Politique de Certificat relative au Certificat Qualifié ou Normalisé E-Trust Pour Personnes Morales

Version 1.1

–

Date de publication : Décembre 2003

Certipost agit en tant que prestataire de service de certification ayant repris entièrement les activités et les responsabilités de Belgacom E-Trust en la matière. Lors de la création de Certipost, l'entièreté de l'activité E-Trust de Belgacom a été transférée vers Certipost.

Politique de Certificat (Certificate Policy - CP) relative au Certificat Qualifié ou Normalisé E-Trust pour personnes morales

Ce document décrit l'applicabilité du certificat de type « Certificat Qualifié ou Normalisé E-Trust pour personnes morales» (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 ou Normalisés qui satisfait aux conditions suivantes et au document Procédures de Contrôle du Prestataire de Services de Certification:

Section		Réf. RFC 2527
A	***Aperçu de la Politique de Certificat Qualifié ou Normalisé E-Trust pour personnes morales***	**1.1**
	Très haut niveau d'assurance quant à l'identité électronique d'une personne morale (ci-après aussi dénommée l'Entreprise) et éventuellement d'un service au sein de cette personne morale comme titulaire du Certificat. Il s'agit d'un Certificat dont la délivrance est conditionnée à la présentation personnelle d'un responsable mandaté représentant la personne morale durant le processus d'enregistrement (ci-après dénommé le Demandeur). Ce Certificat fournit un niveau très élevé de garantie pour assurer le lien entre l'identité électronique d'une personne morale et éventuellement d'un service au sein de cette personne morale, une clé publique et son usage autorisé. Ce Certificat fournit le degré le plus élevé de garantie d'authentification correcte puisque le Demandeur du Certificat doit : – être un responsable dûment mandaté comme représentant la personne morale et ; – 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 Demandeur du Certificat et la vérification des pièces fournissant la preuve de son mandat de représentant de la personne morale et des informations correspondantes devant éventuellement être certifiées. La clé publique ainsi certifiée ne peut être utilisée exclusivement que dans l'un des deux cas suivants : – un contexte de *signature digitale supportée par un certificat qualifié* 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 (cf. Loi du 9 juillet 2001), et du standard technique ETSI 101 456 ; ou (exclusif) – tout autre contexte (e.g., signature digitale normalisée, chiffrement et/ou authentification, ou toute combinaison de ceux-ci, etc.) auquel cas le Certificat répondra au critère de « **Certificat Normalisé** » au sens du standard technique ETSI 102 042. 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	

Section		Réf. RFC 2527
	documents régulatoires ou s'ils ont été certifiés comme conformes à ceux-ci (voir section D1 §5 du présent document). Les Certificats (et les Paires de Clés) utilisés pour la signature digitale devant être supportée par un certificat qualifié sont toujours distincts des certificats de type normalisé.	
B	***Identification de la Politique de Certificat Qualifié ou Normalisé E-Trust pour personnes morales***	
	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. Le présent document reprend et identifie au sein de la même CP globale « **Certificat Qualifié ou Normalisé E-Trust pour personnes morales** » plusieurs Politiques de Certificats suivant l'usage qui peut être fait du Certificat, suivant que la génération de la Paire de Clés a été faite par le Demandeur du Certificat ou par le Prestataire de Services de Certification et suivant que la Clé Privée a été générée et ne peut être utilisée que dans un Dispositif Sécurisé de Création de Signature (Secure Signature Creation Device – SSCD) ou pas. Il en découle deux grands types de Certificats. D'un côté, les **Certificats Qualifiés** dont l'usage est strictement 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 (cf. Loi du 9 juillet 2001). De l'autre côté, les **Certificats Normalisés** dont l'usage est soit le chiffrement, soit l'authentification, soit la signature digitale normalisée (à l'exclusion donc des signatures devant être supportées par un certificat qualifié), soit une combinaison des usages précédents. Ces Certificats sont compatibles avec et satisfont les exigences fournies dans les standards techniques respectivement ETSI 101 456 et ETSI 102 042. Les Certificats émis en accord avec la présente CP globale « Certificat Qualifié ou Normalisé E-Trust pour personnes morales » incluent un ou plusieurs identifiants de Politique de Certificat qui peuvent être utilisés par les parties tierces afin de déterminer l'applicabilité et la fiabilité du Certificat en rapport à une application particulière. Les identifiants pour les Politiques de « Certificat Qualifié ou Normalisé E-Trust pour personnes morales » spécifiées dans le présent document sont repris dans le Tableau 1 ci-dessous.	

Section		Réf. RFC 2527

Certificat Qualifié E-Trust pour personnes morales (pour la Signature Qualifiée uniquement)

	Certificat Qualifié sans SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** Génération des clés par le titulaire: **0.3.2062.9.6.1.25.2.1**
Certificat Qualifié avec SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** Génération des clés par le CSP: **0.3.2062.9.6.1.25.3.1**	Certificat Qualifié sans SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** Génération des clés par le CSP: **0.3.2062.9.6.1.25.4.1**

Certificat Normalisé E-Trust pour personnes morales

	Certificat Normalisé sans SSCD (OID ETSI 102 042) **0.4.0.2042.1.1** et Génération des clés par le titulaire: **0.3.2062.9.6.1.25.6.1**
Certificat Normalisé avec SSCD (OID ETSI 102 042) **0.4.0.2042.1.2** et Génération des clés par le CSP: **0.3.2062.9.6.1.25.7.1**	Certificat Normalisé sans SSCD (OID ETSI 102 042) **0.4.0.2042.1.1** et Génération des clés par le CSP: **0.3.2062.9.6.1.25.8.1**

Tableau 1. Identification de la Politique de Certificat Qualifié ou Normalisé E-Trust pour personnes morales

C	***Applicabilité***	**1.3.4**

- Ce type de Certificat constitue une très haute garantie quant à l'identité électronique d'une personne morale et éventuellement d'un service au sein de cette personne morale comme titulaire du Certificat et pouvant être utilisée pour sécuriser des applications de niveau de sécurité élevé telles que les opérations, par exemple, soit de signature digitale devant être supportée par un certificat qualifié, soit de chiffrement/authentification/signature normalisée.
- 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 digitale devant être supportée par un certificat qualifié ou (exclusif) tout autre usage « normalisé » (à l'exception donc de la signature digitale automatiquement équivalente à la signature manuscrite). Les Certificats (et les Paires de Clés) utilisées pour la signature digitale devant être supportée par un certificat qualifié sont toujours distincts des autres certificats de type normalisés.
- 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 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 (cf. Loi du 9 juillet 2001). Dans ce contexte, cette CP est conforme et rencontre les exigences décrites dans le document « Policy requirements for certification

Section		Réf. RFC 2527
	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 Normalisés émis dans le cadre de cette CP rencontrent les exigences du standard technique ETSI TS 102 042. • 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.	
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 » 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 (cf. Loi du 9 juillet 2001), et du standard technique ETSI 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 émet les Certificats Normalisés sous le label « Normalised Quality Certificate » tel que défini dans et répondant aux exigences du standard technique ETSI 102 042. 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 CAs suivants sont autorisés : **Certipost sa/nv** en tant que Prestataire de Services de Certification, via ses services **Certipost E-Trust** ayant repris le **Belgacom E-Trust Primary CA for Qualified Certificates** pour l'émission des Certificats Qualifiés et le **Belgacom E-Trust Primary CA for Normalised Certificates** pour l'émission des Certificats Normalisés: - *Déclarations de Pratiques de Certification (CPS) :* www.e-trust.be/CPS/QNcerts - *Répertoire Publique de Certificats et CRL :* www.e-trust.be/en/x500 - *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	

[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
	• Pour procéder à l'enregistrement des candidats titulaires d'un Certificat, le Prestataire de Services de Certification utilise les Autorités d'Enregistrement Locales (Local Registration Autority - LRA) agréées suivantes : - Les membres du personnel de Belgacom et de Certipost habilités par le Prestataire de Services de Certification susmentionné comme autorités d'enregistrement. La liste authentifiée de ces LRA habilités est disponible sur www.e-trust.be/CPS/QNcerts • Le Prestataire de Services de Certification garantit uniquement que ses procédures sont implémentées conformément à sa 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 Demandeur, et le cas échéant 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 du Demandeur/titulaire d'un Certificat est générée de façon sécurisée et que le caractère privé de la Clé Privée du Demandeur/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 (cf. Loi du 9 juillet 2001), et du standard technique ETSI TS 101 456 et TS 102 042. • 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 (cf. Loi du 9 juillet 2001) et du standard technique ETSI TS 101 456 et TS 102 042 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 Demandeur du Certificat, et l'Entreprise titulaire du Certificat, ont 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 Demandeur du Certificat***	**2.1.3**
	Le Demandeur du Certificat accepte la Certification Practice Statement (CPS) en vigueur décrivant les Pratiques utilisées pour fournir les Certificats digitaux et éditée par le Prestataire de Services de Certification. Le Demandeur du Certificat accepte la présente CP. En particulier, le Demandeur du Certificat accepte ce qui suit:	

Section		Réf. RFC 2527
	• L'accord contractuel relatif à ce type de Certificat est régi par le droit belge. • Le Demandeur 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 Demandeur du Certificat est responsable de l'exactitude des données transmises au Prestataire de Services de Certification. • Le Demandeur 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 Services de Certification n'est pas responsable de la génération des clés, le Demandeur du Certificat 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 (cf. Loi du 9 juillet 2001) et dans le document « Policy requirements for certification authorities issuing qualified certificates » ETSI TS 101 456. De plus, le Demandeur 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 Demandeur 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 Demandeur 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 code PIN (Personal Identity Number) ou le mot de passe, utilisé pour éviter une utilisation non autorisée de la clé privée ne devra jamais être stocké au même endroit que la clé privée elle-même ou à côté de son support de stockage, ne devra jamais être stocké sans protection, et devra bénéficier d'une protection suffisante. Le Demandeur 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 code PIN ou le mot de passe a été introduit). Le Demandeur 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 Demandeur du Certificat. • Le Demandeur 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 Demandeur du Certificat a été perdue, volée ou potentiellement compromise ; ou – Le Demandeur du Certificat a perdu le contrôle sur sa Clé Privée en raison d'une compromission des données d'activation de celle-ci (par exemple, code PIN) 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 Demandeur 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. • Le Demandeur du Certificat doit informer le Prestataire de Services de Certification de	

Section		Réf. RFC 2527
	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 Demandeur du Certificat doit d'initiative demander la révocation de son Certificat si les informations transmises au Prestataire de Services devenaient en tout ou en partie obsolètes. • Le Demandeur 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 Demandeur 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 Demandeur du Certificat. Pendant la période susmentionnée, le Demandeur du Certificat est responsable de la vérification de l'exactitude du contenu de son Certificat publié. Si le Demandeur 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 Demandeur 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 Demandeur 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 Demandeurs et titulaires d'un Certificat sont correctement identifiés et authentifiés, tant au niveau de l'identité personnelle du Demandeur du Certificat en tant que personne physique, qu'au niveau de la représentativité de ce Demandeur et des éventuelles délégations de mandat afin de représenter valablement la personne morale future titulaire du Certificat, et des informations relatives à cette personne morale titulaire du Certificat. – 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 Demandeur 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 Demandeur du Certificat (format papier ou électronique notarisé). – L'officier d'enregistrement vérifie l'identité du Demandeur du Certificat sur la base de document(s) d'identité valide(s) et reconnu(s) par la législation belge. Ce(s) document(s)	

Section		Réf. RFC 2527
	reprenant notamment le nom complet (nom de famille et prénoms), date et lieu de naissance, adresse physique du Demandeur du Certificat dans le but de permettre le contact avec celui-ci. – L'officier d'enregistrement vérifie les éventuelles mentions relatives à la représentativité du Demandeur par rapport à la personne morale qu'il est censé représenter. – L'officier d'enregistrement vérifie l'exactitude des mentions relatives à (l'identité de) la personne morale future titulaire du Certificat. – L'officier d'enregistrement fera procéder à l'archivage d'une copie des informations fournies lors de la procédure d'enregistrement par le Demandeur 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 au Demandeur et au 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 Demandeur du Certificat, incluant l'accord de celui-ci sur l'ensemble de ses obligations. Ces informations seront conservées pour une période de 30 ans. – Si la Paire de Clés n'est pas générée par le Prestataire de Services de Certification ou l'Autorité d'Enregistrement Locale, la procédure de validation de la requête électronique de Certificat utilisée par l'officier d'enregistrement garantit que le Demandeur du Certificat est en possession de la Clé Privée associée à la Clé Publique devant être certifiée. – 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 l'Entreprise du Demandeur du Certificat***	
	L'Entreprise, représentée par son représentant légal, approuve l'enregistrement du Demandeur du Certificat dans le cadre de l'obtention du Certificat devant certifier une qualité professionnelle impliquant l'Entreprise. L'Entreprise 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 ou Normalisé E-Trust.	

Section		Réf. RFC 2527
	En particulier, l'Entreprise accepte ce qui suit: • La Convention entre l'Entreprise, le Demandeur du Certificat et le Prestataire de Services de Certification est régie par le droit belge • L'Entreprise adhère à toutes les responsabilités du Demandeur du Certificat (décrites dans le contrat du Demandeur du Certificat). • L'Entreprise est responsable de l'exactitude des données transmises par celle-ci au Prestataire de Services de Certification dans le cadre de l'enregistrement du Certificat. En cas de modification de ces informations, l'Entreprise 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 Demandeur (moyennant le fait que le Prestataire de Services de Certification avertisse et informe le Demandeur du Certificat et l'Entreprise par des voies appropriées). • L'Entreprise demandera au Prestataire de Services de Certification de suspendre ou 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). • L'Entreprise 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.6	***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 ou Normalisé E-Trust dans l'ordre suivant : A ces informations certifiées, est accolée la signature de l'autorité de Certification portant sur l'ensemble des informations certifiées.	

Attribut	**Obligatoire / Optionnel/Fixé**	**Valeur**
	Distinguished Name	
Country (C)	Obligatoire	Pays du siège social de l'Entreprise (tel que publié dans les statuts de l'Entreprise)
Locality (L)	Obligatoire	Localité du siège social de l'Entreprise (tel que publié dans les statuts de la Société)
Organisation (O)	Obligatoire/optionnel	Nom officiel de l'Entreprise, qui correspond à la

		personne morale, titulaire (sujet) de ce certificat (tel que publié dans les statuts de l'Entreprise)
OrganisationalUnit (OU)	Optionnel	Unité, Service ou Département de l'Entreprise
OrganisationalUnit (OU)	Obligatoire	« Limitation on transaction value : <transactionValue>» où transactionValue = Valeur, insérée par le Demandeur du Certificat pour indiquer une restriction sur la valeur d'une transaction. Dans le cas où cette valeur n'est pas spécifiée, la valeur par défaut « Not applicable » est insérée.
OrganisationalUnit (OU)	Obligatoire	« Limitation on certificate usage : <certUseValue » où certUseValue = Valeur, insérée par le client pour mettre une restriction sur l'usage de ce Certificat. La liste ci-dessous n'est pas limitative : - si, et seulement si le Certificat utilisé dans le cadre de la fourniture d'un service OCSP, comme défini dans le rfc 2560, la valeur « OCSP » est insérée. - si, et seulement si le Certificat est utilisé dans le cadre de la fourniture d'un service de chrono-estampillage (timestamping), comme défini dans le rfc 3161, la valeur « Timestamping » est inserée. - si aucune valeur n'est spécifiée par le Demandeur du Certificat, la valeur « Not applicable » est insérée.
CommonName (CN)	Obligatoire	« Company Name : <companyName> - VAT Number : <vatNumber> - RC-HR Number : <rchrNumber>» où companyName = Nom officiel de l'Entreprise (personne morale titulaire (sujet) de ce Certificat) ; tel que publié dans les statuts de l'Entreprise ; vatNumber = Numéro TVA de l'Entreprise ; rchrNumber = Numéro de registre de commerce de l'Entreprise.
Extensions :		
DNSName (SubjectAltName)	Optionnel	URL exacte et complète du serveur
KeyUsage (critical)	Obligatoire	<u>Certificats qualifiés :</u> DigitalSignature NonRepudation <u>Certificats Normalisés :</u> Comme indiqué sur le bon de commande rempli par le Demandeur du Certificat
subjectPublicKey	Fixé	Clé publique: longueur de clé: minimum 1024 bit; Exposant public : Fermat-4 (=010001)
CertificatePolicies-policyIdentifier	Fixé	Voir Tableau 1.
CertificatePolicies-policyQualifier-userNotice	Fixé	«{Qualified,Normalised} E-Trust certificate for digital signature for legal persons; {Qualified, Normalised} certificate {with,without} SSCD; Key generation by {the owner,the CSP}. General conditions O.I.D.: 0.3.2062.9.6.2.25.4.1»

CertificatePolicies-policyQualifier-CPS	Fixé	«www.e-trust.be/CPS/QNcerts»
ExtendedKeyUsage	Obligatoire (uniquement dans le cadre de service OCSP ou Timestamping)	OCSP Service : «OCSPSigning », comme défini dans RFC 2560. Ou Timestamping Service : « timeStamping », comme défini dans RFC 3161.
Autre information :		
Issuer	Fixé	«CN = Belgacom E-Trust Primary CA for qualified certificates OU = E-Trust O = Belgacom C = BE» Ou «CN = Belgacom E-Trust Primary CA for Normalised certificates OU = E-Trust O = Belgacom C = BE»
Validity	Fixé	1 an
serialNumber	Fixé	Numéro de série du certificat
Algorithm	Fixé	«Sha1withRSAEncryption»
Version	Fixé	«2» (en conformité avec v3)

F	***Procédure de génération des clés***	

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

Génération des clés par le Demandeur du Certificat

Le Demandeur du Certificat peut procéder lui-même à la génération de sa Paire de Clés, au quel cas :

- Soit, le cas échéant et en accord avec le Bon de Commande, il fournira une disquette contenant la requête PKCS#10 du Certificat lors de son enregistrement auprès de l'officier de l'Autorité d'Enregistrement Locale,
- Soit, et ce 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 Demandeur du Certificat procédera à la génération de la paire de clés et la demande électronique sécurisée au sein de son environnement et compte sécurisé certipost.

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

Si le Demandeur 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 Demandeur du Certificat, deux 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 Demandeur 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 Demandeur du Certificat.
   - L'Officier LRAO procède à la génération de la requête PKCS#10

	• L'Officier LRAO efface toute trace des clés du Demandeur du Certificat sur son environnement logiciel et matériel. Les clés ne sont présentes que sur le support remis au Demandeur 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 • L'Officier CRAO efface toute trace des clés du Demandeur du Certificat sur son environnement logiciel et matériel. Les clés ne sont présentes que sur le support remis au Demandeur du Certificat.	
G	***Procédure de demande du Certificat***	
	1. Le Demandeur du Certificat se procure le Bon de Commande et les Conditions Générales relatifs aux Certificats Qualifiés ou Normalisés E-Trust pour personnes morales (dénommés ci-après « le Bon de Commande » et « les Conditions Générales ») auprès du Prestataire de Services de Certification (voir section D.1 §5). Ensemble avec le CP et le CPS, ceux-ci forment la Convention. Le Demandeur du Certificat peut également demander au Prestataire de Services de Certification de recevoir une copie de ces documents par la poste ou d'obtenir ces documents d'une Autorité d'Enregistrement Locale (Local Registration Authority -- LRA) agréée par le Prestataire de Services de Certification. Ces Bons de Commandes peuvent être obtenus sous une version dite « complète » où le Demandeur du Certificat choisit lui-même les options possibles, ou encore sous une forme intégrée au contrat relatif au service Certipost dans le cadre d'un enregistrement effectué lors de la procédure d'inscription au service Certipost. 2. Le Demandeur du Certificat doit dûment compléter le Bon de Commande et le signer. En signant le Bon de Commande, le Demandeur du Certificat et l'Entreprise acceptent les Conditions Générales, la CP et le CPS. 3. Le Demandeur du Certificat doit constituer un dossier sur base des pièces suivantes : – Le Bon de Commande dûment complété et signé (celui-ci comporte deux volets, l'un rempli et signé par le Demandeur et l'autre rempli et signé par un représentant légal de l'Entreprise); – Une copie (recto / verso) de la carte d'identité valide et officielle du Demandeur du Certificat, de son passeport ou de tout document officiel équivalent. La copie doit être signée par le Demandeur du Certificat; – Les statuts de l'Entreprise. – La demande électronique de Certificat sur disquette (option dans le cas où les clés ne seraient pas générées par le CSP). – Dans le cas où le Demandeur n'est pas un représentant légal de l'Entreprise, – une copie (recto / verso) de la carte d'identité valide et officielle du représentant légal de l'Entreprise ou de son délégué mandaté, de son passeport ou de tout document officiel équivalent. La copie doit être signée par le représentant légal de l'Entreprise ou de son délégué mandaté; – si un délégué mandaté d'un représentant légal a signé le bon de commande, le Demandeur du Certificat doit fournir la preuve que cette personne est habilitée à signer pour le représentant légal. 4. Le Demandeur du Certificat prend rendez-vous avec un officier LRA (LRAO) chez la LRA de son choix agréée dans le contexte de la présente CP (voir section D.1 §5).	

	5. Enregistrement et Validation auprès de l'Autorité d'Enregistrement Locale (LRA). Le Demandeur se présente en personne auprès de la LRA avec laquelle il a rendez-vous avec l'ensemble des documents constituant son dossier : L'Officier LRA (LRAO) vérifie les documents reçus et procède à la vérification : • de l'identité du Demandeur du Certificat sur la base de l'original de la pièce d'identité valide de celui-ci. • sur la base du dossier et des pièces fournies par le Demandeur du Certificat, des mentions devant être certifiées et relatives à la persone morale dont le Demandeur préalablement identifié est le représentant du Demandeur. Si la demande est validée, le LRAO rassemblera les documents collectés pour former le Dossier d'Enregistrement du Demandeur du Certificat, fera procéder à l'archivage d'une copie de façon sécurisée et en préparera l'original pour transmission sécurisée et archivage chez le Prestataire de Services de Certification. 6. Validation Dans le cas où la génération de la paire de clés est requise en central ou lorsque la LRA ne serait pas directement connectée aux Services de Certification du Prestataire de Services de Certification, lors de la collecte d'une part du Dossier d'Enregistrement du Demandeur du Certificat reçu du LRAO, et le cas échéant, d'autre part de la demande électronique de Certificat envoyée par le Client, l'officier de l'Autorité Centrale d'Enregistrement (Central Registration Authority -- CRA) exécute une vérification finale de validation : exactitude des informations fournies dans le Dossier d'Enregistrement du Demandeur reçu du LRAO, rappel du Demandeur du Certificat par téléphone. Lorsqu'elle est acceptée par l'officier CRA (le CRAO), la demande électronique de Certificat est envoyée à l'Autorité de Certification du Prestataire de Services de Certification pour l'émission du Certificat. Lorsque la demande de Certificat est rejetée par le CRAO, ce dernier informera le Demandeur du Certificat de ce rejet et des raisons motivant ce rejet. Dans le cas où la LRA serait directement connectée au service de Certification, 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. 7. Vérification a posteriori Une seconde vérification du dossier est effectuée a posteriori par le Certification Authority Auditor (CAA) du Prestataire de Services de Certification qui vérifie la cohérence entre les Certificats émis et les dossiers reçus des LRAs.	
H	***Emission du Certificat et livraison***	**4.2**
	A la réception d'une demande de Certificat validée, l'Autorité de Certification du Prestataire de Services de Certification fournira le Certificat digital au Demandeur du Certificat. Le certificat est publié conformément à la section I du présent document. Le Demandeur du Certificat recevra son Certificat ou les informations nécessaires pour récupérer son Certificat. Lorsque les clés ont été générées chez le LRAO, le Certificat est copié sur le support contenant les clés, selon le choix du Demandeur du Certificat. Lorsque les clés ont été générées de façon centralisée par le CRAO, le certificat est immédiatement suspendu jusqu'à ce que la procédure de délivrance en mains propres des clés et du certificat y relatif ait été achevée et confirmée au CRA par le LRA, via un formulaire d'accusé de réception dûment signé par le Demandeur du Certificat. A ce moment, le certificat est réhabilité.	
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 Demandeur du Certificat, et l'Entreprise, 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 Demandeur du Certificat, et l'Entreprise, 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 Demandeur du Certificat, et l'Entreprise titulaire de celui-ci, est responsable de la vérification de l'exactitude du contenu de son Certificat publié. Si le Demandeur du Certificat, ou l'Entreprise titulaire de celui-ci, 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 Demandeur d'un Certificat, le représentant légal (ou son délégué mandaté) de l'Entreprise, la LRA ou le Prestataire de Services de Certification peuvent demander la suspension, la réhabilitation après suspension ou la révocation du Certificat. Le Demandeur 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 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 Demandeur 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 Demandeur 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 Demandeur du Certificat et à l'Entreprise 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 le Prestataire de Services de Certification ou l'autorité d'enregistrement (document papier et informations électroniques) et fournies par le Demandeur et 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 Demandeur du Certificat et l'Entreprise peuvent prendre contact avec le helpdesk du Prestataire de Services de Certification: - Certipost E-Trust: - Numéro de téléphone : 0800 33 150 (FR), 0800 22 150 (NL) - Numéro de fax : 0800 933 16 - E-mail : info@e-trust.be . • Le Prestataire de Services de Certification, le Demandeur du Certificat et l'Entreprise 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. Centre Monnaie 1, 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.