Les Certificats Qualifiés émis dans le cadre de cette CP rencontrent les exigences de l'annexe I de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (cf. Loi du 9 juillet 2001). Ils peuvent être utilisés pour supporter les signatures électroniques qui satisfont les exigences d'une signature en relation avec des données sous forme électronique de la même manière qu'une signature manuscrite	

Section		Réf. RFC 2527
	satisfait les exigences en relation avec les données sous forme papier, comme spécifié dans l'article 5.1 de la Directive européenne et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001). Dans ce contexte, cette CP est conforme et rencontre les exigences décrites dans le document « Policy requirements for certification authorities issuing qualified certificates » ETSI TS 101 456 conformément à son chapitre 8 tel que précisé par les clauses reprises dans ce document (voir sections B, C et D du présent document). A cet effet, le Prestataire de Services de Certification publie les éléments supportant cette déclaration de conformité tel qu'indiqué dans la section D du présent document. • Les Certificats émis dans le cadre de cette CP sont émis par une Autorité de Certification qui répond aux exigences de l'annexe II de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (cf. Loi du 9 juillet 2001). • Les Certificats émis dans le cadre de cette CP ne sont pas tous exclusivement destinés à l'utilisation en association avec un Dispositif Sécurisé de Création de Signature (SSCD) au sens de la directive européenne 1999/93/EC. • L'application MyCertipost à laquelle l'utilisation du certificat est limitée, comprend (non-limitatif) la service « electronic registered mail ». Le Certificat Qualifié E-Trust pour application MyCertipost peut être utilisé pour supporter des signatures électroniques dans le cadre du service « electronic registered mail », qui satisfont les exigences d'une signature en relation avec des données sous forme électronique de la même manière qu'une signature manuscrite satisfait les exigences en relation avec les données sous forme papier, comme spécifié dans l'article 5.1 de la Directive européenne et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001).	
D	***Droits, responsabilités et obligations***	***2***
D.1	***Droits, responsabilités et obligations du Prestataire de Services de Certification***	**2.1**
	• Le Prestataire de Services de Certification délivrera des Certificats aux normes • X.509 v3 (ISO 9594-8) • Le Prestataire de Services de Certification émet les Certificats Qualifiés sous le label « Qualified Certificate for MyCertipost application » tel que défini dans et répondant aux exigences de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001), et du standard technique ETSI TS 101 456. A cet effet, le Prestataire de Services de Certification publie les éléments supportant cette déclaration de conformité. • Le Prestataire de Services de Certification garantit que toutes les exigences reprises dans les Politiques de Certificats applicables (reprises dans le Certificat conformément à la section B du présent document) sont respectées et garantit assumer la responsabilité de cette conformité et fournir ces services en conformité avec son CPS. • Informations relatives au(x) Prestataire(s) de Services de Certification autorisé(s) à émettre des Certificats sous la présente CP : - Seuls les CA's suivants sont autorisés : **Certipost** sa via ses services **Certipost E-Trust** et via le **Certipost E-Trust Primary CA for Qualified Certificates** pour l'émission des Certificats Qualifiés pour application MyCertipost. - *Déclarations de Pratiques de Certification (CPS) :* www.e-trust.be/CPS/QNcerts - *Répertoire Publique de Certificats et CRL :* www.e-trust.be/en/x500	

[1] Les données personnelles et les Certificats générés, fournis au Prestataire de Services de Certification et au LRA sont incorporées dans les fichiers de ceux-ci. Ces données seront uniquement utilisées pour la fourniture des services de Certification. Le titulaire de ses données a le droit de consulter celles-ci, de demander leur rectification ou le cas échéant leur suppression.

