tbs internet
Accélérateur de confiance !

Déclaration des Pratiques de Certification de TBS INTERNET

Version 1.13

14 septembre 2021

www.tbs-internet.com

Historique des révisions

Version	*Date*	*Action*	*Commentaire*
V1.13	14/09/2021	MAJ	Précision sur les champs L et ST utilisés dans les certificats serveur
V1.12	24/08/2021	MAJ	Renvoi sur documentation Sectigo pour les certificats serveur Description de la méthode par courrier postal dans 4.2.1 Retrait champs Street et PostalCode des certificats serveur
V1.11	11/02/2020	MAJ	Ajout des intermédiaires Persona 3 Retrait des intermédiaires expirés
V1.10	22/04/2018	MAJ	Update regarding ballot 218
V1.09	29/12/2017	MAJ	Suppression des produits SGC et Intranet Retrait des produits SHA1 plus en vente Actualisation des intermédiaires pour les produits client Retrait des champs OU des certificats emails Transfert de responsabilité
V1.08	08/11/2014	MAJ	Ajout nouveaux intermédiaires SHA2 et modification sections 2.13 & 2.14
V1.07	11/08/2014	MAJ	Actualisation des produits Multiples Sites
V1.06	22/12/2013	MAJ	Création de produits SHA256 Modification des intermédiaires MAJ Processus de validation Ajout OID
V1.05	30/03/2009	Ajouts	Création des produits Email Institua Création des produits SHA256 SGC et Test SHA256 Ajout du support OCSP pour tous les produits sauf le TBS X509 Novice Ajout des ICD SIRENE
V1.04	12/08/2008	Ajouts	1.8.1 à 1.8.4, 4.8 et 6.1 : Extension de la durée de validité de 3 ans à 5 ans
V1.03	03/12/2007	Ajouts	1.8.1 et 1.8.6 : Extension durée de validité de 30 jours à 10 ans 2.1.5 : Fixe écriture des numéros de version 4.1.3 : Introduit l'API pour les partenaires 4.2.1 : Précisions sur la lettre de pouvoir de domaine 4.2.3 à 12 : Précision des champs validés 4.2.8 : La vérification des domaines pour les Multi-Sites des hébergeurs peut être réalisée en comparant les adresses IP correspondants au CN Correction fautes de frappe, grammaire, orthographe : 1.1, 3.5.1, 5.19, 5.41, 5.46, 5.47
V1.02	05/02/2007	Ajouts	Produits Sign&Login

Notes
Document réalisé sous LibreOffice sous Linux

Table des matières

1 Généralités....10
1.1 TBS INTERNET....10
1.2 La DPC de TBS INTERNET....11
1.3 Applicabilité, avenants à/et publication de la DPC....11
1.4 Autres Contrats & Déclarations de pratiques....12
1.5 Responsabilité de TBS INTERNET....12
1.6 Conformité aux normes applicables....12
1.7 Présentation de la politique de certification numérique....12
1.8 Hiérarchie de la PKI TBS INTERNET....16
1.8.1 Certificats mél....16
1.8.2 Certificats serveur standard....16
1.8.3 Certificats serveur Pro Hosting....17
1.8.4 Certificats client généraux....17
1.9 L'Autorité de Certification TBS INTERNET....17
1.10 Les Autorités d'Enregistrement de TBS INTERNET....18
1.10.1 Programme de partenariat Distributeur....19
1.10.2 Programme de partenariat Hébergeur....19
1.10.3 Programme PKI PME....19
1.11 Les abonnés....19
1.12 Les parties utilisatrices....20
2 Technologie....21
2.1 L'infrastructure de l'AC TBS INTERNET....21
2.1.1 Récupération & protection des clés de signature d'une AC racine....21
2.1.2 Processus de génération des clés de signature d'une AC racine....21
2.1.3 Archivage des clés de signature d'une AC racine....21
2.1.4 Procédures employées lors du changement d'une clé de signature d'une AC racine....22
2.1.5 Envoi des clés publiques d'une AC racine aux abonnés....22
2.1.6 Pilotage de l'AC sur le plan physique....22
2.2 Administration des certificats numériques....23
2.3 Répertoires, archives et listes des certificats révoqués....23
2.4 Types de certificats TBS INTERNET....24
2.4.1 Les certificats Serveur TBS INTERNET....24
2.4.2 Les certificats Clients Email de TBS INTERNET....26
2.4.3 Les certificats Client d'authentification de TBS INTERNET....28
2.5 Extensions et dénomination....28
2.5.1 Les extensions d'un certificat numérique....28
2.5.2 Incorporation par référence des extensions et dénomination améliorée....28
2.6 Processus de génération de la clé privée d'un abonné....29
2.7 Protection et sauvegarde de la clé privée d'un abonné....29
2.8 Envoi de la clé publique de l'abonné à TBS INTERNET....29
2.9 Envoi du certificat émis à l'abonné....29
2.9.1 Certificat Serveur....29
2.9.2 Certificat Client d'authentification....30
2.9.3 Certificat Email (tous types)....30
2.10 Envoi du certificat émis à l'intention de l'abonné vers les partenaires....30
2.11 Envoi d'un certificat émis à l'intention de l'abonné vers le détenteur d'un compte PKI PME....30
2.12 Profil des certificats TBS INTERNET....30
2.12.1 Le champ d'extension d'utilisation des clés....30

2.12.2 Le champ Caractère critique de l'extension....31
2.12.3 L'extension Contraintes de base....31
2.13 Profil de la Liste des Certificats Révoqués de TBS INTERNET....31
2.14 Politique de Certification (PC)....32
Certificat Serveur TBS INTERNET – SHA256, Omnidomaine SHA256....33
Certificat Serveur TBS INTERNET – Test SHA256 v2....34
Certificat Serveur TBS INTERNET – Multiples-Sites SHA256....35
Certificat client TBS INTERNET – Utilisateur PKI PME (SHA256 v1)....36
Certificat client TBS INTERNET – Email Professionnel SHA256....37
Certificat client TBS INTERNET – Email Professionnel SHA256 v2017....38
Certificat client TBS INTERNET – Email Professionnel SHA256 v2019....39
Certificat client TBS INTERNET – Email Professionnel Test SHA256....40
Certificat client TBS INTERNET – Email Novice (SHA256)....41
Certificat client TBS INTERNET – Sign & Login SHA256....42
Certificat client TBS INTERNET – Sign & Login SHA256 v2017....43
Certificat client TBS INTERNET – Email Professionnel SHA256 v2019....44
Certificat client TBS INTERNET – Sign & Login Test SHA256....45
3 Organisation....47
3.1 Conformité vis-à-vis de la DPC....47
3.2 Cessation des activités de l'AC....47
3.3 Format des archives....48
3.4 Délai de conservation des archives....48
3.5 Journaux des fonctions centrales....48
3.5.1 Administration de l'AC et du cycle de vie des certificats....49
3.5.2 Évènements liés à la sécurité....49
3.5.3 Informations liées à la demande de certificat....49
3.5.4 Délai de conservation des journaux....50
3.6 Plans de continuité des affaires et reprise sur sinistre....50
3.7 Disponibilité des données de révocation....50
3.8 Publication des informations cruciales....51
3.9 Informations confidentielles....51
3.9.1 Types d'informations considérés comme confidentiels....51
3.9.2 Types d'information non considérés comme confidentiels....51
3.9.3 Accès aux informations confidentielles....52
3.9.4 Divulgation des informations confidentielles....52
3.10 Pratiques et gestion du personnel....52
3.10.1 Rôles de confiance....52
3.10.2 Contrôles en matière de personnel....52
3.11 Publication des informations....52
4 Pratiques et procédures....54
4.1 Conditions nécessaires à la demande de certificat....54
4.1.1 Demandes de certificats de la part d'un partenaire hébergeur....55
4.1.2 Demandes de certificat de la part du titulaire d'un compte PKI PME....55
4.1.3 Moyens utilisés pour faire la demande....55
4.2 Validation des demandes....55
4.2.1 Processus de validation en trois étapes....55
4.2.2 Processus de validation en deux étapes....56
4.2.3 Certificats de type Test....57
4.2.4 Certificats Standard, Ecommerce, Premium, Omnidomaine....57
4.2.5 Certificat Email Novice....57
4.2.6 Certificat Utilisateur : version PKI PME....58
4.2.7 Certificats Multi-Sites....58

4.2.8 Certificats Sign & Login....58
4.2.9 Certificats Test Sign & Login....58
4.2.10 Certificats Email Professionnel....59
4.2.11 Certificats Email Particulier....59
4.3 Informations de validation utilisées lors de la demande d'un certificat....59
4.3.1 Informations saisies pour les demandes issues par les organisations....60
4.3.2 Documents étayant les demandes issues par les organisations....60
4.3.3 Informations saisies pour les demandes issues par un individu....61
4.3.4 Documents étayant les demandes issues par les individus....62
4.4 Conditions de validation des demandes de certificat....62
4.4.1 Confirmation via un tiers des informations concernant une entité professionnelle....62
4.4.2 Affectation d'un numéro de série....63
4.5 Délai nécessaire pour confirmer les données soumises....63
4.6 Approbation et rejet des demandes de certificat....63
4.7 Émission d'un certificat et consentement de l'abonné....63
4.8 Validité du certificat....64
4.9 Acceptation d'un certificat par l'abonné....64
4.10 Vérification des signatures numériques....64
4.11 Confiance vis-à-vis d'une signature numérique....64
4.12 Suspension d'un certificat....65
4.13 Révocation d'un certificat....65
4.13.1 Demande de révocation....65
4.13.2 Mise en application de la révocation....66
4.14 Renouvellement....66
4.15 Refabrication....66
4.16 Avis avant l'expiration....66
5 Conditions légales d'émission....68
5.1 Observations formulées par TBS INTERNET....68
5.2 Informations incorporées par référence dans un certificat numérique TBS INTERNET....68
5.3 Affichage des limitations de responsabilité et du déni de garantie....68
5.4 Publication des données des certificats révoqués....68
5.5 Obligation de vérification de l'exactitude des informations soumises....69
5.6 Publication des informations....69
5.7 Ingérences sur l'installation de TBS INTERNET....69
5.8 Normes....69
5.9 Limitations des partenariats avec TBS INTERNET....69
5.10 Limitation des responsabilités de la société TBS INTERNET vis-à-vis de ses partenaires....70
5.11 Choix des méthodes cryptographiques....70
5.12 Confiance vis-à-vis d'une signature numérique non vérifiée....70
5.13 Demandes de certificat rejetées....70
5.14 Refus d'émission d'un certificat....70
5.15 Obligations de l'abonné....71
5.16 Observations de l'abonné après acceptation d'un certificat....71
5.17 Indemnisation par l'abonné....72
5.18 Obligations des Autorités d'Enregistrement de TBS INTERNET....73
5.19 Obligations de la partie utilisatrice....73
5.20 Légalité des informations....74
5.21 Responsabilité de l'abonné vis-à-vis des parties utilisatrices....74
5.22 Obligation vis-à-vis des agents de contrôle....74
5.23 Utilisation d'un agent....74
5.24 Conditions d'utilisation du répertoire et du site Internet de la société TBS INTERNET....74
5.25 Exactitude des informations....75

5.26 Obligations de la société TBS INTERNET....75
5.27 Aptitude à un but particulier....76
5.28 Autres garanties....76
5.29 Informations non vérifiées de l'abonné....77
5.30 Exclusion de certains éléments des pertes et préjudices....77
5.31 Plan de garantie d'un certificat....78
5.31.1 Certificat Standard....78
5.31.2 Certificat Ecommerce....78
5.31.3 Certificat Premium....78
5.31.4 Certificat Omnidomaine....78
5.31.5 Certificat Email Professionnel, Utilisateur PKI PME....78
5.31.6 Certificat Email Particulier....78
5.31.7 Certificat Sign & Login, Multiples-Sites....78
5.31.8 Certificat Test, Test Sign & Login, Email Novice....78
5.32 Limitations financières par rapport à l'utilisation d'un certificat....79
5.33 Limitations en termes de dommages et pertes....79
5.34 Conflit de règlements....79
5.35 Droits de propriété intellectuelle de la société TBS INTERNET....79
5.36 Violation et autres éléments de préjudice....79
5.37 Propriétés....80
5.38 Droit applicable....80
5.39 Compétence juridique....80
5.40 Règlement des litiges....81
5.41 Ayant droits et ayant cause....81
5.42 Dissociabilité....81
5.43 Interprétation....81
5.44 Sans dispense....82
5.45 Avis....82
5.46 Honoraires....82
5.47 Politique de ré-émission de la société TBS INTERNET....83
5.48 Politique de remboursement de la société TBS INTERNET....83
6 Procédure générale d'émission....84
6.1 Généralités - TBS INTERNET....84
6.2 Certificats émis à des individus et des organisations....84
6.3 Contenu....84
6.3.1 Certificats Serveur....84
6.3.2 Certificat Client Email....85
6.4 Délai nécessaire pour confirmer les données soumises....85
6.5 Procédure d'émission....86
Rédaction du présent document....87

Sigles et expressions utilisés dans la présente DPC

Sigles :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
CSR	Certificate Signing Request ou Demande de signature de certificat
DPC	Déclaration des Pratiques de Certification
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure ou Infrastructure à Clé Publique
PKIX	Infrastructure à clé publique (basée sur les certificats numériques X.509)
PKCS	Public Key Cryptography Standard ou Standards de cryptographie à clé publique
X.509	Standard de l'ITU-T assujettissant les certificats et la structure d'authentification
DCV	Domain Control Validation

Expressions :

Demandeur	Désigne l'entité faisant la demande d'un certificat
Abonné	Désigne l'entité à qui a été émis un certificat
Partie utilisatrice	Désigne l'entité invoquant les informations contenues dans le certificat.
Contrat d'abonnement	Désigne l'accord devant être lu et accepté par le demandeur avant de faire la demande de certificat. Le Contrat d'abonnement est fonction du type de certificat numérique demandé. À cet effet, les différents types de certificats numériques sont présentés au cours du processus de commande en ligne et sont disponibles en référence à l'adresse http://www.tbs-internet.com.com/CA/repository
Contrat de la partie utilisatrice	Le Contrat de la partie utilisatrice désigne l'accord devant être lu et accepté par la partie utilisatrice, et ce avant la validation, l'invocation ou l'utilisation d'un certificat. Ce contrat est disponible en référence à l'adresse http://www.tbs-internet.com.com/CA/repository
Politique de certification	Désigne la Déclaration de la politique choisie par l'émetteur et qui correspond à l'usage prescrit d'un certificat numérique dans le contexte de délivrance dudit certificat.

1 Généralités

Ce document constitue la Déclaration des Pratiques de Certification (DPC) de la société TBS INTERNET et expose les pratiques et principes juridiques, commerciaux et techniques employés par la société TBS INTERNET dans le cadre de ses prestations de délivrance de certificats ; étant entendu que lesdites prestations comprennent mais ne sont pas limitées à l'autorisation, l'émission, l'utilisation et la gestion des certificats numériques basée sur le standard X.509 (PKIX), conformément aux politiques de certification définies par TBS INTERNET. Il définit également les processus de certification sous-jacents à l'intention des Abonnés et décrit les opérations affectant le répertoire de la société TBS INTERNET. La DPC constitue également le moyen de définir avec précision les rôles et responsabilités des parties impliquées dans les pratiques de délivrance de certificats au sein de la PKI de la société TBS INTERNET.

Depuis le 1er avril 2021 les certificats TBS INTERNET X509 serveur sont émis par Sectigo et le document applicable se trouve à https://sectigo.com/legal sous la rubrique « Certificate Policies and Practices ».
Le tableau ci-dessous indique l'équivalence des produits :

Type de certificat TBS INTERNET	Type de certificat SECTIGO
Multiples Sites	Multi-Domain SSL
Test	Trial SSL
Standard	InstantSSL
E-commerce	InstantSSL Pro
Premium	PremiumSSL
Omnidomaine	PremiumSSL Wildcard

1.1 TBS INTERNET

La société TBS INTERNET est une Autorité de Certification (AC) et en tant que telle, délivre des certificats numériques de haute sécurité et d'une extrême fiabilité à l'intention des organisations mais également à l'intention des individus, le tout conformément à la DPC. En sa qualité d'AC, TBS INTERNET occupe plusieurs fonctions en rapport avec les systèmes de clé publique, entre autres : réception des requêtes, délivrance, révocation et renouvellement des certificats numériques ainsi que mise à jour, émission et publication des Listes de Certificats Révoqués (LCR) pour les utilisateurs de la PKI de TBS INTERNET. Dans le cadre de la délivrance de ses prestations de PKI, la société TBS INTERNET s'emploie à respecter, dans tous les aspects matériels, les normes internationales les plus exigeantes, y compris celles concernant la délivrance des certificats qualifiés, soumises à la directive européenne 99/93, au droit applicable à l'utilisation des signatures électroniques, ainsi qu'à toutes les autres législations et règlementations concernées.

La société TBS INTERNET accepte également au sein de son PKI, l'adhésion de tierces parties connues sous le nom d'Autorités d'Enregistrement, qui travaillent sous contrat avec la société TBS INTERNET. Les différentes AE du réseau international de TBS INTERNET émettent des certificats numériques TBS INTERNET ou, le cas échéant, des certificats numériques sous leur marque propre et pour cela, partagent la politique, les pratiques et

l'infrastructure de l'AC.

Cette activité d'AC de TBS INTERNET ne doit pas être confondue avec son activité de courtier en certificats. En tant que courtier, TBS INTERNET est amené à délivrer des certificats de marques différentes pour lesquelles il peut jouer le rôle de revendeur, distributeur ou Autorité d'Enregistrement. Cette activité de courtage n'est pas concernée ni décrite dans ce document.

1.2 La DPC de TBS INTERNET

La DPC de TBS INTERNET constitue une affirmation publique des pratiques de la société et des conditions de délivrance, de révocation et de renouvellement des certificats émis au sein de la hiérarchie du système TBS INTERNET. En accord avec la répartition des tâches propres à une AC, cette DPC est, de manière générale, divisée en plusieurs parties : technique, organisationnelle, pratique et juridique.

L'Autorité en charge de la Politique de Certification chez TBS INTERNET est responsable de la DPC, des accords connexes et des Politiques de Certification référencés dans le document. L'Autorité en charge de la Politique de Certification est joignable à l'adresse suivante :

TBS INTERNET Limited

Britannia House, Athol Street
Douglas, Isle of Man
IM1 1JD
British Isles

Tél : +44-330-684-0000

mél : legal@tbs-internet.com

Cette DPC, les accords connexes et les Politiques de Certification référencés dans ce document sont disponibles en ligne à l'adresse http://www.tbs-internet.com/CA/repository

1.3 Applicabilité, avenants à/et publication de la DPC

L'Autorité en charge de la Politique de Certification pour TBS INTERNET est responsable de la détermination de l'applicabilité des politiques de certification définies dans la DPC. L'Autorité est également responsable de la détermination de l'applicabilité des avenants à la DPC qui sont proposés avant la publication de celui-ci. Après acceptation desdites modifications par l'Autorité en charge de la Politique de Certification, modifications considérées par l'Autorité comme susceptibles d'avoir un impact significatif sur les utilisateurs de la DPC, une version réactualisée de la DPC est publiée dans le répertoire de la société (disponible à l'adresse http://www.tbs-internet.com/CA/repository/), avec une période préalable de trente jours avant l'application desdites modifications et le passage à un nouveau numéro permettant d'identifier la nouvelle version.

Les amendements considérés comme non « significatifs » sont ceux que l'Autorité en charge de la Politique de l'AC considère comme ayant peu ou pas d'impact sur les abonnés et sur les parties utilisatrices des certificats et des LCR émis par l'AC. Ces amendements pourront néanmoins être effectués sans avis préalable aux utilisateurs de la

DPC et sans changer le numéro de version de la DPC.

Un certain nombre de mesures ont été prises pour garantir, autant que possible, que la DPC de TBS INTERNET ne soit pas modifiée et publiée sans l'autorisation de l'Autorité en charge de la Politique de Certification.

La fréquence de publication de cette DPC n'est pas planifié, les changements apportés ainsi que la sortie d'une nouvelle version de ce document se fait lors d'un hypothétique ajout concernant les politiques de certification mise en œuvre par la société TBS INTERNET.

1.4 Autres Contrats & Déclarations de pratiques

La présente DPC rassemble uniquement les documents en rapport avec la prestation par TBS INTERNET, de services de certification. Les documents mentionnés dans la présente section concernent d'autres documents auxquels la DPC pourra, de temps en temps, faire référence (encore qu'il ne s'agit pas d'une liste exhaustive). Le tableau ci-dessous indique le nom des documents concernés, leur emplacement et leur statut de diffusion, qu'il soit public ou privé :

Document	Statut	Emplacement
Déclaration des Pratiques de Certification de la société TBS INTERNET	Public	Répertoire de TBS INTERNET : www.tbs-internet.com/CA/repository
Conditions générales d'utilisation des certificats numériques	Public	Répertoire de TBS INTERNET : www.tbs-internet.com/CA/repository
Contrat de la partie utilisatrice	Public	Répertoire de TBS INTERNET : www.tbs-internet.com/CA/repository

1.5 Responsabilité de TBS INTERNET

Pour en savoir plus sur la responsabilité civile de TBS INTERNET telle que définie par les articles de la DPC, veuillez consulter le Chapitre 5.

1.6 Conformité aux normes applicables

Les pratiques mentionnées dans la présente DPC sont inscrites dans le but de satisfaire, voire dépasser les exigences inhérentes aux normes communément acceptées par l'industrie ou en passe d'être développées, à savoir, entre autres, le programme Webtrust des Autorités de Certification de l'AICPA/CICA, le PKI Practices and Policy Framework ANS X9.79:2001 ainsi que les autres normes de l'industrie relatives aux opérations des AE.

1.7 Présentation de la politique de certification numérique

Un certificat numérique correspond à des données formatées, qui relient cryptographiquement un client identifié à

une clé publique spécifique. De ce fait, un certificat permet à une entité participant à une transaction électronique de prouver son identité aux autres participants dans le cadre de cette transaction. Les certificats numériques sont ainsi utilisés au niveau commercial au même titre qu'une carte d'identité, en tant qu'équivalent numérique.

Comme indiqué de manière détaillée dans la présente DPC, TBS INTERNET propose plusieurs types de certificats spécifiques. Ces différents types de certificats correspondent à des utilisations spécifiques et à des politiques différentes.

Depuis le 1er avril 2021 les certificats TBS INTERNET X509 serveur sont émis par Sectigo et le document applicable se trouve à https://sectigo.com/legal sous la rubrique « Certificate Policies and Practices ».

Demandeur	Type de certificat	Canaux de communication disponibles	Niveaux de validation [1]	Suggestion d'utilisation
~~Société ou individu~~	~~**Certificat Serveur :**~~ ~~*X509 Standard TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~ ~~- PKI PME~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification téléphonique de l'autorisation d'émission auprès du titulaire.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique du domaine (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un site Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~
~~Société ou individu~~	~~**Certificat Serveur :**~~ ~~*X509 Ecommerce TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~ ~~- PKI PME~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification téléphonique de l'autorisation d'émission auprès du titulaire.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique du domaine (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un site Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~
~~Société ou individu~~	~~**Certificat Serveur :**~~ ~~*X509 Premium TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~ ~~- PKI PME~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification téléphonique de l'autorisation d'émission auprès du titulaire.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique du domaine (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un site Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~

1 Niveaux de validation : la société TBS INTERNET ou l'Autorité d'Enregistrement agissant pour le compte de TBS INTERNET gèrent le processus de validation selon un certain nombre de directives extrêmement strictes ; directives données à l'autorité d'enregistrement. La section 1.10 de la présente DPC identifie les différentes autorités d'enregistrement et passe en revue leurs rôles et responsabilités respectifs.

Demandeur	Type de certificat	Canaux de communication disponibles	Niveaux de validation	Suggestion d'utilisation
~~Société ou individu~~	**~~Certificat Serveur :~~** ~~*X509 Omnidomaine TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~ ~~- PKI PME~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification téléphonique de l'autorisation d'émission auprès du titulaire.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique du domaine (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un site Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~
~~Société ou individu~~	**~~Certificat Serveur :~~** ~~*X509 Test TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique du domaine (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un site Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~
~~Société ou individu~~	**~~Certificat Serveur :~~** ~~*X509 Multiples Sites TBS*~~	~~- Site Internet de TBS INTERNET~~ ~~- Espace Client TBS certificats~~ ~~- Réseau Partenaires~~	~~• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande.~~ ~~• Vérification téléphonique de l'autorisation d'émission auprès du titulaire.~~ ~~• Vérification que le Demandeur a l'accord de l'exploitant technique des domaines (DCV).~~	~~Établir une session SSL/TLS entre le serveur hébergeant le certificat et un client (le visiteur) d'un ou plusieurs sites Internet. Ce protocole vise à authentifier le serveur pour le client et à garantir la confidentialité des données qui transitent durant la session SSL/TLS.~~
Société ou individu	**Certificat Client :** *X509 Sign & Login TBS*	- Site Internet de TBS INTERNET - Espace Client TBS certificats - Réseau Partenaires	• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande. • Vérification que le CN n'est pas un FQDN valide pour éviter toute confusion avec un certificat serveur. • Vérification téléphonique de l'autorisation d'émission auprès du titulaire.	Authentifier un utilisateur lors d'une session SSL/TLS ou signer numériquement des documents électroniques. Ceci assure l'origine du document ou de la connexion.
Société ou individu	**Certificat Client :** *X509 Test Sign & Login TBS*	- Site Internet de TBS INTERNET - Espace Client TBS certificats - Réseau Partenaires	• Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande. • Vérification que le CN n'est pas un FQDN valide pour éviter toute confusion avec un certificat serveur.	Authentifier un utilisateur lors d'une session SSL/TLS ou signer numériquement des documents électroniques. Ceci assure l'origine du document ou de la connexion.

Demandeur	Type de certificat	Canaux de communication disponibles	Niveaux de validation	Suggestion d'utilisation
Individu	**Certificat Client :** *X509 Email Professionnel TBS*	- Site Internet de TBS INTERNET - Espace Client TBS certificats - Réseau Partenaires	• Challenge automatique pour vérifier que le titulaire de l'adresse mél a bien demandé le certificat. • Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande. • Vérification que le CN est le nom de l'individu. • Vérification téléphonique de l'autorisation d'émission auprès du titulaire.	Permet de signer numériquement les méls (norme S/MIME). Il permet également le chiffrement du mél avec un correspondant pareillement équipé. Il authentifie également un utilisateur lors d'une session SSL/TLS ou pour signer numériquement des documents électroniques.
Individu	**Certificat Client :** *X509 Test Email Professionnel TBS*	- Espace Client TBS certificats - Réseau Partenaires	• Challenge automatique pour vérifier que le titulaire de l'adresse mél a bien demandé le certificat. • Confirmation du droit à utiliser le nom d'organisation spécifié lors de la demande. • Vérification que le CN est le nom de l'individu.	Permet de signer numériquement les méls (norme S/MIME). Il permet également le chiffrement du mél avec un correspondant pareillement équipé. Il authentifie également un utilisateur lors d'une session SSL/TLS ou pour signer numériquement des documents électroniques.
Individu	**Certificat Client :** *X509 Email Particulier TBS*	- Site Internet de TBS INTERNET - Espace Client TBS certificats - Réseau Partenaires	• Challenge automatique pour vérifier que le titulaire de l'adresse mél a bien demandé le certificat. • Confirmation du droit à utiliser le nom de personne physique. • Vérification que le CN est le nom de l'individu. • Vérification téléphonique de l'autorisation d'émission auprès du titulaire.	Permet de signer numériquement les méls (norme S/MIME). Il permet également le chiffrement du mél avec un correspondant pareillement équipé. Il authentifie également un utilisateur lors d'une session SSL/TLS ou pour signer numériquement des documents électroniques.
Individu	**Certificat Client :** *X509 Email Novice TBS*	- Site Internet de TBS INTERNET - Espace Client TBS certificats - Réseau Partenaires	• Challenge automatique pour vérifier que le titulaire de l'adresse mél a bien demandé le certificat. • Confirmation du droit à utiliser le nom de personne physique. • Vérification que le CN est le nom de l'individu. • Vérification téléphonique de l'autorisation d'émission auprès du titulaire.	Permet de signer numériquement les méls (norme S/MIME). Il permet également le chiffrement du mél avec un correspondant pareillement équipé.

Demandeur	Type de certificat	Canaux de communication disponibles	Niveaux de validation	Suggestion d'utilisation
Individu : représentant d'une organisation	**Certificat Client :** *X509 Utilisateur TBS*	- PKI PME	• Lors de l'ouverture d'un compte PKI, le demandeur doit fournir la preuve de son droit à utiliser le nom d'organisation spécifié lors de la demande. • Recherche d'une adresse mél pour vérifier qu'il s'agit bien d'une adresse distinctive sur le compte PKI Manager. • Vérification que le domaine utilisé dans le mél est bien sur la liste des domaines utilisables (vérifiée à l'ouverture du compte).	Permet de signer numériquement les méls (norme S/MIME). Il permet également le chiffrement du mél avec un correspondant pareillement équipé. Il authentifie également un utilisateur lors d'une session SSL/TLS ou pour signer numériquement des documents électroniques.

Dans la mesure où l'usage suggéré d'un certificat numérique diffère selon l'application, il est fortement recommandé à l'abonné d'étudier au mieux les exigences inhérentes à cette même application, et ce avant de faire la demande du certificat.

1.8 Hiérarchie de la PKI TBS INTERNET

TBS INTERNET travaille en collaboration avec Sectigo (www.sectigo.com, un fournisseur habilité par le programme Webtrust des Autorités de Certification de l'AICPA/CICA) pour les certificats de AC racines. Ce partenariat permet à TBS INTERNET d'offrir des certificats numériques de haute sécurité, et ce en bénéficiant du niveau de confiance associé aux certificats de Sectigo (référencés sous diverses appellations : UTN, AddTrust). La représentation de la PKI de TBS INTERNET ci-dessous illustre parfaitement la hiérarchie utilisée.

1.8.1 Certificats mél

USERTrust RSA Certification Authority (numéro de série = 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ Sectigo RSA Client Authentication and Secure Email CA *(numéro de série = 4d:94:2c:10:d4:3b:e0:94:09:c5:81:2d:3a:2b:06:4f, expiration = Tue 31 Dec 23:59:59 GMT 2030)*

→ *Entité de fin de chaine SSL (numéro de série = x, expiration = 1 an après la date d'émission)*

1.8.2 Certificats serveur standard

USERTrust RSA Certification Authority (numéro de série = 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ TBS X509 CA business 2 *(numéro de série = 34:04:39:64:3d:2e:cb:bd:f4:e6:a9:57:5d:e6:c7:a6, expiration = Sep 22 23:59:59 2024 GMT)*

→*Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 3 ans après la date d'émission)*

1.8.3 Certificats serveur Pro Hosting

USERTrust RSA Certification Authority (numéro de série = 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ TBS X509 CA pro hosting 2 *(numéro de série = d2:28:2e:f0:70:e5:f7:0f:2d:2c:af:12:ee:ae:19:fa, expiration = Sep 22 23:59:59 2024 GMT)*

→Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 3 ans après la date d'émission)

1.8.4 Certificats client généraux

Pour les certificats expirant après 2024 :

USERTrust RSA Certification Authority (numéro de série = 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ TBS X509 CA persona 3 (RSA) *(numéro de série = 14:f0:24:15:22:61:aa:96:cc:7e:9e:2e:84:25:e0:95, expiration = Tue Jun 12 23:59:59 UTC 2029)*

→Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 6 ans après la date d'émission)

ou

USERTrust ECC Certification Authority (numéro de série = 5c:8b:99:c5:5a:94:c5:d2:71:56:de:cd:89:80:cc:26, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ TBS X509 CA persona 3 (ECC) *(numéro de série = 32:06:42:3d:e6:c6:2c:96:8c:8e:c1:9c:f7:6e:04:e3, expiration = Tue Jun 12 23:59:59 UTC 2029)*

→Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 6 ans après la date d'émission)

Ou pour les certicats expirant après 2020 :

USERTrust RSA Certification Authority (numéro de série = 01:fd:6d:30:fc:a3:ca:51:a8:1b:bc:64:0e:35:03:2d, expiration = Mon 18 Jan 23:59:59 GMT 2038)

→ TBS X509 CA persona 2 *(numéro de série = db:7e:d2:93:87:29:3d:ce:e1:7f:21:48:23:66:4b:36, expiration = Sep 22 23:59:59 2024 GMT)*

→Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 4 ans après la date d'émission)

Ou pour les certicats expirant après 2020 et émis avant 2020 :

AddTrust External CA Root (numéro de série = 1, expiration = May 30 10:48:38 2020 GMT)

→ TBS X509 CA persona 2.1 *(numéro de série = 2c:5f:42:58:31:d5:99:f9:85:fd:f0:40:b8:8d:b1:7e, expiration = May 30 10:48:38 2020 GMT)*

→Entité de fin de chaine SSL (numéro de série = x, expiration = 30 jours à 6 ans après la date d'émission)

1.9 L'Autorité de Certification TBS INTERNET

Dans sa fonction en tant qu'Autorité de Certification (AC), la société TBS INTERNET fournit des prestations de certification à partir de sa propre PKI. Et dans cette tâche, la société TBS INTERNET

s'engage à :

- Faire en sorte que ses prestations soient en conformité avec la DPC (ou avec toute pratique commerciale stipulée par une autre AC), entendu que les présentes sont susceptibles d'être modifiées de temps en temps par amendements ; amendements publiés dans le répertoire de TBS INTERNET à l'adresse (http://www.tbs-internet.com/CA/repository/).

- Émettre et publier des certificats dans les délais impartis, conformément aux délais d'émission définis dans la présente DPC.

- À réception d'une demande valable visant à révoquer un certificat, demande effectuée par une personne habilitée à faire une demande de révocation et utilisant les méthodes de révocation spécifiée dans la DPC, révoquer un certificat émis et utilisé dans le cadre de la PKI de TBS INTERNET.

- Publier régulièrement les LCR, conformément à la politique de certification applicable et en conformité avec les articles des présentes.

- Distribuer les certificats émis en accord avec les méthodes décrites dans les présentes.

- Mettre à jour les LCR dans les délais impartis et conformément à la DPC.

- Notifier les abonnés par mél, de l'expiration imminente de leur certificat émis par TBS INTERNET (pour la période spécifiée dans les présentes).

1.10 Les Autorités d'Enregistrement de TBS INTERNET

La société TBS INTERNET a mis en place l'infrastructure nécessairement sécurisée visant à administrer dans son intégralité le cycle de vie des certificats numériques au sein de son PKI. À travers un réseau d'Autorités d'Enregistrement (AE), TBS INTERNET met également a disposition de ses abonnés, des prestations faisant appel aux différents services proposés par les autorités de certification. Ainsi, les AE sont chargées de :

- Accepter, évaluer, approuver ou rejeter l'enregistrement de demandes de certificat.

- Vérifier l'exactitude et l'authenticité des informations fournies par l'abonné lors de la demande, conformément aux instructions de validation spécifiées par la société TBS INTERNET.

- Utiliser des documents officiels ou notariés, ou tout autre document indiqué pour évaluer la demande d'un abonné.

- Vérifier l'exactitude et l'authenticité des informations fournies par l'abonné lors de la procédure de refabrication ou de renouvellement, conformément aux instructions de validation spécifiées par la société TBS INTERNET.

Les AE de TBS INTERNET fonctionnent localement, dans leur propre contexte de partenariat géographique ou professionnel sur approbation et autorisation de la société TBS INTERNET, conformément aux pratiques et procédures spécifiées par la société TBS INTERNET.

La société TBS INTERNET sélectionne ses Autorités d'Enregistrement (AE) parmi ses partenaires. Après avoir reçu la validation leur permettant d'adhérer aux programmes qui les intéressent, les partenaires sont habilités à agir en tant qu'AE pour le compte de la société TBS INTERNET. Les AE sont astreintes à opérer dans les limites des

instructions de validation définies et transmises par TBS INTERNET aux AE dès leur adhésion aux programmes.

1.10.1 Programme de partenariat Distributeur

La société TBS INTERNET a mis en place un réseau de partenaires distributeurs. Par le biais de celui-ci, les partenaires en ayant reçu l'autorisation ont la possibilité d'intégrer les certificats numériques TBS INTERNET dans leur portefeuille de produits. Ces partenaires distributeurs ont la responsabilité de référer leurs clients intéressés par des certificats numériques à TBS INTERNET, qui détient un contrôle total sur tout le cycle de vie du processus de certification, à savoir la demande, l'émission, le renouvellement et la révocation. Du fait de la nature même du programme, les distributeurs doivent auparavant autoriser les commandes en attente des clients via leur compte distributeur, puis TBS INTERNET effectue les recherches nécessaires à la validation de ces commandes de certificat. Les partenaires distributeurs se doivent tous, sans exception, de fournir les preuves de leur statut d'entreprise (se référer à la section 4.3 pour les exemples des documents requis). En outre, ils doivent, avant de pouvoir bénéficier des options du programme, signer un contrat de partenariat distributeur avec TBS INTERNET.

1.10.2 Programme de partenariat Hébergeur

Le programme de Partenariat Hébergeur permet à des organisations fournissant des prestations d'hébergement de gérer le cycle de vie des certificats pour le compte de tiers ou pour leur société ou groupe de sociétés. Ces partenaires ont la possibilité d'initialiser des demandes de certificat pour le compte de leurs clients.

Par le biais d'un « frontal » appelé également « Espace Client », le partenaire Hébergeur peut bénéficier des fonctions propres à une AE, à savoir, entre autres mais non limitée à celle-ci, la possibilité d'émettre des certificats. Le distributeur Hébergeur doit se conformer aux instructions de validation qui lui sont présentées par TBS INTERNET dans le cadre du contrat. Le partenaire Hébergeur se doit de fournir tout document nécessaire à la vérification de ses demandes.

Les partenaires Hébergeurs se doivent tous, sans exception, de fournir les preuves de leur statut d'entreprise (se référer à la section 4.3 pour les exemples des documents requis). En outre, ils doivent, avant de pouvoir bénéficier des options du programme, signer un contrat de partenariat distributeur avec TBS INTERNET.

1.10.3 Programme PKI PME

PKI PME de TBS INTERNET est un service d'infrastructures à clé publique en entreprise entièrement externalisé, qui repose sur l'architecture EPKI de Sectigo. Elle permet aux titulaires d'un compte PKI PME de maîtriser le processus de certification sur l'ensemble de son cycle de vie, à savoir : demande, émission, renouvellement et révocation. Ce service s'applique exclusivement aux certificats à l'intention des serveurs d'entreprise, intranets, extranets, partenaires commerciaux et périphériques matériels.

Par le biais d'un « frontal » appelé également « Zone d'administration », le détenteur d'un compte administrateur PKI PME bénéficie des fonctions propres à une AE, à savoir, entre autres mais non limitée à celle-ci, la possibilité d'émettre certains certificats X509 serveurs TBS et des certificats X509 Utilisateurs TBS.

Le détenteur du compte administrateur du PKI PME ne peut émettre des certificats qu'à l'intention des entreprises légitimes et de leurs représentants : noms de domaine (serveurs), intranets, extranets, partenaires commerciaux, employés et périphériques matériels.

1.11 Les abonnés

Les abonnés aux services TBS INTERNET sont des individus ou des entreprises qui utilisent la PKI pour tout ce qui concerne leurs communications et transactions prises en charge par TBS INTERNET. Les abonnés sont clairement

identifiés dans le certificat. Ils détiennent la clé privée correspondante à la clé publique spécifiée dans le certificat. Avant une quelconque vérification d'identité et l'émission dudit certificat, l'abonné possède le statut de demandeur des services de TBS INTERNET.

1.12 Les parties utilisatrices

Les parties utilisatrices utilisent les services de la PKI pour tout ce qui concerne les certificats TBS INTERNET. Ils se fient raisonnablement à ces mêmes certificats et/ou signatures numériques, sur la base de la comparaison par rapport à une clé publique figurant sur le certificat de l'abonné.

Pour vérifier la validité d'un certificat numérique et avant de pouvoir se fier aux informations figurant sur celui-ci, les parties utilisatrices doivent se référer à la Liste des Certificats Révoqués (LCR) pour vérifier que le certificat n'a pas été révoqué par TBS INTERNET. L'URL de la LCR est indiquée dans le certificat.

2 Technologie

Cette section aborde certains aspects technologiques des services de PKI et de l'infrastructure de TBS INTERNET. Les composants de signature et de gestion de clefs sont opérés par Sectigo. Une description plus détaillée est disponible dans la DPC de Sectigo, disponible sur https://sectigo.com/legal

2.1 L'infrastructure de l'AC TBS INTERNET

Pour fournir ses services de certification, l'infrastructure de l'AC TBS INTERNET repose sur des systèmes d'une extrême fiabilité. Par système d'une extrême fiabilité, nous entendons du matériel informatique, du logiciel et des procédures capables d'apporter une résilience acceptable face aux risques de sécurité, qui fournissent un niveau raisonnable de disponibilité, de fiabilité et de fonctionnement et qui soient en conformité avec la politique de sécurité mise en vigueur.

2.1.1 Récupération & protection des clés de signature d'une AC racine

La protection des paires de clés de signature de l'AC racine se fait à l'aide d'un coprocesseur cryptographique IBM 4578, certifié conforme à la norme FIPS 140-1 Level 4 pour la génération, le stockage et l'utilisation des clés cryptographiques. Les clés de signature, générées par le coprocesseur, sont ainsi cryptées à 2048 bits.

En cas de sinistre et pour pouvoir ultérieurement reconstituer les clés racines, celles-ci sont chiffrées et conservées dans un endroit sûr. La clé de déchiffrement est découpée en **m** nombres de morceaux, chacun sur support amovible et nécessite un nombre spécifique **n** de **m** supports amovibles pour être reconstituée.

Lorsque des clés de signature d'une AC racine doivent être sauvegardées sur un autre module de protection cryptographique, les clés ne sont transférées d'un module à l'autre que dans un format crypté.

2.1.2 Processus de génération des clés de signature d'une AC racine

La société TBS INTERNET génère en toute sécurité et protège ses propres clés à l'aide d'un système d'une extrême fiabilité (le coprocesseur IBM 4758, accrédité à la norme FIPS PUB 140-1 level 4) et s'emploie à prendre toutes les précautions nécessaires pour prévenir leur utilisation accidentelle ou non autorisée.

Ainsi, les clés de l'AC racine TBS INTERNET sont générées conformément aux instructions détaillées du guide de référence Root Key Generation Ceremony Reference. Les activités entreprises et le nom des employés impliqués dans la Root Key Generation Ceremony (procédure de génération des clés racines) sont enregistrés, en cas d'audit ultérieur. Les procédures de génération de clés racines ayant lieu ultérieurement seront également enregistrées dans le guide de référence.

2.1.3 Archivage des clés de signature d'une AC racine

Lorsqu'une paire de clés de signature d'une AC racine arrive à expiration, elle est archivée pendant une durée d'au moins sept ans. Les clés sont archivées dans un module de protection cryptographique sécurisé (dans les mêmes conditions sécurisées qu'avant leur expiration), comme indiqué dans la section 2.1.1 de cette DPC.

2.1.4 Procédures employées lors du changement d'une clé de signature d'une AC racine

En fin de vie d'une clé privée, une nouvelle paire de clés de signature est commandée. Tous les certificats dorénavant émis ainsi que les LCR seront signés avec la nouvelle clé privée. Il est possible que les deux clés, la nouvelle et l'ancienne, soient, à un moment ou à un autre, actives toutes les deux. Pour envoyer le nouveau certificat doté de la nouvelle clé publique aux abonnés et aux parties utilisatrices, les méthodes d'envoi employées sont celles décrites dans la section 2.1.5 de cette DPC.

2.1.5 Envoi des clés publiques d'une AC racine aux abonnés

Tous les certificats d'AC racine de TBS INTERNET sont accessibles dans des répertoires en ligne à l'adresse http://www.tbs-internet.com/CA/repository.

Le certificat UTN USERFirst Hardware est présent dans Internet Explorer 5.01 et supérieur, Netscape 8.1 et supérieur, Opera 8.0 et supérieur, Mozilla 1.76 et supérieur, Konqueror 3.5.2 et supérieur, Safari 1.2 et supérieur, Firefox 1.02 et supérieur, Camino et SeaMonkey et de ce fait, est accessible aux parties utilisatrices par le biais de ces navigateurs.

Le certificat AddTrust External CA Root est présent dans Netscape 4.x et supérieur, Opera 8.00 et supérieur, Mozilla 0.6 et supérieur, Konqueror, Safari 1.0 et supérieur, Camino et SeaMonkey et de ce fait, est accessible aux parties utilisatrices par le biais de ces navigateurs.

TBS INTERNET fourni la chaîne de certification dans son intégralité (voir le chapitre 1.8 de cette DPC) dès l'émission et l'envoi du certificat à l'abonné.

2.1.6 Pilotage de l'AC sur le plan physique

2.1.6.1 TBS INTERNET

L'accès aux équipements gérant le système d'information de TBS INTERNET est restreint par un contrôle d'accès physique. Les locaux disposent de systèmes anti-incendies et d'alimentations électriques secourus.

La société TBS INTERNET affirme sa volonté de prendre toutes les mesures raisonnables possibles pour détecter et empêcher la violation, la perte, la détérioration ou l'utilisation accidentelle de ses actifs, ainsi que l'interruption de ses activités.

2.1.6.2 Sectigo

L'accès aux aires sécurisées au sein de Sectigo est restreint par un contrôle d'accès physique. Ces aires ne sont accessibles qu'aux personnes autorisées (nommées dans les présentes Personnes de confiance). Un certain nombre de systèmes de contrôle d'accès à cartes ont été mis en place, visant à contrôler, surveiller et enregistrer l'accès à l'ensemble des infrastructures de l'installation. L'accès aux installations techniques dans les aires sécurisées est protégé (endroits sous clé et contrôle d'accès logique).

Sectigo s'emploie à prendre toutes les mesures raisonnables possibles pour garantir que les aires sécurisées soient protégées de :

- des incendies et de la fumée susceptibles d'endommager les installations (la protection contre les incendies est en conformité avec la règlementation locale en matière de prévention des incendies).
- d'éventuelles inondations et dégâts des eaux.

Les aires de sécurité de Sectigo sont dotées de deux blocs d'alimentation électrique (un bloc d'alimentation principal et un bloc d'alimentation de secours) qui garantissent un accès continu et ininterrompu à une alimentation électrique. Des systèmes de chauffage/air conditionné, quant à eux, préviennent une éventuelle surchauffe et

maintiennent un niveau d'humidité appropriée.

La société Sectigo affirme sa volonté de prendre toutes les mesures raisonnables possibles pour détecter et empêcher la violation, la perte, la détérioration ou l'utilisation accidentelle de ses actifs, ainsi que l'interruption de ses activités.

2.2 Administration des certificats numériques

L'administration des certificats numériques de TBS INTERNET fait référence aux fonctions suivantes (liste non limitative) :

- Vérification de l'identité du demandeur d'un certificat.
- Autorisation de l'émission des certificats.
- Émission des certificats.
- Révocation des certificats.
- Listage des certificats.
- Distribution des certificats.
- Publication des certificats.
- Stockage des certificats.
- Récupération des certificats en fonction de leur usage prévu.

La société TBS INTERNET gère le processus de certification dans sa totalité, dans son PKI, soit directement soit par le biais d'une AE habilitée par elle. TBS INTERNET ne s'occupe pas des fonctions associées à la génération, à l'émission, à la mise hors-service ou à la destruction de la paire de clés d'un abonné.

2.3 Répertoires, archives et listes des certificats révoqués

La société TBS INTERNET gère et met publiquement à disposition ses répertoires des certificats révoqués par le biais des Listes de Certificats Révoqués (LCR). Toutes les LCR émises par TBS INTERNET sont des listes de révocation X.509v2, en particulier, selon les exigences du RFC3280. Avant de pouvoir se fier aux informations figurant sur un certificat, utilisateurs et parties utilisatrices sont fortement invités à consulter systématiquement les répertoires de certificats révoqués. La société TBS INTERNET actualise et publie une nouvelle LCR toutes les 24 heures, voire plus fréquemment dans des circonstances exceptionnelles. La LCR des certificats des entités d'extrémité est accessible via les URL suivantes :

http://crl.tbs-x509.com/TBSX509CASGC.crl
http://crl.tbs-x509.com/TBSX509CAbusiness.crl
http://crl.tbs-x509.com/TBSX509CAinstitutionnel.crl
http://crl.tbs-x509.com/TBSX509CApersona.crl
http://crl.tbs-x509.com/TBSX509CAprohosting.crl
http://crl.tbs-x509.com/TBSX509CAsignaturecomposants.crl

http://crl.tbs-x509.com/TBSX509CAbusiness2.crl
http://crl.tbs-x509.com/TBSX509CApersona2.crl
http://crl.tbs-x509.com/TBSX509CAprohosting2.crl
http://crl.tbs-x509.com/TBSX509CApersona2-1.crl

http://crl.tbs-x509.com/TBSX509CAPersona3RSA.crl
http://crl.tbs-x509.com/TBSX509CAPersona3ECC.crl

Depuis le 7 novembre 2008 la validation en ligne de la validité des certificats est possible par le protocole OCSP. Les certificats émis depuis cette date contiennent un champ OCSP mentionnant le service http://ocsp.tbs-x509.com

La société TBS INTERNET publie également un répertoire comprenant les informations légales concernant ses services de PKI, à savoir la présente DPC, les différents contrats et avis, les références apparaissant dans cette DPC ainsi que toutes les autres informations que la société considère comme essentielles à la distribution de ses prestations. Le répertoire des informations légales de TBS INTERNET est accessible à l'adresse http://www.tbs-internet.com/CA/repository/

2.4 Types de certificats TBS INTERNET

La société TBS INTERNET propose aujourd'hui un portefeuille de certificats numériques et de produits connexes susceptibles de répondre aux différents besoins des utilisateurs en matière de communication d'entreprise et de communication personnelle sécurisées. Ces produits comprennent, mais ne sont pas limités à la sécurisation des méls, la protection des transactions en ligne et l'identification des personnes quelles qu'elles soient sur le plan juridique ou physique, ou l'identification d'équipements sur un réseau ou dans une communauté.

La société TBS INTERNET est susceptible de mettre à jour ou de développer sa liste de produits, y compris les types de certificats que la société se propose d'émettre, selon son bon jugement. La publication ou la mise à jour de l'éventail de produits offerts par TBS INTERNET ne peut engendrer de réclamation, demande d'indemnisation, remboursement, recours par quelque tierce partie que ce soit. À l'introduction d'un nouveau certificat dans la gamme de produits de TBS INTERNET, une version modifiée de cette DPC sera rendue publique au moins sept jours avant la sortie officielle, sur les sites Internet officiels de TBS INTERNET.

Les certificats suspendus ou révoqués sont comme de juste référencés dans les LCR et publiés dans les répertoires de TBS INTERNET. La société TBS INTERNET ne prévoit pas la séquestre des clés privées d'un abonné. Les différents type de certificats de TBS INTERNET ont des usages et des politiques différentes. Le tarif des certificats est proposés sur les sites de TBS INTERNET. La garantie maximale associée à un certificat est documentée dans la section 5.31.

On recommande aux utilisateurs d'étudier quel certificat convient à leur besoin avant de déposer une demande de certificats, du fait de leur spécificités.

2.4.1 Les certificats Serveur TBS INTERNET

La société TBS INTERNET met à disposition de ses abonnés des certificats Serveur qui, en combinaison avec un serveur Web utilisant le protocole Secure Socket Layer (SSL) attestent de l'identité du serveur public utilisé, activent et authentifient entièrement et totalement les communications - et ce en toute sécurité - entre les clients et les différents partenaires commerciaux. Les certificats Serveur de TBS INTERNET sont proposés en 16 variantes X509 TBS différentes listées ci-dessous. Les prix des différents certificats peuvent être consultés sur les sites Internet officiels respectifs de TBS INTERNET.

a) Le certificat X509 Standard TBS

Le certificat Standard constitue le certificat Serveur d'entrée de gamme de TBS INTERNET. Il est destiné avant tout aux sites Internet effectuant des opérations de commerce électronique ou aux sites Web susceptibles de transférer des données de faible valeur pour/au sein de réseaux internes.

Conformément à la section 4.2.4 (Processus de validation) de cette DPC, les certificats Standard pourront

interroger la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Standard entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui.
Du fait de l'accroissement de la vitesse de validation et de la nature même de l'usage que TBS INTERNET souhaite faire des certificats Standard, ceux-ci affichent une garantie réduite. La garantie maximale associée à un certificat Standard est de 50 $.

b) Le certificat X509 Ecommerce TBS

Le certificat Ecommerce correspond au moyen de gamme des certificats Serveur distribués par TBS INTERNET. Il est destiné avant tout aux sites Internet effectuant des opérations de commerce électronique ou aux sites Web susceptibles de transférer des données dans des réseaux internes.

Conformément à la section 4.2.4 (Processus de validation) de cette DPC, les certificats Ecommerce pourront également interroger la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Ecommerce entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui.

La garantie maximale associée à un certificat Ecommerce est de 2 500 $.

c) Le certificat X509 Premium TBS

Le certificat Premium est le certificat Serveur de niveau professionnel de TBS INTERNET. Il est destiné avant tout aux sites Internet effectuant des opérations de commerce électronique de valeur élevée ou aux sites Web susceptibles de transférer des données dans des réseaux internes.

Conformément à la section 4.2.4 (Processus de validation) de cette DPC, les certificats Premium pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Premium entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui.

La garantie maximale associée à un certificat Premium est de 10 000 $.

d) Le certificat X509 Omnidomaine TBS

Le certificat Omnidomaine est un certificat Serveur de niveau professionnel servant à sécuriser plusieurs sous-domaines, et ce avec un seul certificat. Il est destiné aux sites Internet effectuant des opérations de commerce électronique de valeur élevée ou aux sites Web susceptibles de transférer des données dans des réseaux internes.

Conformément à la section 4.2.4 (Processus de validation) de cette DPC, les certificats Omnidomaine pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Omnidomaine entraînent une validation des informations soumises par le demandeur par des moyens autres (mode asymétrique) que ceux fournis par lui.

La garantie maximale associée à un certificat Omnidomaine est de 10 000 $.

e) Le certificat X509 Test TBS

Les certificats Test sont des certificats Serveur conçus pour aider les clients à utiliser le protocole SSL dans un environnement de test, avant le premier passage à une solution SSL complète.

Ils sont susceptibles d'être utilisés dans un environnement externe et de ce fait, peuvent contenir des informations qu'une partie utilisatrice peut vouloir invoquer. Par conséquent, ces certificats sont tous validés

avant leur émission, conformément à la section 4.2.3 de la présente DPC.

Les certificats Test ne sont destinés à être utilisés que dans le cadre de test et par conséquent, n'impliquent aucune garantie. Ils sont gratuits.

f) Le certificat X509 Multiples Sites TBS

Le certificat Multiples Sites est le certificat Serveur de niveau professionnel de TBS INTERNET. Il est destiné aux ISPs et grands comptes exploitants plusieurs sites web ou domaines sur la même machine ou le même répartiteur de charge. Ce certificat contient plusieurs champs CN.

Conformément à la section 4.2.8 (Processus de validation) de cette DPC, les certificats Multi-Sites pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Multi-Site entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui. Le nom usuel principal est vérifié.

Il n'y a pas de garantie associé à ce certificat.

2.4.2 Les certificats Clients Email de TBS INTERNET

La société TBS INTERNET met à disposition de ses clients des certificats Client Email qui, combinés à une application mél prenant en charge le protocole S/MIME, permet à un abonné de signer numériquement un mél à l'intention des parties utilisatrices, ou aux parties utilisatrices de crypter un mél à l'intention de l'abonné. Les prix des différents certificats peuvent être consultés sur les sites Internet officiels de TBS INTERNET correspondants.

a) Certificats Email Novice

Les certificats Email Novice ne peuvent être utilisés par une personne comme outil de représentation d'une entreprise.

Conformément à la section 4.2.6 (Processus de validation) de cette DPC, en effectuant un contrôle de validité de l'adresse mél, la société TBS INTERNET considère qu'un abonné possède ou détient l'accès direct à l'adresse mél figurant sur le certificat Email Novice. Cependant, dans la mesure où la vérification de l'abonné n'a pas lieu, son identité ne peut être garantie.

b) Les certificats Utilisateur PKI PME

Les certificats Utilisateur PKI PME sont émis à l'intention des personnes physiques uniquement et peuvent être utilisés par une personne comme outil de représentation d'une entreprise, dans la mesure où le nom de celle-ci figure sur le certificat.

Les certificats Utilisateur sont mis à disposition des détenteurs d'un compte PKI PME TBS INTERNET. Le compte PKI PME peut être ainsi utilisé pour effectuer une demande de certificat TBS INTERNET (Serveur ou Client Email). Il contient les coordonnées de l'entreprise (nom, adresses, pays) de la société détentrice du compte.

Les administrateurs autorisés du compte PKI PME peuvent se connecter en ligne sur le compte et faire une demande de certificat Utilisateur pour les employés ou le personnel autorisé de l'entreprise uniquement.

Conformément à la section 4.2.7 (Processus de validation) de cette DPC, TBS INTERNET valide le droit de la société concernée à utiliser le nom de domaine figurant sur le certificat Utilisateur. L'entreprise devra attester de la légitimité de la personne nommée lors de la demande et ce avant l'émission du certificat Utilisateur.

c) Les certificats Email Professionnel

Les certificats Email Professionnel sont émis à l'intention des personnes physiques ou d'un service d'une personne morale et peuvent être utilisés par une personne comme outil de représentation d'une entreprise, dans la mesure où le nom de celle-ci figure sur le certificat.

Conformément à la section 4.2.11 (Processus de validation) de cette DPC, les certificats Email Professionnel pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Email Professionnel entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui. En effectuant un contrôle de validité de l'adresse mél, la société TBS INTERNET considère qu'un abonné possède ou détient l'accès direct à l'adresse mél figurant sur le certificat.

Il n'y a pas de garantie associé à ce certificat.

d) Les certificats Test Email

Les certificats Test Email permettent de tester la signature électronique

Conformément à la section 4.2.11 (Processus de validation) de cette DPC, les certificats Test Email pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Email entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui. En effectuant un contrôle de validité de l'adresse mél, la société TBS INTERNET considère qu'un abonné possède ou détient l'accès direct à l'adresse mél figurant sur le certificat.

Il n'y a pas de garantie associé à ce certificat.

f) Les certificats Email Particulier

Les certificats Email Particulier sont émis à l'intention des personnes physiques dans un cadre privé et ne peuvent pas être utilisés par une personne comme outil de représentation d'une entreprise.

Conformément à la section 4.2.12 (Processus de validation) de cette DPC, les certificats Email Particulier pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Email Particulier entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui. En effectuant un contrôle de validité de l'adresse mél, la société TBS INTERNET considère qu'un abonné possède ou détient l'accès direct à l'adresse mél figurant sur le certificat.

Il n'y a pas de garantie associé à ce certificat.

2.4.3 Les certificats Client d'authentification de TBS INTERNET

La société TBS INTERNET met à disposition de ses clients des certificats client d'authentification permettent de s'authentifier de façon forte auprès d'un serveur SSL/TLS ou encore de signer électroniquement des documents. Il ne permet pas d'utiliser le protocole S/MIME. Les prix des différents certificats peuvent être consultés sur les sites Internet officiels de TBS INTERNET correspondants.

a) Certificats Sign & Login

Les certificats Sign & Login permettent d'identifier des utilisateurs personnes physiques ou morales afin de leur attribuer des droits dans des systèmes ou pour signer des documents. Ils remplacent les certificats Client Auth.

Conformément à la section 4.2.9 (Processus de validation) de cette DPC, les certificats Sign & Login pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification. Toutes les demandes de certificats Sign & Login entraînent une validation des informations soumises par le demandeur par des moyens autres que ceux fournis directement par lui.

Il n'y a pas de garantie associé à ce certificat.

b) Certificats Test Sign & Login

Les certificats Test Sign & Login permettent de tester l'authentification par certificats ainsi que la signature électronique.

Conformément à la section 4.2.10 (Processus de validation) de cette DPC, les certificats Test Sign & Login pourront également se servir de la base de données de TBS INTERNET, qui aide ainsi le processus de demande de certification.

Il n'y a pas de garantie associé à ce certificat.

2.5 Extensions et dénomination

2.5.1 Les extensions d'un certificat numérique

TBS INTERNET utilise le standard de cryptographie X.509, version 3 pour générer les certificats numériques utilisés dans son PKI. X.509v3 permet à une AE d'ajouter certaines extensions à la structure de base des certificats. TBS INTERNET utilise un certain membre d'extensions pour les types d'utilisation prévus par le standard X.509v3, conformément à l'amendement 1 de l'ISO-IEC 9594-8, 1995. Le X.509v3 est la norme de l'Union Internationale des Télécommunications (UIT) pour les certificats numériques.

2.5.2 Incorporation par référence des extensions et dénomination améliorée

Le champ Dénomination étendue correspond à un champ supplémentaire à l'usage des organisations sur un certificat au standard X.509v3. Les renseignements saisis dans le champ Unité administrative peuvent également être inclus dans le champ d'extension Politique de certification du certificat que la société TBS INTERNET est susceptible de renseigner.

2.6 Processus de génération de la clé privée d'un abonné

L'abonné est seul responsable de la génération de la clé privée utilisée lors de la demande d'un certificat. La société TBS INTERNET ne prévoit aucune prestation en termes de sauvegarde, récupération, dépôt ou génération de clés.

Lors de la demande de certificat, l'abonné est seul responsable de la génération du bi-clé RSA correspondant au type de certificat faisant l'objet de la demande. Durant cette même demande, l'abonné devra soumettre une clé publique ainsi que des informations personnelles/professionnelles, sous la forme d'une demande de signature de certificat (Certificate Signing Request ou CSR).

Habituellement, les demandes de certificats Serveur sont générées à l'aide des outils de génération de clé, disponibles dans le logiciel serveur web de l'abonné. Ainsi, généralement, les demandes de certificat Client et Email s'effectuent à l'aide du logiciel fournisseur de services cryptographiques au standard FIPS 140-1 Niveau 1, de toute manière présent dans les navigateurs les plus utilisés.

2.7 Protection et sauvegarde de la clé privée d'un abonné

L'abonné est seul responsable de la protection de ses clés privées. Les prestations proposées par la société TBS INTERNET n'impliquent en rien la génération, la protection ou la distribution desdites clés.

La société TBS INTERNET recommande fortement à ses abonnés d'utiliser un mot de passe ou un moyen d'identification équivalent, et ce pour empêcher un accès non autorisé et l'utilisation frauduleuse de la clé privée de l'abonné.

2.8 Envoi de la clé publique de l'abonné à TBS INTERNET

Les demandes de certificats Serveur sont générées à partir du logiciel de serveur Web de l'abonné. Les demandes sont soumises à TBS INTERNET sous la forme d'une demande de signature de certificat (CSR) au standard PKCS #10. La soumission de la demande se fait électroniquement via le site Internet de TBS INTERNET ou par le biais d'une AE habilitée par TBS INTERNET.

Les demandes de certificats Client et Email sont quant à elles générées à partir du logiciel fournisseur de services cryptographiques présent dans le navigateur de l'abonné. Elles sont soumises à TBS INTERNET sous la forme d'une demande de signature de certificat (CSR) au standard PKCS #10. Du fait du logiciel présent, généralement, le navigateur de l'abonné suffit à soumettre automatiquement les demandes.

2.9 Envoi du certificat émis à l'abonné

L'envoi des certificats à l'abonné concerné dépend du type de certificat :

2.9.1 Certificat Serveur

Tous les certificats serveur sont envoyés par mél à l'abonné sur l'adresse mél du contact technique indiquée lors de la demande.

2.9.2 Certificat Client d'authentification

Tous les certificats Client d'authentification sont envoyés par mél à l'abonné sur l'adresse mél du contact technique indiquée lors de la demande.

2.9.3 Certificat Email (tous types)

Dès l'émission d'un certificat Email, l'abonné reçoit par mél un lien pour récupérer son certificat. L'abonné doit alors se rendre sur le lien de récupération en utilisant le même ordinateur et la même session que celui sur lequel a été effectuée la demande de certificat.

2.10 Envoi du certificat émis à l'intention de l'abonné vers les partenaires

Les certificats serveur émis à l'abonné et dont la demande a été faite par le biais d'un partenaire distributeur ou hébergeur sont envoyés par mél au contact technique désigné par le partenaire. Le plus souvent ce contact est un employé du partenaire, mais il peut aussi être l'abonné.

2.11 Envoi d'un certificat émis à l'intention de l'abonné vers le détenteur d'un compte PKI PME

Les certificats Serveur émis à l'abonné et dont la demande a été faite par le biais d'un compte PKI PME sont envoyés par mél au contact administratif du compte concerné.

Les certificats Utilisateur émis sont envoyés conformément à la section 2.9.3 de cette DPC.

2.12 Profil des certificats TBS INTERNET

Le profil d'un certificat contient les champs ci-dessous :

2.12.1 Le champ d'extension d'utilisation des clés

Les certificats TBS INTERNET sont utilisés à des fins d'ordre général et peuvent être utilisés sans restriction aucune, quelle que soit la zone géographique ou le domaine d'application. Pour utiliser et invoquer un certificat TBS INTERNET, la partie utilisatrice doit utiliser un logiciel prenant en charge le standard X.509v3. Les certificats TBS INTERNET comprennent le champ d'extension d'utilisation de clé. Celui-ci sert à spécifier les raisons motivant l'utilisation du certificat et à limiter techniquement les fonctionnalités du certificat lorsque ce dernier est utilisé avec un logiciel prenant en charge le standard X.509v3. La confiance que peut inspirer l'utilisation de ce champ d'extension dépend de la bonne implémentation logicielle du standard X.509v3 ; critère sur lequel la société TBS INTERNET n'a aucun contrôle.

Voici ci-dessous les raisons possibles reconnues par le standard X.509v3, et pouvant être invoquées :

a) Signature numérique (*digitalSignature*) - vérification des signatures numériques pour un but autre que ceux identifiés dans les alinéas b), f) ou g), c'est-à-dire, authentification de l'entité, authentification de l'origine des données, et vérification de leur intégrité

b) Non-répudiation (*nonRepudiation*) – vérification des signatures numériques utilisées pour la fourniture d'un service de non-répudiation qui protège contre tout déni frauduleux d'une action quelconque effectuée par l'entité signataire (à l'exception d'une signature de certificat ou de liste LCR, comme dans les alinéas f) ou g) ci-dessous)

c) Chiffrement de clé (*keyEncipherment*)– chiffrement de clés ou d'autres informations de sécurité, par exemple pour pouvoir ensuite transporter la clé

d) Chiffrement de données (*dataEncipherment*) - chiffrement de données utilisateur, autres que des clés ou des informations de sécurité comme dans l'alinéa c) ci-dessus

e) Agrément de clé (*keyAgreement*) – utilisé comme clé d'agrément d'une clé publique

f) Signature de certificat de clé (*keyCertSign*) – vérification de la signature d'une AC sur un certificat, utilisé uniquement sur les certificats émis par une AC

g) Signature de liste LCR (*cRLSign*) - vérification de la signature d'une AC sur une LCR

h) Crypter seulement (*encipherOnly*) - clé d'agrément en clé publique à utiliser uniquement pour chiffrer des données avec une clé d'agrément

i) Déchiffrement seulement (*decipherOnly*) - agrément de clé pour une clé publique, utilisé exclusivement pour le déchiffrement de données lorsque la raison Agrément de clé est également utilisée

2.12.2 Le champ Caractère critique de l'extension

Le champ Caractère critique de l'extension dénote deux utilisations différentes du champ d'utilisation de clé. Si l'extension comporte l'annotation « critique », alors la clé du certificat doit être utilisée uniquement pour les utilisations mentionnées. Le fait d'utiliser cette clé pour un but autre constituerait une violation de la politique de l'émetteur. Si l'extension ne comporte pas l'annotation « critique », le champ d'utilisation de clé est simplement là pour aider le demandeur à trouver la bonne clé, selon l'application ou l'utilisation particulière souhaitée.

2.12.3 L'extension Contraintes de base

L'extension Contraintes de base indique si le sujet du certificat est habilité à agir en tant qu'AC ou uniquement en tant qu'entité finale. La confiance que peut inspirer l'utilisation de ce champ d'extension dépend de la bonne implémentation logicielle du standard X.509v3 ; critère sur lequel la société TBS INTERNET n'a aucun contrôle.

2.13 Profil de la Liste des Certificats Révoqués de TBS INTERNET

Le profil de la liste des certificats révoqués de TBS INTERNET repose sur les critères définis par le tableau ci-dessous :

Version	[Version 1]

Issuer Name (Nom de l'émetteur)	countryName (Nom du pays)=[Nom du pays émetteur du certificat racine], organisationName (Nom de l'organisation) =[Root Certificate Organisation (Organisation émettrice du certificat racine)], commonName (Nom d'usage) =[Root Certificate Common Name (Nom d'usage de l'émetteur du certificat racine)] [UTF8String encoding]	
This Update (Mise à jour actuelle)	[Date of Issuance] (Date d'émission)	
Next Update (Mise à jour suivante)	[Date of Issuance + 24 hours] (Date d'émission + 24 heures)	
Revoked Certificates (Certificats révoqués)	*CRL Entries (Entrées dans les LCR)*	
	Certificate Serial Number (Numéro de série du certificat)	[Certificate Serial Number] (Numéro de série du certificat)
	Date and Time of Revocation (Date et heure de révocation)	[Date and Time of Revocation] (Date et heure de révocation)

2.14 Politique de Certification (PC)

La politique de Certification (PC) constitue l'énoncé de la politique choisie par l'émetteur et qui correspond à l'usage prescrit d'un certificat numérique dans le contexte de délivrance dudit certificat. L'identificateur de la politique correspond à un numéro unique au sein d'un domaine spécifique, qui permet d'identifier sans ambiguïté la politique concernée, y compris la politique de certification.

Depuis août 2021 les certificats serveur contiennent soit un champ ST, soit un champ L. Le champ ST est utilisé de préférence sauf s'il n'y a pas de champ ST pour le pays (C). Ce type de profil remplace progressivement le profil avec les deux champs ST et L.

Voici, ci-dessous, les différents profils de certificats TBS INTERNET :

Certificat Serveur TBS INTERNET – SHA256, Omnidomaine SHA256

Certificat Serveur TBS INTERNET – SHA256, Omnidomaine SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA business 2
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	ST	*State (Département ou Région)*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=71:F2:0B:A9:A3:ED:CB:03:4A:0C:3C:01:3B:BE:4C:44:6D:EB:2A:F8	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Authentification Serveur (1.3.6.1.5.5.7.3.1), Authentification Client (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.1.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://cps.usertrust.com Objet Identifier (OID) = 2.23.140.1.2.2	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrust.com/TBSX509CAbusiness2.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CAbusiness2.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	
Subject Alternative Name (Nom Alternatif)	Au minimum la copie du CN du Sujet	
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256	
Thumbprint (Empreinte)		

Certificat Serveur TBS INTERNET – Test SHA256 v2

Certificat Serveur TBS INTERNET – Test SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA business 2
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	30 jours	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	ST	*State (Département ou Région)*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=71:F2:0B:A9:A3:ED:CB:03:4A:0C:3C:01:3B:BE:4C:44:6D:EB:2A:F8	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Authentification Serveur (1.3.6.1.5.5.7.3.1), Authentification Client (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.1.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://cps.usertrust.com Objet Identifier (OID) = 2.23.140.1.2.2	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrust.com/TBSX509CAbusiness2.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CAbusiness2.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	
Subject Alternative Name (Nom Alternatif)	Au minimum la copie du CN du Sujet	
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256	
Thumbprint (Empreinte)		

Certificat Serveur TBS INTERNET – Multiples-Sites SHA256

Certificat Serveur TBS INTERNET – Multiples-Sites SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA pro hosting 2
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	ST	*State (Département ou Région)*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=B8:DF:18:26:12:80:30:DD:8D:E6:28:A2:E0:B2:A2:33:6E:69:A6:52	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Authentification Serveur (1.3.6.1.5.5.7.3.1), Authentification Client (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Subject Alternative Name (autre sujet)	DNS:FQDN, [...] (liste des CN)	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.3.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://cps.usertrust.com/ Object Identifier (OID) = 2.23.140.1.2.2	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrust.com/TBSX509CAprohosting2.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CAprohosting2.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256	
Thumbprint (Empreinte)		

Certificat client TBS INTERNET – Utilisateur PKI PME (SHA256 v1)

Certificat client TBS INTERNET – Utilisateur PKI PME (SHA256)		
Signature Algorithm (de signature)	Sha2	
Issuer (Émetteur)	CN	TBS X509 CA persona 2.1
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	E	Email address (Adresse mél)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=E2:12:13:9C:CF:0C:D9:83:5C:36:4A:3D:19:D1:F2:91:B1:75:37:76	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://Cps.usertrust.com	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2-1.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2-1.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256	
Thumbprint (Empreinte)		

Certificat client TBS INTERNET – Email Professionnel SHA256

Certificat client TBS INTERNET – Email Professionnel SHA256 (après le 11 novembre 2014)		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2.1
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	E	Email address (Adresse mél)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	ST	*Département / région*
	C	*Country (Pays)*
	TelephoneNumber	*Numéro de téléphone*
	userId	*Identificateur utilisateur*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=E2:12:13:9C:CF:0C:D9:83:5C:36:4A:3D:19:D1:F2:91:B1:75:37:76	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://Cps.usertrust.com	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2-1.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2-1.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256	

Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Email Professionnel SHA256 v2017

Certificat client TBS INTERNET – Email Professionnel SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans / 4 ans / 5 ans / 6 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	E	Email address (Adresse mél)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	ST	*Département / région*
	C	*Country (Pays)*
	TelephoneNumber	*Numéro de téléphone*
	userId	*Identificateur utilisateur*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrust.com/TBSX509CApersona2.crl	
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com	

Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Email Professionnel SHA256 v2019

Certificat client TBS INTERNET – Email Professionnel SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 3 (RSA or ECC)
	O	TBS INTERNET Ltd.
	L	Douglas
	ST	Isle of Man
	C	IM
Validity (Validité)	1 an / 2 ans / 3 ans / 4 ans / 5 ans / 6 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	E	Email address (Adresse mél)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	ST	*Département / région*
	C	*Country (Pays)*
	TelephoneNumber	*Numéro de téléphone*
	userId	*Identificateur utilisateur*
Authority Key Identifier (Identificateur de clé d'autorité)	RSA: KeyID=0A:F0:98:9C:FC:23:50:84:5A:CE:0A:06:62:C7:74:98:59:67:6A:92 ECC: KeyID=3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://tbsinternet.crl.sectigo.com/TBSX509CAPersona3RSA.crl or URL=http://tbsinternet.crl.sectigo.com/TBSX509CAPersona3ECC.crl	

Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://tbsinternet.crt.sectigo.com/TBSX509CAPersona3RSA.crt or URL=http://tbsinternet.crt.sectigo.com/TBSX509CAPersona3ECC.crt [2]OCSP Full Name (Nom complet): URL=http://tbsinternet.ocsp.sectigo.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Email Professionnel Test SHA256

Certificat client TBS INTERNET – Email Professionnel Test SHA256 (après le 11 novembre 2014)		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2.1
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	30 jours	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	E	Email address (Adresse mél)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	TEST USE ONLY - NO WARRANTY ATTACHED
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	ST	*Département / région*
	C	*Country (Pays)*
	TelephoneNumber	*Numéro de téléphone*
	userId	*Identificateur utilisateur*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=E2:12:13:9C:CF:0C:D9:83:5C:36:4A:3D:19:D1:F2:91:B1:75:37:76	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	

Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2-1.crl
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2-1.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Email Novice (SHA256)

Certificat client TBS INTERNET – Email Novice (à partir du 8 septembre 2014)		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	COMODO RSA Client Authentication and Secure Email CA
	O	COMODO CA Limited
	L	Salford
	ST	Greater Manchester
	C	QB
Validity (Validité)	1 an	
Subject (Sujet)	E	Email address (Adresse mél)
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=82:AF:6C:8C:F8:C5:FE:96:61:7C:E8:1F:3D:2B:71:48:5E:C4:8B:C0	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.6449.1.2.1.3.5	
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.comodoca.com/http://crl.comodoca.com/COMODORSAClientAuthenticationandSecureEmailCA.crl	

Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.comodoca.com/COMODORSAClientAuthenticationandSecureEmailCA.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.comodoca.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Sign & Login SHA256

Certificat client TBS INTERNET – Sign & Login SHA256 (après le 11 novembre 2014)		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2.1
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*X509 Sign&Login TBS*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=E2:12:13:9C:CF:0C:D9:83:5C:36:4A:3D:19:D1:F2:91:B1:75:37:76	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://Cps.usertrust.com	

CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2-1.crl
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2-1.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Sign & Login SHA256 v2017

Certificat client TBS INTERNET – Sign & Login SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	1 an / 2 ans / 3 ans / 4 ans / 5 ans / 6 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*X509 Sign&Login TBS*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=53:79:BF:5A:AA:2B:4A:CF:54:80:E1:D8:9B:C0:9D:F2:B2:03:66:CB	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1	

CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2.crl
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Email Professionnel SHA256 v2019

Certificat client TBS INTERNET – Email Professionnel SHA256		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 3 (RSA or ECC)
	O	TBS INTERNET Ltd.
	L	Douglas
	ST	Isle of Man
	C	IM
Validity (Validité)	1 an / 2 ans / 3 ans / 4 ans / 5 ans / 6 ans	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*X509 Sign&Login TBS*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	RSA: KeyID=0A:F0:98:9C:FC:23:50:84:5A:CE:0A:06:62:C7:74:98:59:67:6A:92 ECC: KeyID=3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	
Basic Constraint (Contrainte de base)	CA = non	
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1	

CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://tbsinternet.crl.sectigo.com/TBSX509CAPersona3RSA.crl or URL=http://tbsinternet.crl.sectigo.com/TBSX509CAPersona3ECC.crl
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://tbsinternet.crt.sectigo.com/TBSX509CAPersona3RSA.crt or URL=http://tbsinternet.crt.sectigo.com/TBSX509CAPersona3ECC.crt [2]OCSP Full Name (Nom complet): URL=http://tbsinternet.ocsp.sectigo.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

Certificat client TBS INTERNET – Sign & Login Test SHA256

Certificat client TBS INTERNET – Sign & Login Test SHA256 (après le 11 novembre 2014)		
Signature Algorithm (de signature)	Sha256	
Issuer (Émetteur)	CN	TBS X509 CA persona 2.1
	OU	TBS INTERNET CA
	O	TBS INTERNET
	L	Caen
	ST	Calvados
	C	FR
Validity (Validité)	30 jours	
Subject (Sujet)	CN	Common Name (Nom d'usage)
	O	*Organisation*
	OU	*Organisation Unit (Service dans l'organisation)*
	OU	*X509 Sign&Login TBS*
	OU	*TEST USE ONLY - NO WARRANTY ATTACHED*
	OU	*ICD SIRENE si applicable à cette Organisation*
	L	*Locality (Ville)*
	S	*Street (Rue)*
	POBox	*Boite Postale*
	PostalCode	*Code Postal*
	C	*Country (Pays)*
Authority Key Identifier (Identificateur de clé d'autorité)	KeyID=E2:12:13:9C:CF:0C:D9:83:5C:36:4A:3D:19:D1:F2:91:B1:75:37:76	
Key Usage (Critical)(Utilisation de clé (Critique))	Digital Signature (Signature numérique) , Key Encipherment (Chiffrement de clé) (A0)	
Extended Key Usage (Extensions d'utilisation de clé)	Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2)	

Basic Constraint (Contrainte de base)	CA = non
Certificate Policies (Politiques de Certification)	[1]Certificate Policy (Politique de certification) : PolicyIdentifier (Identificateur de la politique) = 1.3.6.1.4.1.12983.2.6.1 [1,1]Policy Qualifier Info (Info Qualificateur de politique) : Policy Qualifier Id =CPS Qualifier (Qualificateur) : http://Cps.usertrust.com
CRL Distribution Points (Points de distribution LCR)	[1]CRL Distribution Point (Point de distribution LCR) Distribution Point Name (Nom du point de distribution) : Full Name (Nom complet): URL=http://crl.usertrustt.com/TBSX509CApersona2-1.crl
Authority Information Access (Accès à l'information sur l'autorité)	[1]Authority Info Access (Accès à l'information sur l'autorité) Access Method=Certification Authority Issuer (Méthode d'accès = certificat de l'émetteur) Alternative Name (autre nom): URL=http://crt.usertrust.com/TBSX509CApersona2-1.crt [2]OCSP Full Name (Nom complet): URL=http://ocsp.usertrust.com
Thumbprint Algorithm (Algorithme Thumbprint)	SHA256
Thumbprint (Empreinte)	

3 Organisation

La société TBS INTERNET est basée sur l'Ile de Man et opère ou fait opérer ses infrastructures en Union Européenne, au Royaume-Uni ou sur l'Ile de Man. Tous les sites concernées par l'AC sont assujettis à une politique de sécurité conçue pour, dans la limite du raisonnable, détecter, prévenir et empêcher un accès physique ou logique non autorisé aux installations afférentes. Cette partie de la DPC expose les grandes lignes de la politique de sécurité, des mécanismes de contrôle d'accès logique et physique, des niveaux de services et de la politique du personnel qui sont appliqués pour permettre que les opérations de l'AC s'effectuent en toute sécurité et en toute confiance.

3.1 Conformité vis-à-vis de la DPC

La société TBS INTERNET s'engage à respecter la présente DPC ainsi que les autres obligations contractées par le biais d'autres accords au cours de ses prestations de services.

3.2 Cessation des activités de l'AC

En cas de cessation des opérations et de l'AC pour quelque raison que ce soit, la société TBS INTERNET s'engage à fournir sans retard un préavis informant de la cessation de ses activités et à transférer ses responsabilités aux entités qui lui succèderont, à conserver ses archives et ses recours. Avant de cesser ses activités, la société TBS INTERNET prendra, dans la mesure du possible, les mesures suivantes :

- Donner aux abonnés détenant des certificats en cours de validité, un préavis de quatre-vingt-dix (90) jours les informant de son intention de cesser son activité en tant qu'AC.
- Révoquer tous les certificats non révoqués ou non expirés à la fin du préavis de quatre-vingt-dix (90) jours, sans recherche de consentement de la part de l'abonné.
- Donner en temps opportun un préavis de révocation à chacun des abonnés concernés.
- Prendre, dans la limite du raisonnable, toutes les mesures possibles afin de conserver ses archives conformément à la présente DPC.
- Se réserver le droit de prendre les dispositions de succession nécessaire à la ré-émission des certificats par une AC successeur disposant de toutes les autorisations nécessaires pour agir ainsi et qui s'engage à se conformer à toutes les règles essentielles, dans la mesure où ses opérations sont au moins aussi sécurisées que celles de la société TBS INTERNET.

Les conditions du présent article peuvent varier selon le contrat, dans la mesure où lesdites modifications affectent uniquement les parties contractantes.

3.3 Format des archives

La société TBS INTERNET ou son opérateur technique conserve ses archives au format papier ou au format électronique pendant une certaine période ; période mentionnée à la section 3.4 de la présente DPC. La société TBS INTERNET est en droit d'exiger auprès de ses abonnés de délivrer les documents susceptibles de soutenir la demande de certificat.

Avant d'être admise comme Autorité d'enregistrement, les autorités ayant soumis leur candidature devront présenter un certain nombre de documents, qui devront être validés par TBS INTERNET. Les documents à délivrer sont mentionnés, selon la situation, dans le contrat de partenariat distributeur, le contrat de partenariat hébergeur, le contrat pour titulaires d'un compte PKI PME, etc.

Dans leur rôle d'Autorité d'enregistrement de TBS INTERNET, les AE sont en droit d'exiger auprès des abonnés un certain nombre de documents susceptibles d'étayer leurs demandes de certificat. Le cas échéant, elles doivent conserver les archives correspondant auxdites demandes, conformément aux pratiques de conservation et de protection des archives employées par la société TBS INTERNET et spécifiées dans la présente DPC.

3.4 Délai de conservation des archives

La société TBS INTERNET ou son opérateur technique conserve les archives des certificats numériques qu'elle délivre, ainsi que les documents associés à ces mêmes certificats pendant une période d'au moins sept ans. La période de conservation commence à la date d'expiration ou de révocation du certificat concerné. Les exemplaires sont conservés, quel que soit le statut des certificats (expirés ou révoqués, par exemple). Les archives pourront être conservées au format papier ou au format électronique ou dans tout autre format que la société TBS INTERNET ou son opérateur technique jugera acceptable.

Ces mêmes archives sont conservées dans un lieu sécurisé hors site, et dans un format empêchant toute modification, destruction ou échange de données possibles.

3.5 Journaux des fonctions centrales

En cas de vérification, la société TBS INTERNET ou son opérateur technique conserve les journaux au format physique ou électronique, de certains évènements liés aux fonctions centrales. Les journaux sont entièrement sauvegardés sur un support amovible et ledit support conservé dans un endroit sécurisé hors site, et ce tous les jours. Ces supports ne sont manipulés que par le personnel de TBS INTERNET ou son opérateur technique en visite au centre de données. Lorsqu'ils ne se trouvent pas au centre de données, ces supports sont conservés dans un endroit sécurisé, dans un bureau verrouillé à clef sur le site de développement, ou hors site sur une installation de stockage sécurisée.
Un journal de vérification est conservé, chargé de détailler chaque mouvement du support amovible concerné. Ces journaux sont archivés par l'administrateur système toutes les semaines. Les journaux d'évènements, quant à eux, sont examinés par la direction de l'AC, eux aussi toutes les semaines. Les journaux actuellement en écriture ainsi que les journaux archivés sont conservés dans un format empêchant toute modification, destruction ou échange de données possibles. Lorsqu'il arrive en fin de vie, le support amovible est effacé par un logiciel professionnel de destruction de données entièrement sécurisé, édité par une tierce partie. Les certificats de destruction sont, eux aussi, archivés.

Les journaux comportent tous sans exception les éléments d'information suivants :

•Date et heure de saisie

•Numéro de série ou numéro consécutif de chaque saisie

•Méthode de saisie

•Source de chaque saisie

•Identité de l'entité ayant entré la saisie dans le journal

3.5.1 Administration de l'AC et du cycle de vie des certificats

•Fonctions d'administration des clés de signature d'AC racine, comprenant la génération des clés, la sauvegarde, la récupération et la destruction

•Administration du cycle de vie des certificats de l'abonné, comprenant entre autres, la gestion des demandes de certificats ayant été validées ou n'ayant pas abouti, l'émission des certificats, la ré-émission des certificats et le renouvellement des certificats

•Gestion des demandes de révocation des certificats de l'abonné, comprenant les raisons justifiant la révocation

•Gestion des changements d'affiliation de l'abonné ; changements susceptibles de remettre en cause la validité d'un certificat existant,

•Émission, création et mise à jour des listes des certificats révoqués,

•Détention des clés et des périphériques et supports de conservation des clés,

•Compromission des clés privées

3.5.2 Évènements liés à la sécurité

- Panne système, crash de logiciel et panne matériel
- Opérations effectuées par le personnel de TBS INTERNET ou son opérateur technique sur le système de l'AC : mises à jour logiciel, mises à niveau et remplacements de matériel, par exemple
- Évènements sur les modules de protection cryptographique : utilisation, désinstallation, entretien ou réparation, voire mise au rebut
- Tentatives d'accès – réussies ou avortées - à la PKI de TBS INTERNET ou son opérateur technique
- Entrées et sorties sécurisées des visiteurs de l'installation de l'AC

3.5.3 Informations liées à la demande de certificat

- Les documents et autres informations connexes présentés par le demandeur dans le cadre du processus de validation de la demande
- Lieux de stockage, qu'il soit physique ou électronique, des documents présentés

3.5.4 Délai de conservation des journaux

La société TBS INTERNET ou son opérateur technique conserve les journaux pendant une période de sept ans, ou pendant la période conforme au droit applicable.

3.6 Plans de continuité des affaires et reprise sur sinistre

Afin de garantir l'intégrité de ses prestations de services, la société TBS INTERNET ou son opérateur technique met en place, documente et teste régulièrement un certain nombre de procédures et de plans de continuité des affaires et de reprise sur sinistre. Ces plans sont révisés et mis à jour dès que nécessaire, mais au moins une fois par an.

- La société TBS INTERNET ou son opérateur technique a mis en place et fait fonctionner un système d'AC de sauvegarde entièrement opérationnel. Ce système de sauvegarde est immédiatement disponible dans l'éventualité où le système principal tombe en panne. L'ensemble du matériel informatique critique est hébergé dans des locaux en colocalisation gérés par un centre de données professionnel. Ce même matériel informatique est doublé par un matériel de secours hébergé dans les mêmes locaux. L'alimentation électrique et les fils de connexion sont, eux aussi, doublés. Le matériel de secours est prêt à prendre le relais et à fournir les prestations de l'AC. Il nous permet de garantir un temps d'indisponibilité système d'1 heure maximum (en cas de panne critique).
- La sauvegarde des logiciels critiques de l'AC est effectuée toutes les semaines, puis conservée hors site.
- La sauvegarde des informations critiques de l'activité est effectuée tous les jours, puis conservée hors site.
- Les différentes opérations de la société TBS INTERNET ou son opérateur technique sont réparties entre plusieurs sites. Les sites disposent tous d'installations capables de gérer le cycle de vie des certificats, à savoir pour les opérations suivantes entre autres mais non limitées à celles-ci, les demandes, les émissions, les révocations et les renouvellements desdits certificats.

En plus d'un système d'AC de secours entièrement opérationnel, la société TBS INTERNET ou son opérateur technique dispose également d'installations dédiées à l'activation d'un système d'AC de secours, ainsi que d'un deuxième site situé à une distance raisonnable du premier, au cas où le site principal devait souffrir d'une perte totale de ses systèmes opérationnels. Le présent plan de reprise de l'exploitation normale sur sinistre énonce l'obligation pour la société TBS INTERNET ou son opérateur technique de faire tout son possible pour minimiser les interruptions de ses prestations en tant qu'AC.

3.7 Disponibilité des données de révocation

La société TBS INTERNET publie les listes des certificats révoqués (LCR) pour permettre aux parties utilisatrices de vérifier la signature numérique issue d'un certificat numérique émis par elle. Chaque LCR contient un certain nombre de données saisies correspondant à tous les certificats révoqués mais non expirés. Cette LCR est valable 24 heures. La société TBS INTERNET émet une nouvelle LCR toutes les 24 heures, comprenant un numéro consécutif croissant délivré pour chaque LCR émise. Dans certaines circonstances, la société TBS INTERNET pourra publier de nouvelles LCR avant l'expiration de la LCR actuelle. Toutes les LCR sont archivées (conformément aux instructions de la section 3.4 de la présente DPC) pendant 7 ans, voire plus longtemps si nécessaire.

Depuis le 7 novembre 2008 la société TBS INTERNET prend en charge le protocole de vérification en ligne du statut des certificats OCSP (Online Certificate Status Protocol) via le service http://ocsp.tbs-x509.com

3.8 Publication des informations cruciales

La société TBS INTERNET publie la présente DPC, les modalités d'utilisation des certificats, le contrat des parties utilisatrices et les exemplaires de l'ensemble des contrats de partenariat dans le répertoire officiel de la société à l'adresse http://www.tbs-internet.com/CA/repository. C'est à l'Autorité en charge de la politique de certification de TBS INTERNET que revient la responsabilité de maintenir à jour le répertoire de la société TBS INTERNET. Toutes les mises à jour, modifications et présentations d'ordre juridique sont conservées conformément aux procédures d'archivage énumérées dans la section 3.5 de la présente DPC.

3.9 Informations confidentielles

La société TBS INTERNET observe les règles du droit applicable sur la protection des données personnelles ; données considérées comme confidentielles.

3.9.1 Types d'informations considérés comme confidentiels

La société TBS INTERNET considère comme confidentiels les types d'information suivants et s'engage à prendre toutes les mesures raisonnables en son pouvoir pour empêcher la divulgation desdites informations à des personnes non autorisées.

- Contrat d'abonnement
- Archives des demandes de certificats et documents soumis en vue d'étayer les demandes de certificats, que celles-ci aient été validées ou non
- Archives des transactions et archives des audits financiers
- Rapport et archive de suivi des audits externes ou internes, à l'exception des rapports d'audit de WebTrust qui sont susceptibles d'être publiés à la discrétion de la société TBS INTERNET.
- Plans de continuité des affaires et plans de reprise de l'exploitation normale après sinistre.
- Archives et suivis internes des opérations de l'infrastructure de TBS INTERNET, de la gestion des certificats et des données et prestations d'inscription.

3.9.2 Types d'information non considérés comme confidentiels

Les abonnés sont informés du fait que les données de révocation de tous les certificats émis par l'AC TBS INTERNET sont des informations publiques publiables toutes les 24 heures. Les données concernant toute demande de certificat de la part d'un abonné, estampillées de la marque PUBLIC conformément au contrat d'abonnement concerné et soumises dans le cadre de ladite demande de certificat sont publiées au sein même dudit certificat numérique, conformément aux instructions de la section 2.12.4 de la présente DPC.

3.9.3 Accès aux informations confidentielles

Les employés occupant des postes de confiance dans la société gèrent l'ensemble des informations en toute confidentialité. Les employés de l'AE/LRA, tout particulièrement, devront se conformer aux exigences du droit anglais sur la protection des données personnelles.

3.9.4 Divulgation des informations confidentielles

La société TBS INTERNET n'est, en aucun cas, assujettie à la divulgation des informations confidentielles qu'elle détient, quelles qu'elles soient, sauf mention contraire de la loi, et sans une demande raisonnablement justifiée et authentifiée par une partie habilitée à agir ainsi, et spécifiant :

- La partie pour laquelle la société TBS INTERNET se doit de garder des informations confidentielles
- La partie demandant lesdites informations confidentielles
- Une injonction d'un tribunal le cas échéant

3.10 Pratiques et gestion du personnel

En accord avec la présente DPC, la société TBS INTERNET s'engage à respecter les pratiques d'administration et de gestion du personnel ; pratiques garantissant raisonnablement la loyauté et la compétence de ses employés, ainsi que l'exécution satisfaisante des obligations desdits employés.

3.10.1 Rôles de confiance

Le terme « rôles de confiance » fait référence à l'accès, par les employés, au système de gestion des comptes de la société TBS INTERNET, comprenant les autorisations d'utilisation fonctionnelle distribuées à titre personnel. Il revient aux membres de l'équipe administrative de décider des autorisations ; les autorisations signées par eux étant archivées.

Le personnel de confiance doit s'identifier et s'authentifier auprès du système avant qu'un accès quel qu'il soit, puisse être autorisé. L'identification se fait par le biais d'un nom d'utilisateur tandis que l'authentification nécessite la saisie d'un mot de passe et la présence d'un certificat numérique.

3.10.2 Contrôles en matière de personnel

L'ensemble du personnel de confiance est soumis à une vérification d'antécédent, et ce avant que l'accès au système de la société TBS INTERNET ne soit accordé. La formation du personnel s'effectue via une relation mentorale impliquant les cadres supérieurs de l'équipe à laquelle ce personnel est rattaché.

3.11 Publication des informations

Les services de certification ainsi que le répertoire de la société TBS INTERNET sont accessibles de plusieurs manières différentes :

•Sur Internet : www.tbs-internet.com

•Par courriel à l'adresse legal@tbs-internet.com

4 Pratiques et procédures

Cette section est consacrée au processus de demande de certificat, et aux informations requises pour réussir et étayer la demande.

4.1 Conditions nécessaires à la demande de certificat

Les demandeurs de certificat doivent tous sans exception compléter le processus d'inscription, à savoir :

- Générer une paire de clés au format RSA ou ECC et apporter la preuve à la société TBS INTERNET de la propriété de la moitié clé privée de la paire de clés, et ce en délivrant une demande de signature de certificat (CSR) valide au standard PKCS#10,
- Faire, dans la mesure du raisonnable, tout leur possible pour protéger l'intégrité de la moitié clé privée de la paire de clés,
- Soumettre à la société TBS INTERNET une demande de certificat comprenant les informations de demande spécifiées dans la présente DPC, la moitié clé publique d'une paire de clés, et accepter les conditions du contrat d'abonnement qui les concerne,
- Fournir la preuve de leur identité via la soumission des documents officiels exigés par la société TBS INTERNET lors du processus d'inscription.

Les demandes de certificats sont soumises soit directement à la société TBS INTERNET, soit à l'une des AE habilitées par la société. Le tableau suivant renseigne sur la ou les entités impliquées dans le processus de demande de certificat. La société TBS INTERNET émet tous les certificats quels qu'ils soient, quelle que soit l'entité chargée du traitement de la demande.

Type de certificat	**Entité sujette à l'inscription**	**Entité chargée du traitement**	**Autorité délivrant le certificat**
Certificat Serveur *conformément à la section 2.4.1 de la présente DPC*	Entité finale : abonné	TBS INTERNET ou AE	TBS INTERNET
Certificat Serveur *conformément à la section 2.4.1 de la présente DPC*	Partenaire pour le compte de l'entité finale, l'abonné	TBS INTERNET ou AE	TBS INTERNET
Certificat Client Email *conformément à la section 2.4.2 de la présente DPC*	Entité finale : abonné	TBS INTERNET ou AE	TBS INTERNET
Certificat Client Email *conformément à la section 2.4.2 de la présente DPC*	Partenaire pour le compte de l'entité finale, l'abonné	TBS INTERNET ou AE	TBS INTERNET
Certificat Utilisateur PKI PME *conformément à la section 2.4.2 de la présente DPC*	Entité finale : abonné	Titulaires d'un compte PKI PME	TBS INTERNET

Certificat Client Auth *conformément à la section 2.4.3 de la présente DPC*	Entité finale : abonné	TBS INTERNET ou AE	TBS INTERNET
Certificat Client Auth *conformément à la section 2.4.3 de la présente DPC*	Partenaire pour le compte de l'entité finale, l'abonné	TBS INTERNET ou AE	TBS INTERNET

4.1.1 Demandes de certificats de la part d'un partenaire hébergeur

Les partenaires hébergeurs sont habilités à exercer les fonctions d'une AE conformément aux pratiques et aux politiques spécifiées dans la présente DPC. L'AE pourra ainsi faire suivre la demande pour le compte du demandeur conformément au programme de partenariat.

Le cas échéant, l'AE est responsable de toutes les opérations effectuées pour le compte du demandeur, détaillées dans la section 4.1 de la présente DPC. Les responsabilités du partenaire hébergeur sont décrites dans les directives et le contrat de distribution pour hébergeur.

4.1.2 Demandes de certificat de la part du titulaire d'un compte PKI PME

Le titulaire d'un compte PKI PME exerce les fonctions d'AE conformément aux pratiques et aux politiques spécifiées dans la présente DPC. L'AE fait la demande de certificat Serveur pour un serveur donné, ou un certificat Utilisateur pour un employé donné sous un nom de domaine validé par la société TBS INTERNET, et qui appartient ou peut légalement être utilisé par l'organisation détentrice du compte PKI PME.

4.1.3 Moyens utilisés pour faire la demande

De manière générale, les demandeurs devront compléter les formulaires en ligne mis à disposition par la société TBS INTERNET ou par les AE sur les sites Internet officiels concernés. Les partenaires hébergeurs peuvent utiliser une API pour déposer les demandes.

Les demandes des titulaires de compte PKI PME s'effectuent par le biais de la console d'administration MMC du compte EPKI, une console Internet hébergée et maintenue par l'opérateur Sectigo.

4.2 Validation des demandes

Avant d'émettre un certificat, la société TBS INTERNET effectue un certain nombre de contrôles destinés à valider l'authenticité des informations saisies par l'abonné durant la demande de certificat. Les différents contrôles, détaillés ci-dessous, dépendent du type de produit :

4.2.1 Processus de validation en trois étapes

Ce processus en trois étapes sous-entend la révision manuelle par la société TBS INTERNET, des informations saisies par le demandeur durant la demande (conformément à la section 4.3 de la présente DPC), et ce afin de vérifier que :

1. Le demandeur est une personne morale capable de répondre de ses actes, qu'elle soit une organisation ou un individu.

    •Validée par la production des documents officiels de la société, comme l'extrait de registre du commerce, les statuts de la société, une licence de commercialisation ou tout autre document

pertinent.
•Pour les demandes émises par les entités sans personnalité morale, production des documents tels qu'une copie de pièce d'identité associée à une facture d'électricité ou un chèque bancaire original annulé, ou encore tout autre document pertinent.

2. Le contact administratif désigné par le demandeur confirme verbalement ou devant un officier de justice, un expert comptable (enregistré à l'ordre des experts comptables) ou un commissaire au compte (enregistré à l'ordre des commissaires au compte) la demande de certificat et ses caractéristiques (CN ou nom de domaine, nom de l'organisation). Ce contact est soit une personne physique employée par le demandeur, soit membre de son équipe dirigeante, soit si le demandeur est un individu, l'individu lui même ou son tuteur.
•La validation peut être réalisée verbalement en joignant le contact administratif par le biais d'un numéro de téléphone fournit par un service d'annuaire tiers. Un message peut lui être laissé afin qu'il retourne l'appel.
•La validation peut être réalisée verbalement en joignant le contact administratif par le biais d'un numéro de téléphone obtenu sur un contrat, une facture, ou autre document adéquat émanant d'un opérateur téléphonique, un bailleur, ou d'un titre de propriété du nom de domaine si celui-ci est pleinement qualifié. Un message peut lui être laissé afin qu'il retourne l'appel.
•La validation peut être réalisée par l'envoi d'un courrier physique par un transporteur postal ou privé contenant un code aléatoire retourné par le contact administratif.
•La validation peut être réalisée devant un officier de justice, un expert comptable (enregistré à l'ordre des experts comptables) ou un commissaire au compte (enregistré à l'ordre des commissaires au compte). Dans ce cas un document confirmant les éléments essentiels du certificat est signé devant lui par le demandeur, représenté par le contact administratif.
•Lorsque le contact administratif a déjà validé une demande de certificat soit verbalement soit par écrit pour la même personne morale demandeuse dans les trois derniers mois, et que le contact est temporairement injoignable, l'étape peut être validée en envoyant un mél le notifiant de cette validation par défaut. Ce mél l'informe de la validation et lui donne la démarche à suivre pour répudier le certificat si nécessaire.
•Lorsque le contact administratif a déjà validé une demande de certificat soit verbalement soit par écrit pour la même personne morale demandeuse dans les douze derniers mois, et que le contact est temporairement injoignable, l'étape peut être validée en envoyant un mél contenant un code aléatoire qu'il devra retourner sur l'interface web pour confirmer son accord.

3. L'exploitant technique du nom domaine confirme la légitimité de la demande en validant un challenge DCV. La validation s'effectue au moyen d'un challenge DCV Email, DCV HTTP ou HTTPS, ou DCV DNS. Le processus est automatisé et est géré par un robot opéré par la PKI qui peut alors délivrer le certificat.

Les revendications susmentionnées sont vérifiées soit par le biais d'un examen des documents étayant la demande, soit d'une recherche auprès des bases de données officielles tierces, ou d'une combinaison de ces choix.

4.2.2 Processus de validation en deux étapes

Ce processus en deux étapes sous-entend la révision, automatique ou manuelle, par la société TBS INTERNET, des informations saisies par le demandeur durant la demande (conformément à la section 4.3 de la présente DPC), et ce afin de vérifier que :

1. Le demandeur est une personne morale capable de répondre de ses actes, qu'elle soit une organisation ou un individu.

•Validée par la production des documents officiels de la société, comme l'extrait de registre du commerce, les statuts de la société, une licence de commercialisation ou tout autre document pertinent.
•Pour les demandes émises par les entités sans personnalité morale, production des documents tels qu'un relevé de compte, une copie du passeport, une copie du permis de conduire ou tout autre document pertinent.

2. L'exploitant technique du nom domaine confirme la légitimité de la demande en validant un challenge DCV. La validation s'effectue au moyen d'un challenge DCV Email, DCV HTTP ou HTTPS, ou DCV DNS. Le processus est automatisé et est géré par un robot opéré par la PKI qui peut alors délivrer le certificat.

Les revendications susmentionnées sont vérifiées soit par le biais d'un processus automatique, soit d'un examen des documents étayant la demande, soit d'une recherche auprès des bases de données officielles tierces, ou d'une combinaison de ces choix.

4.2.3 Certificats de type Test

TBS INTERNET traite ces demandes de certificat à l'aide de sa base de données de sociétés. Si les informations saisies lors de la demande correspondent aux archives contenues dans la base de données, l'émission du certificat peut être semi-automatique, après une simple relecture humaine pour vérifier l'adéquation entre la demande et la base de données.

Si les informations saisies lors de la demande ne correspondent pas aux archives, TBS INTERNET suit le processus de validation en deux étapes mentionné dans la section 4.2.2 de la présente DPC.

La société TBS INTERNET a mis en place dans le cadre de ses comptes Partenaires d'un système de profilage des demandes de certificats. Ces profils sont mis en place après un processus de validation en quatre étapes mentionné dans la section 4.2.1 de la présente DPC. Ces profils sont ensuite utilisés comme des filtres lors de la réception de commandes via l'Espace Client, qui nécessite une authentification personnelle.

Si la demande émane d'un utilisateur dûment authentifié dans un compte Partenaire et que ce compte dispose d'un filtre qui correspond au profil du certificat demandé, le certificat peut être commandé automatiquement.

La validation de ce type de certificats peut dans certains cas être déléguée à la société Sectigo. Elle applique dans ce cas une authentification décrite dans la section 4.2.2 de sa CPS version 2.4

Les champs contenant des informations validées sont CN, O, L, S, C.

4.2.4 Certificats Standard, Ecommerce, Premium, Omnidomaine

Les certificats Standard, Ecommerce, Premium, et Omnidomaine sont traités manuellement par un membre du service de validation de la société TBS INTERNET, conformément au processus de validation en quatre étapes mentionné dans la section 4.2.1 de la présente DPC. TBS INTERNET pourra utiliser sa base de données pour compléter le processus de validation.

Les demandes de certificats émanant d'un utilisateur dûment authentifié dans un compte Partenaire et dont le profil du certificat correspond à un filtre existant peuvent être émis automatiquement.

La validation de ce type de certificats peut dans certains cas être délégué à la société Sectigo. Elle applique dans cas une authentification décrite dans la section 4.2.3 de sa CPS version 2.4

Les champs contenant des informations validées sont CN, O, L, S, C.

4.2.5 Certificat Email Novice

Le certificat Email Novice n'est pas validé *(persona non-validated).* La société TBS INTERNET valide uniquement le droit du demandeur à utiliser l'adresse mél soumise. Cette procédure s'effectue via la délivrance par courriel d'un challenge permettant au seul demandeur de confirmer son adresse mél.

Ce certificat ne bénéficie d'aucune garantie.

Le champ contenant une information validée est E.

4.2.6 Certificat Utilisateur : version PKI PME

Les versions PKI PME des certificats X509 Utilisateur TBS ne sont disponibles que par le biais d'un compte PKI PME. Elles sont émises uniquement à l'intention des adresses mél associées à des noms de domaine approuvés. Le titulaire du compte PKI PME doit d'abord soumettre un nom de domaine à la société TBS INTERNET ainsi que la preuve de propriété dudit nom de domaine, ou du droit à utiliser celui-ci. La validation a alors eu lieu conformément aux spécifications de la section 4.2.1 de la présente DPC. Après validation du nom de domaine, la société TBS INTERNET est en mesure d'autoriser le titulaire du compte PKI PME à utiliser les adresses mél associées au nom de domaine.

C'est à l'administrateur attitré du compte PKI PME qu'il revient d'effectuer les demandes de certificats Utilisateur. L'administrateur soumet les informations concernant l'entité finale utilisatrice du certificat Utilisateur, pour le compte de ladite entité finale. Un courriel est alors envoyé à cette dernière ; courriel contenant les informations de connexion uniques permettant à l'entité de se connecter à l'infrastructure de génération et de distribution des certificats opérée par la société Sectigo pour TBS INTERNET.

Dès que l'entité finale se connecte à l'infrastructure, son navigateur crée une clé publique et une clé privée. La clé publique est délivrée à la société TBS INTERNET, qui émet alors un certificat Utilisateur en version PKI PME contenant la clé publique.

Les champs contenant des informations validées sont CN, E, O, L, S, C.

4.2.7 Certificats Multi-Sites

Les certificats Multi-Sites sont traités manuellement par un membre du service de validation de la société TBS INTERNET, conformément au processus de validation en quatre étapes mentionné dans la section 4.2.1 de la présente DPC. TBS INTERNET pourra utiliser sa base de données pour compléter le processus de validation.

Du fait que les certificats Multi-Sites et Multi-Sites SHA256 contiennent une liste de noms additionnels (champs SAN) en plus d'un nom usuel principal (champ CN), tous les éléments doivent être validés avec un mécanisme DCV (Domain Control Validation) qui assure que le Demandeur a bien le contrôle technique du domaine.

Les champs contenant des informations validées sont CN, O, L, S, C.

4.2.8 Certificats Sign & Login

Les certificats Sign & Login sont traités manuellement par un membre du service de validation de la société TBS INTERNET, conformément au processus mentionné dans la section 4.2.1 de la présente DPC. TBS INTERNET pourra utiliser sa base de données pour compléter le processus de validation.

La spécificité de ces certificats est que le nom usuel n'est pas un nom de domaine. De ce fait au lieu de vérifier le droit d'usage du nom de domaine, TBS INTERNET vérifie que le nom usuel (CN) n'est pas un nom de domaine.

Les demandes de certificats émanant d'un utilisateur dûment authentifié dans un compte Partenaire et dont le profil du certificat correspond à un filtre existant peuvent être émis automatiquement.

Les champs contenant des informations validées sont CN, O, L, S, C.

4.2.9 Certificats Test Sign & Login

TBS INTERNET traite ces demandes de certificat à l'aide de sa base de données de sociétés. Si les informations saisies lors de la demande correspondent aux archives contenues dans la base de données, l'émission du certificat peut être semi-automatique, après une simple relecture humaine pour vérifier l'adéquation entre la demande et la base de données.

Si les informations saisies lors de la demande ne correspondent pas aux archives, TBS INTERNET suit le

processus de validation mentionné dans la section 4.2.2 de la présente DPC. TBS INTERNET vérifie que le nom usuel (CN) n'est pas un nom de domaine.

Les demandes de certificats émanant d'un utilisateur dûment authentifié dans un compte Partenaire et dont le profil du certificat correspond à un filtre existant peuvent être émis automatiquement.

Les champs contenant des informations validées sont CN, O, L, S, C.

4.2.10 Certificats Email Professionnel

Les certificats Email Professionnel sont traités manuellement par un membre du service de validation de la société TBS INTERNET, conformément au processus de validation en trois étapes mentionné dans la section 4.2.1 de la présente DPC. TBS INTERNET pourra utiliser sa base de données pour compléter le processus de validation.

Les demandes de certificats émanant d'un utilisateur dûment authentifié dans un compte Partenaire et dont le profil du certificat correspond à un filtre existant peuvent être émis automatiquement.

La spécificité de ces certificats est que le nom usuel n'est pas un nom de domaine mais un nom de service ou de personne physique. Dans ce dernier cas, au lieu de vérifier le droit d'usage du nom de domaine, TBS INTERNET vérifie la personne physique qui doit aussi être le contact administratif. Pour se faire, une copie de pièce d'identité est nécessaire.

Le système de TBS INTERNET émet systématiquement un mél à l'adresse à certifier. Il contient un challenge permettant au seul demandeur de confirmer son adresse mél. Cette confirmation est un pré-requis pour l'émission du certificat.

Les champs contenant des informations validées sont CN, E, O, L, S, C.

4.2.11 Certificats Email Particulier

Les certificats Email Particulier sont traités manuellement par un membre du service de validation de la société TBS INTERNET, conformément au processus de validation en trois étapes mentionné dans la section 4.2.1 de la présente DPC. TBS INTERNET pourra utiliser sa base de données pour compléter le processus de validation.

Les demandes de certificats émanant d'un utilisateur dûment authentifié dans un compte Partenaire et dont le profil du certificat correspond à un filtre existant peuvent être émis automatiquement.

Ce certificat ne dispose pas de champ Organisation puisque ce produit est destiné aux personnes physiques dans un cadre privé. La vérification porte alors sur l'identité de la personne grâce à une copie de pièce d'identité et une facture d'électricité. De plus, si la personne physique n'est pas répertoriée à l'annuaire, un chèque de banque original annulé est requis. D'autres documents peuvent être demandés afin de vérifier la demande de certificat.

Le système de TBS INTERNET émet systématiquement un mél à l'adresse à certifier. Il contient un challenge permettant au seul demandeur de confirmer son adresse mél. Cette confirmation est un pré-requis pour l'émission du certificat.

Les champs contenant des informations validées sont CN, E, O, L, S, C.

4.3 Informations de validation utilisées lors de la demande d'un certificat

Les demandes de certificats sont étayées par la production des documents nécessaires à l'établissement de l'identité du demandeur.

De temps en temps, la société TBS INTERNET se réserve le droit de modifier les conditions relatives aux informations saisies par les demandeurs, et ce pour satisfaire les exigences fixées par elle, pour répondre au nouveau contexte commercial inhérent à l'utilisation d'un certificat numérique, et pour se conformer au droit applicable.

4.3.1 Informations saisies pour les demandes issues par les organisations

Pour qu'un certificat TBS INTERNET puisse être émis à l'intention d'une organisation, la société TBS INTERNET a besoin des éléments d'information décisifs suivants. Les éléments estampillés de la marque PUBLIC sont présents sur le certificat et sont par conséquent dans le domaine public. Les éléments non estampillés restent confidentiels, conformément aux articles sur la protection de la vie privée inscrits dans la présente DPC.

- Nom légal de l'organisation (PUBLIC)
- Service ou département au sein de l'organisation (PUBLIC)
- Rue, ville, code postal, pays (PUBLIC)
- Numéro de TVA (le cas échéant)
- Numéro DUNS / Société (le cas échéant)
- Identification du logiciel serveur
- Informations de paiement
- Nom complet, fonction, adresse mél et téléphone du contact administratif
- Nom complet, fonction, adresse mél et téléphone du contact technique
- Représentant de l'organisation et contacts de facturation
- Nom usuel : Nom de domaine complet / Nom du serveur réseau / IP publique / Nom de service / Nom de personne / Référence de nommage (PUBLIC)
- Clé publique (PUBLIC)
- Preuve du droit à l'utilisation du nom
- Preuve de l'existence et du statut juridique de l'organisation
- Preuve de l'attribution d'un numéro de téléphone
- Contrat d'abonnement, signé (en cas de demande par des moyens autres que les moyens traditionnels)

4.3.2 Documents étayant les demandes issues par les organisations

Les documents nécessaires à une demande de certificat de la part d'une organisation sont les suivants, à délivrer partiellement ou en totalité :

- Enregistrement au registre du commerce
- Statuts de la société

- Patente
- Certificat de conformité
- Charte de la société
- Certificat de l'autorité compétente, autorisant l'organisation à effectuer des opérations commerciales
- Certificat d'immatriculation à la TVA
- Charte d'une société par actions
- Document officiel éventuel émis par le représentant habilité d'une organisation gouvernementale
- Courrier officiel émis par le bureau du doyen ou du directeur de l'établissement (pour les établissements rattachés l'éducation nationale)

La société TBS INTERNET pourra, à sa seule discrétion, accepter d'autres documents officiels émis par l'organisation, et susceptibles d'étayer une demande.

4.3.3 Informations saisies pour les demandes issues par un individu

Pour qu'un certificat TBS INTERNET puisse être émis à l'intention d'un individu, la société TBS INTERNET a besoin des éléments d'information décisifs suivants :

- Nom légal de l'individu (PUBLIC)
- Service ou département au sein de l'organisation (PUBLIC)
- Rue, ville, code postal, pays (PUBLIC)
- Numéro de TVA (le cas échéant)
- Identification du logiciel serveur
- Informations de paiement
- Nom complet, fonction, adresse mél et téléphone du contact administratif
- Nom complet, fonction, adresse mél et téléphone du contact technique
- Représentant de l'organisation et contacts de facturation
- Nom usuel : Nom de domaine complet / Nom du serveur réseau / IP publique ou privée / Nom de service / Nom de personne / Référence de nommage (PUBLIC)
- Clé publique (PUBLIC)
- Preuve du droit à l'utilisation du nom
- Preuve de l'attribution d'un numéro de téléphone

- Contrat d'abonnement, signé (en cas de demande par des moyens autres que les moyens traditionnels)

4.3.4 Documents étayant les demandes issues par les individus

Les documents nécessaires à une demande de certificat de la part d'un individu comprennent les éléments d'identification suivants :

- Carte Nationale d'Identité
- Passeport
- Permis de conduire
- Chèque de banque annulé
- Facture d'électricité
- Document d'imposition fiscale

La société TBS INTERNET pourra accepter, à sa seule discrétion, d'autres documents officiels susceptibles d'étayer la demande.

4.4 Conditions de validation des demandes de certificat

À réception d'une demande de certificat numérique et sur la base des informations soumises, la société TBS INTERNET est en mesure de confirmer les informations suivantes :

- Le demandeur de certificat est la même personne que la personne identifiée dans la demande de certificat.
- Le demandeur détient la clé privée associée à la clé publique à inclure dans le certificat.
- Les informations devant être publiées dans le certificat sont véridiques, à l'exception jusqu'à présent des informations concernant l'abonné qui n'ont pas encore été vérifiées.
- Tout agent au représentant faisant la demande d'un certificat comportant la clé publique d'un demandeur est habilité à faire cette demande.

Pour tous les types de certificats TBS INTERNET, l'abonné a pour obligation à tout moment de contrôler la véracité des informations soumises et de notifier la société TBS INTERNET de tout changement susceptible d'affecter la validité du certificat. En cas de non-respect des obligations exposées dans le contrat d'abonnement, le certificat numérique de l'abonné sera révoqué sans avis préalable à l'abonné. Ce dernier devra payer tous les frais dûs non encore payés dans le cadre du contrat.

4.4.1 Confirmation via un tiers des informations concernant une entité professionnelle

La société TBS INTERNET est susceptible d'utiliser les services d'une tierce partie aux fins de se faire confirmer les informations concernant une entité professionnelle demandant un certificat numérique. La société TBS INTERNET se réserve le droit d'accepter les confirmations issues d'organisations tierces, d'autres bases de données tierces et d'entités gouvernementales.

Parmi les différentes vérifications entreprises, la société TBS INTERNET pourra également examiner les transcriptions des registres de commerce ; transcriptions confirmant l'immatriculation de la société demandeur et citant les membres du conseil d'administration de ladite société, les membres de la direction et les directeurs représentant cette même société.

La société TBS INTERNET est susceptible d'utiliser tout moyen de communication mis à sa disposition pour établir l'identité du demandeur d'une organisation ou d'un individu demandeur. La société TBS INTERNET se réserve le droit de refuser toute demande, à sa seule discrétion.

4.4.2 Affectation d'un numéro de série

La société TBS INTERNET affecte des numéros de série aux certificats qui apparaissent sur ceux-ci. Les numéros de série sont exclusifs à chaque certificat.

4.5 Délai nécessaire pour confirmer les données soumises

La société TBS INTERNET s'engage à prendre toutes les mesures raisonnables pour confirmer les informations saisies lors des demandes de certificat, et émettre le certificat numérique dans un délai raisonnable.

Elle s'engage à ce que tous les certificats soient émis dans les deux jours ouvrés après réception de toutes les informations de validation requises définies dans la présente DPC.

4.6 Approbation et rejet des demandes de certificat

Après que toutes les validations requises et nécessaires par la demande aient été complétées, la société TBS INTERNET est en mesure d'approuver la demande de certificat numérique.

Lorsque la validation d'une demande n'aboutit pas, la société TBS INTERNET rejette celle-ci. TBS INTERNET se réserve le droit de rejeter les demandes d'émission de certificat de certains demandeurs si, de son propre jugement, elle considère que, en émettant un certificat à l'intention des parties concernées, le nom et la réputation de confiance de la société TBS INTERNET sont susceptibles d'être entachés, ternis ou sa valeur amoindrie. Le cas échéant, la société TBS INTERNET se réserve le droit d'agir ainsi sans obligations vis-à-vis des conséquences préjudiciables de perte ou de frais occasionnés par son rejet de la demande.

Les demandeurs dont les demandes ont été rejetées pourront faire une autre demande ultérieurement.

4.7 Émission d'un certificat et consentement de l'abonné

La société TBS INTERNET émet un certificat après approbation de la demande dudit certificat. Le certificat numérique est considéré comme valable à partir du moment où l'abonné l'accepte (cf section 4.9 de la présente DPC). Le fait que la société TBS INTERNET émette un certificat numérique implique l'acceptation par elle de la demande de certificat.

4.8 Validité du certificat

Les certificats sont valables dès l'émission de ceux-ci par la société TBS INTERNET et leur acceptation par l'abonné. De manière générale, la période de validité d'un certificat serveur est de 1 an. La période de validité d'un certificat client peut aller de 1 à 6 ans. Cependant, la société TBS INTERNET se réserve le droit de proroger ces périodes de validité au-delà de la période standard.

4.9 Acceptation d'un certificat par l'abonné

Le certificat émis est soit envoyé par mél, soit installé sur l'ordinateur/module de sécurité de l'abonné via une méthode de distribution en ligne. On considère qu'un abonné accepte un certificat dès lors que :

- L'abonné utilise le certificat.
- Il s'est écoulé une période de 30 jours depuis la date d'émission du certificat.

4.10 Vérification des signatures numériques

La vérification d'une signature numérique sert à vérifier que :

- La clé privée correspondant à la clé publique listée dans le certificat est bien celle qui a créé la signature numérique.
- Les données signées associées à cette signature numérique n'ont pas été modifiées depuis que la signature numérique a été créée.

4.11 Confiance vis-à-vis d'une signature numérique

La décision finale d'accepter ou de refuser la confiance accordée à une signature numérique vérifiée revient exclusivement à la partie utilisatrice. Une signature numérique ne doit inspirer confiance que si :

- Ladite signature numérique a été créée durant la période de validité du certificat. Elle peut être vérifiée par rapport au certificat qui a été validé.
- La partie utilisatrice a vérifié le statut de révocation du certificat en consultant les listes de certificats révoqués concernées par ledit certificat ou en vérifiant le statut en ligne via OCSP, et confirmation a été faite que le certificat n'a pas été révoqué.
- La partie utilisatrice reconnaît qu'un certificat numérique est émis à l'intention d'un abonné dans un objectif précis ; que la clé privée associée au certificat numérique peut être utilisée uniquement dans le cadre des utilisations suggérées par la présente DPC et définies sous l'appellation d'identificateurs d'objet (Object Identifiers) dans le profil du certificat.

Cette confiance vis-à-vis de la signature numérique est raisonnablement acceptée dans la limite des articles de la présente DPC concernant la partie utilisatrice et dans le contrat de la partie utilisatrice. Si les circonstances de cette confiance nécessitent un dépassement des garanties actuellement délivrées par la société TBS INTERNET dans le cadre des articles de la présente DPC, la partie utilisatrice doit obtenir ces garanties supplémentaires.

Les garanties ne sont valables que si les étapes susmentionnées ont été suivies.

4.12 Suspension d'un certificat

La société TBS INTERNET ne prévoit pas la suspension des certificats.

4.13 Révocation d'un certificat

La révocation d'un certificat a pour but de terminer de manière permanente la période opérationnelle d'un certificat, et ce avant que celui-ci n'atteigne la fin normale de sa période de validité. La société TBS INTERNET révoquera un certificat numérique lorsque :

•Il y a eu perte, vol, modification, divulgation non autorisée ou risque compromettant la sécurité de la clé privée associée au certificat.
•L'abonné ou la société TBS INTERNET ont failli à l'une des obligations matérielles définies par la présente DPC.

•Les obligations définies par la présente DPC de l'abonné ou de la société TBS INTERNET n'ont pas été respectées en temps voulu ou ont été empêchées suite à une catastrophe naturelle, à une panne de communication ou à une panne informatique, ou pour toute autre cause raisonnablement indépendante de la volonté de la personne fautive. En conséquence, on considère que les informations d'une tierce partie sont matériellement menacées ou compromises.

•Il y a eu modification des informations concernant l'abonné contenues dans le certificat.

•Les informations fournies par l'abonné pour obtenir le certificat sont partiellement ou totalement erronées.

4.13.1 Demande de révocation

L'abonné ainsi que toute autre partie habilitée dans cette affaire (AE, par exemple) peuvent demander la révocation d'un certificat. Avant celle-ci, la société TBS INTERNET vérifiera que la demande de révocation a été :

- Faite par l'organisation ou l'entité individuelle ayant fait la demande de certificat,
- Faite par l'AE pour le compte de l'organisation ou de l'entité individuelle utilisant l'AE pour effectuer une demande de certificat.

Pour authentifier une demande de révocation, la société TBS INTERNET suit la procédure suivante :

✔ La demande de révocation peut être faite par le biais de la page statut du certificat. Un système de challenge s'assure de la confirmation d'un des deux contacts nommés lors de la demande de certificat. Lorsque la demande est confirmée, le certificat est automatiquement révoqué.

✔ Hors de ce processus automatique, une demande de révocation peut envoyée par le contact administratif associée à la demande de certificat. La société TBS INTERNET pourra, le cas échéant, exiger que la demande de révocation soit également faite par le contact au sein de l'organisation et/ou le contact de facturation.

✔ À réception de la demande de révocation, la société TBS INTERNET confirmera auprès du contact administratif par un moyen autre que celui utilisé pour la demande de révocation, soit par téléphone, soit par fax.

- ✔ Le personnel de validation de la société TBS INTERNET ordonnera alors la révocation du certificat. L'identité des employés du personnel de validation, ainsi que les raisons évoquées pour justifier la révocation seront archivées, conformément aux procédures d'archivage couvertes par la présente DPC.

4.13.2 Mise en application de la révocation

Dès la révocation d'un certificat, la période opérationnelle dudit certificat est considérée comme terminée avec effet immédiat. Le numéro de série du certificat révoqué est placé dans la liste des certificats révoqués (LCR) et reste présent dans la LCR quelque temps après la fin de la période de validité du certificat. Les LCR sont actualisées toutes les 24 heures et publiées sur le site Internet de TBS INTERNET. Cependant, dans certaines circonstances, la LCR pourra exceptionnellement faire l'objet d'une publication plus fréquente. Si le certificat dispose du champ OCSP, l'information de révocation est également disponible en ligne quelques minutes après la révocation via OCSP.

Le protocole OCSP permet grâce à un serveur OCSP appelé OCSP « responder » de vérifier en ligne et en quasi temps-réel (sous 3H) les statuts des certificats. La réponse retournée par le serveur sera alors soit « good », soit « revoked », ou bien « unknown ».

Les serveur OCSP sont conformes à la norme RFC 2560.

4.14 Renouvellement

En fonction de l'option sélectionnée lors de la demande, la période de validité des certificats TBS INTERNET est d'un an (365 jours) à plusieurs années à partir de la date d'émission. Cette information se trouve dans un champ dédié sur le certificat.

Les frais de renouvellement se trouvent sur les sites Internet officiels de TBS INTERNET et sont indiqués dans les courriers envoyés aux abonnés dès que le ou les certificats approchent de leur date d'expiration.

Les procédures et conditions des demandes de renouvellement sont les mêmes que les conditions d'émission et de validation envoyées aux nouveaux clients.

4.15 Refabrication

Les procédures et conditions des demandes de refabrication diffèrent de celles employées lors de la délivrance ou d'un renouvellement de certificat. Un simple contrôle de cohérence par rapport à la demande initiale est effectuée, sauf pour les certificats dont la liste des CN ou SAN peut être modifiée. Dans cette situation, les ajouts ou modifications font l'objet d'un audit.

Les frais de refabrication se trouvent sur les sites Internet officiels de TBS INTERNET.

4.16 Avis avant l'expiration

La société TBS INTERNET s'engage à prendre toutes les mesures raisonnables pour notifier les abonnés via

courriel, de l'expiration imminente d'un certificat numérique. Les avis sont normalement envoyés dans les 56 jours avant l'expiration d'un certificat.

5 Conditions légales d'émission

Cette section a pour but de commenter les diverses observations formulées, garanties et limitations légales des certificats numériques TBS INTERNET.

5.1 Observations formulées par TBS INTERNET

La société TBS INTERNET formule à l'intention de tous les abonnés et de toutes les parties utilisatrices, certaines observations concernant ses prestations publiques, décrites ci-dessous. Elle se réserve le droit de modifier lesdites observations selon son bon jugement ou selon le droit applicable.

5.2 Informations incorporées par référence dans un certificat numérique TBS INTERNET

La société TBS INTERNET incorpore par référence, dans chaque certificat numérique qu'elle émet, les informations suivantes :

- Les modalités d'utilisation du certificat numérique.
- Les éventuelles politiques de certification applicables mentionnées sur le certificat émis par la société TBS INTERNET, y compris l'endroit où la présente DPC peut être consultée.
- Les éléments obligatoires et nécessaires au standard X.509v3.
- Les éléments personnalisés mais non obligatoires au standard X.509v3.
- Le contenu des extensions et des dénominations améliorées non entièrement exprimées sur le certificat.
- Toute autre information pouvant être indiquée comme telle et apparaissant dans un champ sur le certificat.

5.3 Affichage des limitations de responsabilité et du déni de garantie

Les certificats de la société TBS INTERNET peuvent inclure une brève déclaration énonçant les limitations de responsabilité, les limitations dans la valeur des transactions à accomplir, la période de validation ainsi que le but recherché du certificat, et enfin les dénis de garantie susceptibles d'être appliqués. L'abonné s'engage, avant de contracter un certificat, à accepter les conditions générales spécifiées par la société TBS INTERNET. