Politique de Certificat relative au Certificat Qualifié ou Normalisé de Notaire / Collaborateur du Notariat

Version 1.04 Final

–

Certificate Policy – CP for Qualified or Normalized Certificate for Notary / Collaborator's of Notaries Organisations

Politique de Certificat relative au Certificat Qualifié ou Normalisé de Notaire / Collaborateur du Notariat

Ce document décrit l'applicabilité du certificat de type « Certificat Qualifié ou Normalisé (ci-après dénommé le « Certificat ») de Notaire / Collaborateur du Notariat » (ci-après dénommé le « Titulaire ») émis par le Prestataire de Services de Certification (Certification Service Provider – CSP) selon cette CP, les procédures à suivre et les responsabilités des parties impliquées, conformément aux Déclarations de Pratique de Certification en vigueur (Certification Practice Statements – CPS) du Prestataire de Services de Certification. Il s'agit d'une Politique de Certificat relative à des Certificats Qualifiés ou Normalisés et qui satisfait aux conditions suivantes :

Section		Réf. RFC 2527
A	***Aperçu de la Politique de Certificat Qualifié ou Normalisé de Notaire / Collaborateur du Notariat***	**1.1**
	Très haut niveau d'assurance quant à l'identité électronique personnelle et professionnelle du titulaire du certificat dans le cadre ou à l'occasion de l'exercice de la profession de Notaire, de Candidat Notaire ou de Collaborateur du Notariat. Il s'agit d'un certificat pour lequel la délivrance est conditionnée par la présentation personnelle du titulaire durant le processus d'enregistrement. Ce certificat fournit un niveau très élevé de garantie pour assurer le lien entre l'identité personnelle, la clé publique, son usage autorisé et les informations relatives à la qualification professionnelle du titulaire du certificat. Ce certificat fournit le degré le plus élevé de garantie d'authentification correcte puisque le titulaire du certificat doit : • soit se rendre en personne auprès d'une Autorité d'Enregistrement Locale (Local Registration Authority - 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 et la vérification des données fournissant la preuve de son rôle du Notaire / Collaborateur du Notariat et des informations correspondantes devant 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 qualifiée auquel cas le certificat répond 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) • un contexte de chiffrement et/ou d'authentification auquel cas le certificat répond 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) se déclare(nt) conforme(s) à celle-ci et aux	

Section		Réf. RFC 2527
	règlements et standards techniques ous'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 et le chiffrement (et/ou authentification) sont toujours distincts.	
B	***Identification de la Politique de Certificat Qualifié ou Normalisé de Notaire / Collaborateur du Notariat***	
	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'applications 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 de Notaire / Collaborateur du Notariat** » plusieurs Politiques de Certificats suivant l'usage qui peut être fait du certificat (signature digitale ou chiffrement/authentification), suivant que la clé privée a été générée sur la carte ou non et ne peut être utilisée que dans un Dispositif Sécurisé de Création de Signature (Secure Signature Creation Device – SSCD). Il en découle deux grands types de certificats. D'un côté les **Certificats Qualifiés** dont l'usage est strictement réservé à la signature digitale, 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 strictement réservé soit au chiffrement, soit à l'authentification, soit à la signature digitale normalisée (à l'exclusion donc des signatures qualifiées), soit une combinaison des usages précédents. Ces certificats sont compatibles avec et satisfont les exigences spécifiées 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 de Notaire / Collaborateur du Notariat » 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 Qualifiés ou Normalisés de Notaire / Collaborateur du Notariat spécifiés dans le présent document sont repris dans le Tableau 1 ci-dessous.	

Certificat Qualifié de Notaire / Collaborateur du Notariat pour la Signature uniquement	Certificat Normalisé de Notaire / Collaborateur du Notariat pour le Chiffrement et l'Authentification
Certificat Qualifié avec SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** Génération des clés par le CSP: **0.3.2062.9.6.1.26.3.1**	Certificat Normalisé avec SSCD (OID ETSI 102042) : 0.4.0.2042.1.2 Génération des clés par le CSP: **0.3.2062.9.6.1.26.7.1**

Tableau 1. Identification de la Politique de Certificat Qualifié ou Normalisé de Notaire / Collaborateur du Notariat

Section		Réf. RFC 2527
C	***Applicabilité***	**1.3.4**
	• Ce type de certificat constitue une très haute garantie d'identité électronique professionnelle pouvant être utilisée pour sécuriser des applications de niveau de sécurité élevé telles que les opérations, soit de signature digitale, soit de chiffrement/authentification, effectuées dans le cadre de l'exercice de la profession du titulaire du certificat. • Il incombe toutefois aux parties de choisir les applications pour lesquelles elles ont confiance dans le certificat, en fonction de la nature et du niveau de sécurité des procédures suivies pour l'émission du certificat (décrits respectivement 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 exclusivement utilisée que dans un contexte de signature digitale, ou de chiffrement et authentification. Les certificats (et les paires de clés) utilisés pour la signature digitale et le chiffrement (et authentification) sont toujours distincts. • 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 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 décrites dans le standard technique ETSI 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 sont 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. Les Certificats Qualifiés émis dans le cadre de cette CP ne sont toutefois pas des Certificats Qualifiés dit « publics » étant donnés que leur utilisation est limitée au cadre de l'exercice de la profession du titulaire du certificat. La présente CP se voit donc adjoindre des contraintes supplémentaires par rapport aux CP de Certificat Qualifiés Public : • Obligation pour le titulaire de s'adresser à une Autorité Locale d'Enregistrement (Local Registration Authorities – LRA) agréée et formée par la FRNB et le Prestataire de Services de Certification, • Obligation pour le titulaire de fournir au Prestataire de Services de Certification, via	

Section		Réf. RFC 2527
	la LRA agréée, les preuves d'identification supplémentaires décrites dans la procédure de demande de certificat de la présente CP (section E) • Si le titulaire est un Notaire, la Chambre Nationale des Notaires (CNN) validera le «rôle» du titulaire («Role of Holder») . • Intervention permise de la FRNB ou la CNN, via les LRA agréées, dans le cadre des procédures de révocation/suspension (voir section J de la présente CP).	
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 délivre des certificats conformes 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 TS 101 456 (excepté les clauses 7.2.9 et 7.5.2, en conformité avec son chapitre 8). 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 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. • Prestataire(s) de Services de Certification autorisé(s) à émettre des certificats sous la présente CP : - **Belgacom E-Trust** via le **Belgacom E-Trust Primary CA for Qualified Certificates** pour l'émission des Certificats Qualifiés et via le **Belgacom E-Trust Primary CA for Normalised Certificates** pour l'émission des Certificats Normalisés **(www.e-trust.be/CPS/)** : - *Déclarations de Pratiques de Certification (CPS) :* www.e-trust.be/CPS/ - *Répertoire Publique de Certificats et CRL :* www.e-trust.be/en/x500 - *Déclaration de conformité :* www.e-trust.be/CPS/ • Pour procéder à l'enregistrement du titulaire, le Prestataire de Services de Certification utilise l' Autorité Locale d'Enregistrement (Local Registration Autority - LRA) agréée : le département au sein de la FRNB représentées par les personnes figurant dans la liste authentifiée disponible sur www.e-notariat.be • 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, à sa CPS et aux procédures internes de contrôle 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 par des voies appropriées).	

Section		Réf. RFC 2527
	• 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 clés 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 titulaire du certificat a le droit de consulter et de modifier les données personnelles le concernant[1]. Le Prestataire de Services de Certification s'engage à faire clairement mention des droits du titulaire du certificat 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 Déclaration de Pratiques de Certification (Certification Practice Statement - CPS) en vigueur du Prestataire de Services de Certification décrivant les pratiques utilisées pour fournir les certificats digitaux et éditée par le Prestataire de Services de Certification. Le titulaire du certificat accepte la présente Politique de Certificat (Certificate Policy - 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. • 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 propriétaire et 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 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 code PIN ou 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	

[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, ainsi que de s'opposer, sur demande et sans frais, à tout usage desdites données à des fins de marketing direct.

Section		Réf. RFC 2527
	n'est pas responsable de l'utilisation de la paire de clés du titulaire du certificat. • La paire de clés sera générée via le dispositif SSCD et le certificat ne sera utilisé avec la clé privée qu'uniquement via ce dispositif. • 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, code PIN) ou pour une autre raison ; et/ou – Les données certifiées sont devenues inexactes ou ont changé. Son xertificat 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 immédiatement informer le Prestataire de Services de Certification de toute modification dans les informations contenues dans son certificat. Son certificat sera alors révoqué immédiatement. • Le 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 qualification professionnelle devenaient en tout ou en partie obsolètes. • Le titulaire du certificat accepte que son certificat soit publié immédiatement après sa création dans le Certificate Public Registry (Registre public de Certificat) du Prestataire de Services de Certification, auprès duquel tout tiers peut librement consulter et obtenir copie du certificat, ce que le titulaire du certificat accepte. • Le certificat est réputé accepté par le titulaire du certificat dès la survenance du premier des événements suivants, soit le 7ième jour après sa publication sur le Registre Public de Certificat (Certificate Public Registry) de Belgacom E-Trust, 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 Belgacom E-Trust sans délai. Belgacom E-Trust révoquera alors le certificat et prendra les mesures appropriées pour ré-émettre un certificat. Ceci constitue le seul recours du titulaire du certificat 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 la FRNB, en sa qualité d'Autorité Locale d'Enregistrement, de toute information utilisée pour l'enregistrement, pour la fourniture 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 contrat afférent constitué du bon de commande et des conditions générales et la présente CP (section D1).	
D.3	***Droits, responsabilités et obligations de l'Autorité d'Enregistrement Locale (LRA)***	
	La FRNB, en tant qu'Autorité Locale d'Enregistrement (LRA) est tenue contractuellement de respecter scrupuleusement les procédures d'enregistrement décrites dans les Déclarations	

Section		Réf. RFC 2527
	de Pratiques de Certification (CPS) du Prestataire de Services de Certification. La FRNB, en qualité de 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 mentions relatives à la qualité professionnelle. La FRNB obtient une validation de la part de la Chambre nationale des Notaires (CNN = CLRAO ou « Chief Local Registration Authority Officer »), par exemple dans le cas d'un Notaire – Que les requêtes de certificats transmises au Prestataire de Services de Certification sont complètes, correctes, valides et dûment autorisées. En particulier : – La FRNB est responsable de la génération et du stockage de la paire de clés sur le support SSCD 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 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. – 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), dates 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 E du présent document, les mentions relatives à la qualité professionnelle du titulaire du certificat (qu'elles soient obligatoires ou optionnelles). – L'officier d'enregistrement archivera 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 : – L'information utilisée pour vérifier l'identité et les mentions relatives à la qualité professionnelle du 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 par le CSP 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 FRNB, en tant que 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.	

Section		Réf. RFC 2527
	La classification des données et la responsabilités 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 FRNB 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 Chambre Nationale des Notaires (CNN)***	
	La Chambre Nationale des Notaires, via son représentant légal, donnera son accord pour l'enregistrement des Notaires pour l'obtention d'un certificat en vérifiant la qualité du demandeur dans les bases de données a sa disposition. La CNN accepte : • La Certification Practice Statement (CPS) en vigueur éditée par le Prestataire de Services de Certification et décrivant les pratiques utilisées pour fournir les certificats digitaux du Prestataire de Services de Certification. • La présente Certificate Policy (CP). En particulier, ce qui suit: • L'accord contractuel entre la CNN, le titulaire du certificat et le Prestataire de Services de Certification est régi par le droit belge. • La CNN reconnait être informé de toutes les responsabilités incombant au Notaire / candidat Notaire, titulaire du Certificat décrites dans le Bon de Commande et les Conditions Générales relatifs à l'obtention du Certificat, et marque son accord sur celles-ci. • La CNN est responsable de l'exactitude des données transmises au Prestataire de Services de Certification dans le cadre de l'enregistrement du Notaire. En cas de modification de ces informations, la CNN en informera immédiatement le Prestataire de Services de Certification, qui réagira 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 (moyennant le fait que le Prestataire de Services de Certification avertisse et informe le Notaire et la CNN par des voies appropriées). • La CNN demandera au Prestataire de Services de Certification de suspendre ou révoquer le certificat d'un titulaire à chaque fois que cela est requis dans la présente CP et le CPS en vigueur (section 4.4). Les procédures de suspension et de révocation sont décrites dans la section I du présent document. • La CNN 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 relatifs à l'obtention du certificat, et la présente CP (section D1).	
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	

Section		Réf. RFC 2527
	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 D1 §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 du titulaire émis.	

Attribut (X.500)	**Obligatoire / Option**	**Valeur**
Informations relatives au titulaire du certificat		
Common Name (CN)	Obligatoire	**<nom et prénom du titulaire du certificat>**
NotaryEntity Number (OU NN)	Obligatoire pour les Notaires Optionnel pour les Collaborateurs du notariat	**<Numéro identifiant le titulaire>**
Country (C)	Obligatoire	**<Nationalité du titulaire du certificat (Pays)>**
Date of Birth	Obligatoire	**<Date de naissance>**
Organization (O)	Obligatoire pour les Notaires Optionnel pour les Collaborateurs du notariat	**<Nom de la compagnie provinciale du titulaire du certificat> si applicable ou nom officiel de l'organisation**
Organization Unit	Obligatoire	**<Numéro de L'étude Notariale> si disponible, ou description du département**
Professional Address	Optionnel	**<Adresse professionnelle>**
E-mail address	Obligatoire	**<Adresse E-mail du titulaire>**
Internet Site	Optionnel	**<URL du site Web du titulaire>**
Telephone	Optionnel	**<Numéro de téléphone du titulaire>**
Fax	Optionnel	**<Numéro de fax du titulaire>**
Quality (OU Title)	Obligatoire	**<Titre du titulaire >**
Role of Holder (OU Role)	Obligatoire pour les Notaires Optionnel pour les Collaborateurs du Notariat	**< « Notaire/Notaris », seulement pour des Notaires en fonction, ou la fonction du titulaire>**
Extensions		

Section				Réf. RFC 2527
	KeyUsage	Obligatoire	• Certificat Qualifié: “DigitalSignature & Non-Repudation ” • Certificat Normalisé: “DigitalSignature, Authentication, Encryption”	
	Extended Key Usage	Fixe	• Certificat Qualifié: “s/MIME” • Certificat Normalisé: “s/MIME & ssl-Client”	
	Informations sur la Politique de Certificat			
	CP OID	Fixe	• Certificat Qualifié : *“0.4.0.1456.1.1”* (ETSI 101456) : & *“0.3.2062.9.6.1.26.3.1”* • Certificat Normalisé: *“0.4.0.2042.1.1”* (ETSI 102042) & *“0.3.2062.9.6.1.26.7.1”*	
	CP Summary	Fixe	“Belgacom E-Trust Certificate Policy for Qualified or Normalized Certificates for Notary’s or collaborators of notaries organizations”	
	CPS/CP Location	Fixe	www.e-trust.be/CPS/	
	Transaction limit	Fixe	N/A (pas de limitation)	
	Usage limitation	Fixe	N/A (pas de limitation)	
	Informations Générales			
	Version	Fixe	2 (Pour X.509 version 3)	
	SerialNumber		Numéro de série du Certificat	
	Algorithm	Fixe	Sha1RSA	
	SubjectPublicKey	Obligatoire	<Certificate Holder’s public key (1024 bit)> Public Key: Key Length 1024 bit Public Exponent: Fermat-4 (=010001)	
	Validity	Fixe	2 years	
	Issuer	Fixe	CN = Belgacom E-Trust Primary CA for <Qualified>/<Normalised> Certificates OU = E-Trust O = Belgacom C = BE	
F	***Procédure de génération des clés***			
	La taille des clés doit être au minimum de 1024 bits. • Le LRAO introduit le mot de passe (ou code PIN) qui protége ses propres clés, pour démarrer le logiciel pour communiquer avec le Certification Authority« WebRAO » • L’Officier LRA (LRAO) procède à la génération des clés sur le SSCD du titulaire • Le LRAO procède à la génération de la requête PKCS#10 • certificatcertificat			
G	***Procédure de demande du certificat***			

Section		Réf. RFC 2527
	1. Le titulaire remplit le bon de commande via le site ''E-notariat'' de la FRNB Le Titulaire télécharge le bon de commande du site, l'imprime, et le signe. Le titulaire en garde un copie a domicile 2. Le titulaire constitue le dossier avec : 2.1. Le bon de commande complété et signé (avec les conditions générales) 2.2. Une copie recto/verso signée de sa carte d'identité Et, dans le cas des collaborateurs du Notariat 2.3. Une copie recto/verso signée de la carte d'identité de la responsable de l'organisation du titulaire 2.4. La signature et l'autorisation de la responsable sur le bon de commande 3. Le titulaire envoie le bon de commande complété à la FRNB via fax (de préférence) ou E-mail (dans ce cas, sans les copies des cartes d'identités) 4.Le LRAO contrôle le dossier et vérifie si le demandeur mentionné dans le bon de commande se trouve dans ses bases de données. Le LRAO demande une autorisation formelle au CLRAO (=CNN) pour délivrer le certificat demandé avec le rôle de « Notaire ». Une fois cette autorisation reçue, le LRAO poursuit la procédure prévue. 7. Le LRAO personnalise une carte à puce pour le futur titulaire. Avec son logiciel de LRA(O), il génère la paire de clés, introduit les données à certifier et envoie la requête. Lorsqu'il reçoit en retour le certificat, il le stocke sur la carte à puce. 8.. Dans cette procédure, il est attendu que chaque certificat créé est immédiatement suspendu pour des raisons de sécurité. 9. Le LRAO adapte les codes PIN et PUK de la carte à puce. 10. Le LRAO fixe un rendez-vous avec le titulaire pour un ''face-to-face'' par exemple dans une compagnie provinciale. A ce moment là, le LRAO mentionne au titulaire les éventuelles pièces manquantes (ou autres remarques) afin que celui-ci puisse compléter le dossier avant le rendez-vous. Il insistera éventuellement afin que la copie de la carte d'identité, et les autorisations ad hoc si nécessaire, ne soi(en)t pas oubliée(s). 11. Le titulaire se rend au rendez-vous avec le dossier complet. 12. Le LRAO contrôle l'identité du titulaire ainsi que le dossier original. 13. Le LRAO remet le lecteur de carte à puce et la carte à puce au titulaire. 14. Le titulaire remplit l'accusé de réception et le titulaire et le LRAO le signent. Le LRAO faxe ensuite l'accusé de réception à l'Autorité de Suspension & Révocation (Suspension Revocation Authority – SRA). Le SRA lèvera alors la suspension afin que le titulaire puisse utiliser immédiatement les certificats. 15. Le LRAO donne également un formulaire au titulaire qui servira de demande de suspension, de révocation ou d'annulation de la suspension des certificats. 16. Le LRAO archive une copie du dossier et envoie l'original à Belgacom E-Trust. 17. Le titulaire change les codes PIN et PUK avec le software délivré avec le lecteur de carte à puce. La Chambre Nationale des Notaires (CNN) aura la responsabilité d'autorité d'enregistrement	

Section		Réf. RFC 2527
	« CLRAO » ou « Chief Local Registration Authority Officer ». La CNN doit valider la qualité, ou rôle, de Notaire. La validation des requêtes de certification sera effectuée par le Président ou un membre du comité qu'il aura délégué.	
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 LRAO et le publiera conformément à la section I du présent document. Lorsque les clés ont été générées chez le LRAO, le certificat est copié sur le support contenant les clés (SSCD). Le titulaire recevra son certificat digital, stocké sur le support SSCD.	
I	***Acceptation du certificat et publication de 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 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 dès la survenance du premier des événements suivants, soit le 7ième 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	
J	***Procédure de Suspension/ Réhabilitation après Suspension / Révocation***	**4.4**
	Le titulaire d'un certificat, la responsable de l'organisation du titulaire, la FRNB (LRA), la CNN (CLRA) ou le Prestataire de Services de Certification peuvent demander la suspension, la réhabilitation après suspension ou la révocation du certificat. Le titulaire d'un certificat, sera averti 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	

Section		Réf. RFC 2527

disposition des parties par le Prestataire de Services de Certification (annexé aux Conditions Générales).

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 demande de **suspension**:

- Le demandeur doit avertir l'Autorité de Suspension & Révocation (Suspension & Revocation Authority – SRA) du Prestataire de Services de Certification ayant émis le certificat concerné par la demande.
- La SRA procédera à un rappel du demandeur (« call-back ») pour obtenir la confirmation de la demande de suspension.
- La SRA procède à la suspension du certificat à dater de la confirmation.
- Dans les 14 jours ouvrables, le demandeur envoie par fax ou par courrier postal au Prestataire de Services de Certification le formulaire de revocation/suspension rempli, faute de quoi le certificat sera réhabilité.
- La suspension d'un certificat, confirmée par formulaire 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 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 par la demande pour demander à recevoir un formulaire de demande de réhabilitation après suspension d'un certificat ou utiliser celui disponible en annexe des Conditions Générales.
- Le demandeur doit se rendre auprès d'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)
- Contacter la SRA pour demander à recevoir un formulaire de demande de révocation de certificat ou utiliser celui disponible en annexe des Conditions Générales.
- Se rendre auprès d'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 procèdera 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 suspension 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.
- Quand le LRA peut établir que les données certifiées ne sont plus valides, le LRA peut procéder directement à la révocation. Le LRA doit motiver cette action.
- **La révocation d'un certificat est définitive.**

Section		Réf. RFC 2527
K	***Procédure de renouvellement des clés, du certificat***	
	Le Prestataire de Services de Certification s'assure que les requêtes émises par un titulaire d'un certificat qui a déjà préalablement été 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 ou encore suite à un changement dans les données certifiées. Le Prestataire de Services de Certification s'assure : • Que l'information utilisée pour vérifier l'identité du titulaire est toujours valide, et pour ce faire : – la même procédure que lors de l'enregistrement initial est prévue (cfr. Section G du présent document) OU, – dans le cas d'un renouvellement et pour autant que les clés et le certificat du titulaire 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. • Si les termes et conditions générales du Prestataire de Services de Certification ont changé, le Prestataire de Services de Certification les communiquera au 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 Certipost (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). Le titulaire du certificat a le droit de consulter et de rectifier ces données ainsi que de s'opposer, sur demande et sans frais, à tout usage desdites données à des fins de marketing direct.	
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 Service Center (Qualified et Normalised Cas)** - Tel. : +32 70 22 55 44 - Fax : +32 70 22 55 01 - E-mail : Support.fr@contact.certipost.be • Le Prestataire de Services de Certification et le titulaire du Certificat s'engagent à tout	

[2] Afin d'exécuter ces tâches efficacement, Certipost (E-Trust) 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, 1000 Bruxelles. Les données seront uniquement utilisées pour la fourniture des services Certipost (E-Trust). Le titulaire du Certificat a le droit de consulter et de rectifier ces données ainsi que de s'opposer, sur demande et sans frais, à tout usage desdites données à des fins de marketing direct.

Section		Réf. RFC 2527
	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.	