Section		Réf. RFC 2527
	- *Déclaration de conformité :* www.e-trust.be/CPS/QNcerts - *Autorité de Suspension /Révocation :* 078/15 24 70 (disponible 24h/24 et 7j/7), formulaire de suspension/révocation disponible à l'adresse suivante www.e-trust.be/CPS/QNcerts • Pour procéder à l'enregistrement des candidats titulaires à l'obtention d'un Certificat, le Prestataire de Services de Certification utilise les Autorités d'Enregistrement Locales (Local Registration Autority - LRA) agréées suivantes : - Les bureaux de Poste et autres autorités locales d'enregistrement agréés pour procéder à l'enregistrement des utilisateurs MyCertipost tels que repris dans la liste disponible sur www.mycertipost.be - Les autorités locales d'enregistrement agréés pour procéder à l'enregistrement tels que repris dans la liste disponible sur www.e-trust.be/CPS/QNCerts. • Le Prestataire de Services de Certification garantit uniquement que ses procédures sont implémentées conformément à son CPS et aux Procédures de Contrôle en vigueur et que tout Certificat émis indiquant l'identifiant (Object Identifier - OID) d'une CP a été émis conformément aux stipulations de cette CP, aux procédures de contrôle et à son CPS en vigueur. • Voir les sections 2.1, 2.2, et 2.3 du CPS du Prestataire de Services de Certification en vigueur pour les droits, responsabilités et obligations additionnels du Prestataire de Services de Certification. • Dans certains cas décrits dans la CPS en vigueur (RFC 2527 - section 4.4), le Prestataire de Services de Certification a le droit de révoquer / suspendre le Certificat (moyennant le fait que le Prestataire de Services de Certification avertisse et informe le titulaire du Certificat par des voies appropriées). • Lorsque le Prestataire de Services de Certification est responsable de la génération des clés, celui-ci garantit que toute Paire de Clés générée par ses soins pour le compte d'un titulaire d'un Certificat est générée de façon sécurisée et que le caractère privé de la Clé Privée du titulaire du Certificat est assuré conformément aux exigences de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001), et du standard technique ETSI TS 101 456. • Lorsque le Prestataire de Services de Certification est responsable de la préparation et de la délivrance d'un Dispositif (Sécurisé) de Création de Signature, le Prestataire de Services de Certification garantit que s'il fournit un tel dispositif, celui-ci est fourni de façon sécurisée conformément aux exigences de la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001) et du standard technique ETSI TS 101 456 et que la Paire de Clé sera générée via ce dispositif. • En la matière, le Prestataire de Services de Certification doit respecter la vie privée des personnes concernées et attacher donc une grande importance et faire preuve d'une grande précaution lors du traitement de ces données. Les données personnelles fournies au Prestataire de Services de Certification sont incorporées dans ses fichiers. Les données seront uniquement utilisées pour la fourniture des services de Certification. Le client titulaire du Certificat a le droit de consulter et de modifier ces données.[1] Le Prestataire de Services de Certification s'engage à faire clairement mention des droits du client dans le cadre du respect de la vie privée sur ses contrats de souscription aux Certificats. • Le Prestataire de Services de Certification s'engage également à garantir la confidentialité des données autres que celles publiées dans les Certificats.	
D.2	***Droits, responsabilités et obligations du titulaire du Certificat***	**2.1.3**
	Le titulaire du Certificat accepte la Certification Practice Statement (CPS) en vigueur décrivant les Pratiques utilisées pour fournir les Certificats digitaux et éditée par le	

Section		Réf. RFC 2527
	Prestataire de Services de Certification. Le titulaire du Certificat accepte la présente CP. En particulier, le titulaire du Certificat accepte ce qui suit: • L'accord contractuel relatif à ce type de Certificat est régi par le droit belge. • Le candidat titulaire du Certificat soumet une information précise, correcte et complète au Prestataire de Services de Certification en conformité avec le type de Certificat et la (les) Politique(s) de Certificat reprises en section B du présent document et en particulier en conformité avec les procédures d'enregistrement correspondantes. Le titulaire du Certificat est responsable de l'exactitude des données transmises au Prestataire de Services de Certification. • Le titulaire du Certificat n'utilisera sa Paire de Clés qu'en conformité avec toute limitation qui lui aura été notifiée soit dans le Certificat soit via un accord contractuel. • Lorsque le Prestataire de Certification n'est pas responsable de la génération des clés, le candidat titulaire du Certiifcat est responsable de la génération de sa Paire de Clés et le fera conformément à la Politique de Certificat choisie parmi celles reprises en section B du présent document et en utilisant un algorithme et une longueur de clé (1024 bits minimum) reconnus comme satisfaisant aux exigences de la Politique de Certificat correspondante, conformément aux dispositions contractuelles prises avec le Prestataire de Services de Certification et en particulier, dans le cas d'un Certificat Qualifié, conformément aux exigences d'une signature électronique tel que défini dans la directive européenne 1999/93/EC et sa transposition dans la loi belge fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification (Loi du 9 juillet 2001) et dans le document « Policy requirements for certification authorities issuing qualified certificates » ETSI TS 101 456. De plus, le titulaire du Certificat garantit être le seul à posséder la Clé Privée associée à la Clé Publique devant être certifiée. • Si la CP applicable exige l'utilisation d'un dispositif (sécurisé) de création de signature, la Paire de Clés sera générée via ce dispositif et le Certificat sera utilisé pour créer ces signatures uniquement via ce dispositif. • • Le titulaire du Certificat est contraint de protéger sa clé privée à tout moment contre la perte, la divulgation à une autre partie, la modification et l'utilisation non autorisée, conformément à la CPS en vigueur et à la présente CP. A partir de la création de sa paire de clés privée et publique, le titulaire du Certificat est personnellement responsable de la confidentialité et de l'intégrité de sa clé privée. Tout usage de sa clé privée est supposé être le fait de son propriétaire. Le mot de passe, utilisé pour éviter une utilisation non autorisée de la clé privée ne sera jamais stocké au même endroit que la clé privée elle-même ou à côté de son support de stockage, ne sera jamais stocké sans protection, et bénéficiera d'une protection suffisante. Le titulaire du Certificat ne laissera pas sa clé privée sans surveillance dans un état non verrouillé (ex. : sans surveillance dans une station de travail lorsque le mot de passe a été introduit). Le titulaire du Certificat est seul responsable de l'utilisation de sa clé privée, le Prestataire de Services de Certification n'est pas responsable de l'utilisation de la paire de clés du titulaire du Certificat. • Le titulaire du Certificat demandera au Prestataire de Services de Certification de suspendre ou révoquer son Certificat à chaque fois que cela est requis dans la CPS en vigueur (section 4.4), en particulier lorsque : – La Clé Privée du titulaire du Certificat a été perdue, volée ou potentiellement compromise ; ou – Le titulaire du Certificat a perdu le contrôle sur sa Clé Privée en raison d'une compromission des données d'activation de celle-ci (par exemple, mot de passe) ou pour une autre raison ; et/ou – Les données certifiées sont devenues inexactes ou ont changé. Son Certificat sera alors révoqué immédiatement. Les procédures de suspension et de révocation sont décrites dans la section J du présent document • Le titulaire du Certificat doit informer immédiatement les Services de Certification du Prestataire de Services de Certification de toute modification dans les informations contenues dans son Certificat. Son Certificat sera alors révoqué immédiatement.	

Section		Réf. RFC 2527
	• Le client titulaire du Certificat doit informer le Prestataire de Services de Certification de toute modification dans les informations non présentes dans le Certificat, mais ayant été transmises au Prestataire de Services de Certification lors de l'enregistrement. Le Prestataire de Services de Certification rectifiera les informations enregistrées. • Le titulaire du Certificat doit d'initiative demander la révocation de son Certificat si les informations transmises au Prestataire de Services de Certification pour prouver une qualité professionnelle devenaient en tout ou en partie obsolètes. • Le titulaire du Certificat accepte que son Certificat digital soit publié immédiatement après sa création dans le Certificate Public Registry (Registre Public de Certificat) du Prestataire de Services de Certification. • Le Certificat est réputé accepté par le titulaire du Certificat dès la survenance du premier des événements suivants, soit le 8ième jour après sa publication sur le Registre Public de Certificat (Certificate Public Registry) du Prestataire de Services de Certification, soit au moment de la première utilisation par le titulaire du Certificat. Pendant la période susmentionnée, le titulaire du Certificat est responsable de la vérification de l'exactitude du contenu de son Certificat publié. Si le titulaire du Certificat remarque une incohérence entre les informations de l'accord contractuel et le contenu de son Certificat, il doit en informer le Prestataire de Services de Certification sans délai. Le Prestataire de Services de Certification révoquera alors le Certificat et prendra les mesures appropriées pour ré-émettre un certificat. Ceci constitue le seul recours du Client concernant la non-acceptation du Certificat. • Le titulaire du Certificat accepte la conservation pour une période de 30 ans par le Prestataire de Services de Certification et l'Autorité d'Enregistrement Locale, de toute information utilisée pour l'enregistrement, pour la fourniture éventuelle d'un Dispositif (Sécurisé) de Création de Signature, pour procéder à une suspension ou révocation du Certificat et la transmission de cette information à des tierces parties sous les mêmes conditions que requises dans la présente CP dans le cas d'une cessation des activités du Prestataire de Services de Certification. • Le titulaire du Certificat accepte les droits, obligations et responsabilités du Prestataire de Services de Certification. Ils sont décrits dans la CPS en vigueur, le bon de commande et les conditions générales afférentes et la présente CP (section D1).	
D.3	***Droits, responsabilités et obligations de l'Autorité d'Enregistrement Locale (LRA)***	
	L'Autorité d'Enregistrement Locale (LRA) est tenue contractuellement de respecter scrupuleusement les procédures d'enregistrement décrites dans les Déclarations de Pratiques de Certification (CPS) du Prestataire de Services de Certification (voir section D.1 §5). La LRA, garantit : • Que les titulaires d'un Certificat sont correctement identifiés et authentifiés, tant au niveau de l'identité personnelle du titulaire du Certificat en tant que personne physique, qu'au niveau des éventuelles mentions relatives à la qualité professionnelle de celui-ci. • Que, le cas échéant, les requêtes de Certificats transmises au Prestataire de Services de Certification sont complètes, correctes, valides et dûment autorisées. En particulier : • L'officier d'enregistrement informe le titulaire du Certificat des termes et conditions relatifs à l'utilisation du Certificat. Ceux-ci sont repris dans le Bon de Commande et les Conditions Générales à signer par le titulaire du Certificat (format papier ou électronique notarisé). • L'officier d'enregistrement vérifie l'identité du titulaire du Certificat sur la base de document(s) d'identité valide(s) et reconnu(s) par la législation belge. Ce(s) document(s) reprenant notamment le nom complet (nom de famille et prénoms), date et lieu de naissance, adresse physique du titulaire du Certificat dans le but de permettre le contact avec celui-ci. • L'officier d'enregistrement vérifie, dans le but de leur Certification tel que repris à la	

Section		Réf. RFC 2527
	section E du présent document, les éventuelles mentions relatives à la qualité professionnelle du titulaire du Certificat. • Dans le cas où le titulaire du Certificat serait associé à une personne morale, une preuve de cette association est validée par l'officier d'enregistrement. • L'officier d'enregistrement fera procéder à l'archivage d'une copie des informations fournies lors de la procédure d'enregistrement par le titulaire du Certificat et transmises dans leur intégralité au Prestataire de Services de Certification; en particulier : – Copie de toute information utilisée pour vérifier l'identité et les éventuelles mentions relatives à la qualité professionnelle du candidat titulaire du Certificat, incluant tout numéro de référence sur la documentation utilisée pour vérification et toute limitation sur sa validité, – Copie de l'accord contractuel signé par le titulaire du Certificat, incluant l'accord de celui-ci sur l'ensemble de ses obligations. Ces informations seront conservées pour une période de 30 ans. • Le respect des exigences relatives à la protection des données personnelles dans le cadre des opérations d'enregistrement. La LRA est tenue contractuellement de prendre les mesures précises et appropriées vis à vis : • De la sécurité physique des informations et le cas échéant des systèmes ; • De l'accès logique aux logiciels éventuels; • Du personnel en charge de l'enregistrement. La classification des données et la responsabilité sur ces données sont cruciales, sont concernées : • Les données elles-mêmes, sous forme papier (données d'enregistrement, guides et procédures, …), et le cas échéant, sous forme électronique ; • Les logiciels utilisés et leur configuration ; • Les équipements (hardware, outils de télécommunications, …), et leur configuration ; • Les accès physiques aux données (bâtiments, coffres forts, contrôle d'accès et accès conditionnel aux logiciels, …). La LRA garantit que ces éléments sont gérés et classés afin d'éviter des impacts possibles dus à une perte de confidentialité, d'intégrité voire de disponibilité de ces éléments.	
D.4	***Droits, responsabilités et obligations de la société (ou Organisation) du titulaire du Certificat (le cas échéant)***	
	La Société (ou Organisation), représentée par son représentant légal, approuve l'enregistrement du titulaire du Certificat dans le cadre de l'obtention du Certificat devant certifier une qualité professionnelle impliquant la Société (ou Organisation). La Société (ou Organisation) approuve: • la Certification Practice Statement (CPS) en vigueur éditée par le Prestataire de Services de Certification et décrivant les Pratiques utilisées pour fournir les Certificats. • la présente Certificate Policy (CP) du Certificat Qualifié E-Trust pour application Certipost. En particulier, la Société (ou Organisation) accepte ce qui suit: • La Convention entre la Société (ou l'Organisation), le titulaire du Certificat et le Prestataire de Services de Certification est régie par le droit belge • La Société (ou Organisation) adhère à toutes les responsabilités du Client décrites dans le contrat Client. • La Société (ou Organisation) est responsable de l'exactitude des données transmises par celle-ci au Prestataire de Services de Certification dans le cadre de l'enregistrement du titulaire de Certificat. En cas de modification de ces informations, la Société (ou	

Section		Réf. RFC 2527
	Organisation) en informera immédiatement les Services du Prestataire de Services de Certification, qui réagiront en conséquence. • Dans certains cas décrits dans la CPS en vigueur (section 4.4), le Prestataire de Services de Certification a le droit de révoquer / suspendre le Certificat d'un titulaire (moyennant le fait que le Prestataire de Services de Certification avertisse et informe le titulaire du Certificat et la Société (ou Organisation) par des voies appropriées). • La Société (ou Organisation) demandera au Prestataire de Services de Certification de suspendre ou de révoquer le Certificat à chaque fois que cela est requis dans la CPS en vigueur (section 4.4). Les procédures de suspension et de révocation sont décrites dans la CPS en vigueur (section 4.4). • La Société (ou Organisation) accepte les droits, obligations et responsabilités du Prestataire de Services de Certification. Ils sont décrits dans la CPS en vigueur, le contrat et la présente CP (section D).	

D.5 ***Droits, responsabilités et obligations des tiers***

Les tiers qui se basent sur les Certificats émis selon la présente CP :

- Vérifient la validité du Certificat en vérifiant le contenu et la signature du Prestataire de Services de Certification sur le Certificat et le cas échéant la chaîne de Certification associée, l'état de suspension ou de révocation éventuelle du Certificat, du Certificat du Prestataire de Services de Certification ayant émis le Certificat ou d'un Certificat de la chaîne de Certification qui y est éventuellement associée, en se référant aux Listes de Révocation des Certificats (CRLs) du Prestataire de Services de Certification (voir section D.1 §5 du présent document).
- Tiennent compte de toutes les limitations sur l'usage du Certificat décrites dans le Certificat, les documents contractuels et la présente CP.
- Prennent toutes autres précautions prescrites dans la présente CP ou ailleurs quant à l'usage du Certificat.

E ***Identification et Authentification - Informations certifiées*** **3.1**

Les informations suivantes sont vérifiées (voir section G: "Procédure de demande de Certificat" de la présente CP) et certifiées dans le Certificat Qualifié E-Trust pour application MyCertipost dans l'ordre suivant :

Attribut	**Obligatoire / Optionnel/Fixé**	**Valeur**
Distinguished Name		
Country (C)	Obligatoire	Nationalité du titulaire du Certificat (Pays)
Locality (L)	Obligatoire	Lieu de naissance du titulaire du Certificat (Localité)
Organisation (O)	Obligatoire	Pour des personnes physiques, il s'agit de mention « Private Person », pour des organisations, il s'agit du nom officiel de la Société (ou Organisation) employant le titulaire du Certificat (tel que publié dans les statuts de la Société (ou Organisation))
OrganisationalUnit (OU)	Fixé	« Limitation on transaction value: Not applicable »
OrganisationalUnit (OU)	Fixé	« Limitation on certificate usage: for use within Certipost application only»
OrganisationalUnit (OU)	Obligatoire	"Date of birth: <jj/mm/aaaa>" (Date de naissance du titulaire du Certificat)
CommonName (CN)	Obligatoire	Nom et Prénom(s) du titulaire du Certificat tels que repris sur sa carte d'identité ou document équivalent.
Extensions :		
KeyUsage	Fixé	NonRepudation
subjectPublicKey	Fixé	Clé publique: longueur de clé: minimum 1024 bit; exposant pulic : Fermat-4 (=010001)
CertificatePolicies-policyIdentifier	Fixé	Voir tableau 1.
CertificatePolicies-policyQualifier-userNotice	Fixé	«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	Fixé	http://www.e-trust.be/CPS/QNcerts
0.3.2062.7.1.5.1.1	Fixé	«E-Trust Qualified Certificate for Use within MyCertipost application only»

subjectKeyIdentifier	Fixé	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	Fixé	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	Fixé	0.4.1862.1.1 { id-etsi-qcs 1}
Other information :		
Issuer	Fixé	«CN = Certipost E-Trust Primary CA for qualified certificates O = Certipost C = BE»
Validity	Fixé	1 an
SerialNumber	Fixé	Numéro de série du certificat
Algorithm	Fixé	"Sha1withRSAEncryption"
Version	Fixé	2 (en conformité avec v3)

Remarquez que l'extension critique « 0.3.2062.7.1.5.1.1 » est une extension privée de E-Trust, qui a comme but d'indiquer clairement que ce certificat ne peut être utilisé que dans le cadre des services qui sont offert par l'application Certipost.
A ces informations certifiées, est accolée la signature de l'autorité de Certification portant sur l'ensemble des informations certifiées.

F *Procédure de génération des clés*

La taille des clés doit être au minimum de 1024 bits.

Génération des clés par le titulaire du Certificat

Le candidat titulaire du Certificat procède lui-même à la génération de sa Paire de Clés. Dans le cadre d'un enregistrement effectué lors de la procédure d'inscription au service Certipost auprès d'une LRA agréée à cet effet, le candidat titulaire du Certificat procédera à la génération de la paire de clés et la demande électronique sécurisée au sein de son environnement sécurisé MyCertipost.

Génération des clés par le Prestataire de Services de Certification ou l'Autorité d'Enregistrement Locale

Si le candidat titulaire du Certificat désire faire procéder à la génération de sa paire de clés par le Prestataire de Services de Certification et sur accord contractuel du candidat titulaire, trois cas peuvent se présenter :

1. L'Officier LRAO dispose d'un logiciel de génération de clés et requête de certificat :
   - L'Officier LRAO procède à la génération des clés :
     - L'Officier LRAO demande au candidat titulaire du Certificat d'introduire le mot de passe (ou code PIN) qui protégera ses clés.
     - L'Officier LRAO copie les clés sous format standard PKCS sur le support choisi (par exemple, disquette ou SSCD). Les clés se présentent sous forme d'un fichier protégé par le mot de passe (ou code PIN) choisi par le candidat titulaire du Certificat.
   - L'Officier LRAO procède à la génération de la requête PKCS#10
   - L'Officier LRAO efface toute trace des clés du candidat titulaire du Certificat sur son environnement logiciel et matériel. Les clés ne sont présentes que sur le

support remis au titulaire du Certificat.

2. L'Officier LRAO ne dispose pas de logiciel de génération de clés et de requête de certificat et transmet la requête à l'Officier CRAO :
   - L'Officier CRAO (Central Registration Authority Officer) procède à la génération des clés
   - L'Officier CRAO procède à la génération de la requête PKCS#10

3. Dans le cadre d'un enregistrement effectué lors de la procédure d'inscription au service MyCertipost auprès d'une LRA accréditée à cet effet, le candidat titulaire du Certificat pourra, dans la mesure où ce service sera disponible, au sein de son environnement et compte sécurisé MyCertipost, demander au Prestataire de Services de Certification de générer sa paire de clés et la demande électronique de certificat. Ceci peut s'effectuer dans et via un Dispositif Sécurisé de Création de Signature. Ce Dispositif Sécurisé de Création de Signature lui sera alors remis en mains propres par courrier recommandé physique avec accusé de réception, tandis que le mot de passe (ou PIN) protégeant celui-ci lui sera fourni de façon sécurisée par un autre canal.
   Si la génération de la paire de clés ne s'effectue pas dans et via un Dispositif Sécurisé de Création de Signature, Certipost envoiera la clé privée encryptée dans son environnement sécurisé MyCertipost. La code qui protège sa clé privée lui sera envoyée via un autre chemin.

G ***Procédure de demande du Certificat***

- Le client dispose préablement d'un **account MyCertipost**.

- Si le Client désire de générer sa paire de clés lui-même (seulement pour usage privé) : Le Client remplit, dans son environnement sécurisé personnel MyCertipost auquel il aura accès au moyen de ses codes d'accès, le bon de commande du type Certificat Qualifié pour personne privée.

- Si le client désire que Certipost génère son pair de clés (seulement pour des employées) :
  Le Client désire acquérir un Certificat pour un usage professionnel. A cette fin, il remplit le bon de commande du type Certificat Qualifié pour employée pour usage limitée à l'application MyCertipost.
  Le bon de commande est disponible à l'adresse Internet suivante : http://www.e-trust.be/CPS/QNCerts.
  Le Client remplit le bon de commande et le signe. Le Client faxe son bon de commande vers les Services de Régistration de Certipost E-Trust. Les coordonnées sont disponible sur le site http://www.e-trust.be/CPS/QNCert.
  Le Client remplit ce Bon de Commande et le signe. Le Client faxe ce Bon de Commande au service de registration de Certipost. Les coordonnées du service de registration de Certipost sont disponibles à http://www.e-trust.be/CPS/QNCerts.

- En remplissant et en signant le Bon de Commande, le Client accepte les présentes Conditions Générales, ainsi que la "Certificate Policy" (ci-après la "CP") et le "Certification Practice Statement for Qualified or Normalised Certificates" (ci-après le "CPS"), relatifs aux Certificats Qualifiés ou Normalisés E-Trust, tels que ces documents sont disponibles en ligne à l'adresse Internet suivante : http://www.e-trust/CPS/QNcerts, et dont le Client reconnaît avoir pris connaissance, lesquels documents formeront, avec le Bon de Commande, la convention des Parties (ci-après la "Convention").

Validation :

Dans le cas d'une requête électronique via le Bon de Commande en ligne disponible dans son environnement sécurisé personnel Certipost la seconde vérification du dossier est effectuée a posteriori par l'Auditeur de l'Autorité de Certification (Certification

	Authority Auditor -- CAA) du Prestataire de Services de Certification qui vérifie la cohérence entre les Certificats émis et les dossiers reçus des LRA.	
H	***Emission du Certificat***	**4.2**
	– Si le Client a généré lui-même son pair de clés (seulement pour usage privée), l'émission du Certificat sera effectuée en ligne dans le cours de la procédure de commande de certificats pour application MyCertipost. – Si Certipost a généré le pair de clé pour lui, Certipost envoiera sa clé privé encryptée dans son compte sécurisé MyCertipost. Le code, nécessaire afin de décrypter sa clé privée sera communiqué via un chemin sécurisé différent. Si Certipost a crée le pair de clé sur un SSCD, Certipost envoiera le code PIN via son compte sécurisé. Le SSCD lui sera envoyé via un chemin sécurisé différent.	
I	***Acceptation du Certificat et Publication du Certificat***	**4.3**
	Publication du Certificat dans le Registre Public de Certificats du Prestataire de Services de Certification. Une fois le Certificat émis par le Prestataire de Services de Certification, il est publié immédiatement dans le Registre Public de Certificat du Prestataire de Services de Certification. Ce Registre est public et accessible en permanence. *Acceptation* • Le titulaire du Certificat, et le cas échéant l'Organisation, accepte que son Certificat digital soit publié immédiatement après sa création dans le Registre Public de Certificat du Prestataire de Services de Certification. • Le Certificat est réputé accepté par le titulaire du Certificat, et le cas échéant l'Organisation, dès la survenance du premier des événements suivants, soit le 8ième jour après sa publication sur le Registre Public de Certificat (Certificate Public Registry) du Prestataire de Services de Certification, soit au moment de la première utilisation par le titulaire du Certificat. Pendant la période susmentionnée, le titulaire du Certificat, et le cas échéant l'Organisation, sont responsable de la vérification de l'exactitude du contenu de son Certificat publié. Si le titulaire du Certificat, ou le cas échéant l'Organisation, remarque une incohérence entre les informations de l'accord contractuel et le contenu de son Certificat, il/elle doit en informer le Prestataire de Services de Certification sans délai. Le Prestataire de Services de Certification révoquera alors le Certificat et prendra les mesures appropriées pour ré-émettre un Certificat. Ceci constitue le seul recours concernant la non-acceptation du certificat.	
J	***Procédure de Suspension/ Réhabilitation après Suspension / Révocation***	**4.4**
	Le titulaire d'un Certificat, le représentant légal (ou son délégué mandaté) de l'Organisation pour le cas des Certificats d'employés, et la LRA peuvent demander la suspension, la réhabilitation après suspension ou la révocation du Certificat. Le titulaire d'un Certificat et si applicable le représentant légal (ou son délégué mandaté) seront avertis lors de la suspension, la réhabilitation après suspension ou la révocation du Certificat. Les informations relatives au statut de la suspension ou révocation d'un Certificat sont mises à disposition de tous, en tout temps, par le Prestataire de Services de Certification comme indiqué en section D1 §5 du présent document. Un formulaire de suspension / réhabilitation après suspension / révocation est mis à disposition des parties par le Prestataire de Services de Certification à l'adresse suivante : http://www.e-trust.be/CPS/QNcerts). Les demandes et rapports liés à une suspension ou une réhabilitation après suspension ou une révocation, seront traités dès leur réception, authentifiés et confirmés de la façon	

	suivante : Dans le cas d'une **suspension**: • Le demandeur doit contacter l'Autorité de Suspension Révocation (Suspension Revocation Authority – SRA) du Prestataire de Services de Certification ayant émis le Certificat concerné pour demander à recevoir un formulaire de demande de suspension d'un Certificat ou utiliser celui disponible à l'adresse suivante : http://www.e-trust.be/CPS/QNcerts. • La SRA procédera à un call back pour obtenir la confirmation de la demande de suspension. • La SRA procédera à la suspension effective du Certificat à dater de la réception de la demande. Le formulaire doit être envoyé par fax ou par courrier postal au Prestataire de Services de Certification dans les 14 jours ouvrables faute de quoi le Certificat sera réhabilité. • La suspension d'un Certificat sera établie pour une période d'un (1) mois. Après cette période, une nouvelle demande de suspension doit être introduite pour prolonger la période de suspension d'un (1) mois, dans le cas contraire, le certificat sera automatiquement révoqué. Dans le cas d'une **réhabilitation après suspension**: • Le demandeur doit contacter l'Autorité de Suspension Révocation (Suspension Revocation Authority – SRA) du Prestataire de Services de Certification ayant émis le Certificat concerné pour demander à recevoir un formulaire de demande de réhabilitation après suspension d'un Certificat ou utiliser celui disponible à l'adresse suivante : http://www.e-trust.be/CPS/QNcerts. • Le demandeur doit prendre rendez-vous avec une Autorité d'Enregistrement Locale agréée par le Prestataire de Services de Certification et se présenter avec le formulaire dûment rempli et la copie (recto/verso) signée de sa carte d'identité. • L'Officier de l'Autorité d'Enregistrement Locale procédera à la vérification des documents fournis et de l'identité du demandeur. Si la requête est validée, l'Officier transmettra la demande à la SRA. • La SRA procédera à la réhabilitation du Certificat endéans les 24 heures à dater de la réception de la demande. Dans le cas d'une **révocation**, le demandeur doit: • Le demandeur doit procéder à la demande de suspension du Certificat (voir ci-dessus) • Le demandeur doit contacter la SRA pour demander à recevoir un formulaire de demande de révocation de Certificat ou utiliser celui disponible à l'adresse suivante : http://www.e-trust.be/CPS/QNcerts. • Le demandeur doit prendre rendez-vous avec une Autorité d'Enregistrement Locale agréée par le Prestataire de Services de Certification et se présenter avec le formulaire dûment rempli et la copie (recto/verso) signée de sa carte d'identité. • L'Officier de l'Autorité d'Enregistrement Locale procédera à la vérification des documents fournis et de l'identité du demandeur. Si la requête est validée, l'Officier transmettra la demande à la SRA. La SRA procédera à la révocation du Certificat à dater de la réception de la demande de révocation. • Le Certificat sera révoqué (ou réhabilité) après une période d'investigation de maximum 10 jours ouvrables. • La révocation d'un Certificat est définitive.	
K	***Procédure de renouvellement des clés, du Certificat et de mise à jour***	
	Le Prestataire de Services de Certification s'assure que les requêtes émises par le titulaire d'un Certificat qui a déjà été préalablement valablement enregistré sont complètes, valides et autorisées. Ceci inclut le renouvellement du Certificat et/ou des clés suivant une révocation ou suite à l'approche de l'échéance. Le Prestataire de Services de Certification s'assure : • Que l'information utilisée pour vérifier l'identité du client titulaire du Certificat est toujours valide, et pour ce faire, – la même procédure que lors de l'enregistrement initial est prévue (cfr. Point G de la	

	présente CP), OU – dans le cas d'un renouvellement et pour autant que les clés et le Certificat du titulaire du Certificat soient toujours valides (non révoqués, suspendus ou expirés), le Prestataire de Services de Certification acceptera une requête signée électroniquement par la clé privée dont la clé publique est certifiée et accompagnée d'un texte, également dûment signé électroniquement, stipulant qu'aucune information du dossier n'a changé depuis la demande précédente, pour autant que le key usage du certificat en question permette la signature. • Si les termes et conditions générales du Prestataire de Services de Certification ont changé, le Prestataire de Services de Certification les communiquera au client titulaire du Certificat • Le Prestataire de Services de Certification n'émettra un Certificat pour une clé précédemment certifiée que si la sécurité des paramètres cryptographiques relatifs à cette clé est toujours suffisante et que la clé en question n'a pas été compromise.	
L	***Protection de la vie privée et des données personnelles***	
	Les informations collectées par E-Trust ou l'autorité d'enregistrement (document papier et informations électroniques) et fournies par le titulaire du Certificat dans le cadre de la demande de Certificat et de la livraison sont dûment archivées et protégées selon la Loi belge sur la protection de la vie privée[2] (cf. la notice sur ce point reprise dans les conditions générales).	
M	***Plaintes et règlement de conflits***	
	• En cas de problèmes techniques ayant trait au Certificat et en cas de plaintes ayant trait aux services fournis sur base de la présente Politique de Certificat, le titulaire du Certificat peut prendre contact avec le helpdesk du Prestataire de Services de Certification: - Certipost E-Trust : - Numéro de téléphone : 070/22 55 33 - Numéro de fax : 070/22 55 01 - E-mail : feedback.fr@contact.certipost.be Le Prestataire de Services de Certification et le titulaire du Certificat s'engagent à tout mettre en œuvre afin de trouver un règlement à l'amiable pour tout conflit relatif à la validité, l'interprétation ou l'exécution de la convention qui les lie. A défaut d'un règlement à l'amiable, le conflit relatif à la validité, l'interprétation ou l'exécution de la convention qui les lie sera porté devant les tribunaux de Bruxelles.	

[2] Afin d'exécuter ces tâches efficacement, Certipost utilise des bases de données avec ces données personnelles. En la matière, Certipost doit respecter la vie privée des personnes concernées et attacher donc une grande importance et faire preuve d'une grande précaution lors du traitement de ces données. Les données personnelles fournies à Certipost sont incorporées dans les fichiers de CERTIPOST S.A., Quai de Willebroeck, 22, 1000 Bruxelles. Les données seront uniquement utilisées pour la fourniture des services Certipost E-Trust. Vous avez le droit de consulter et de modifier ces données.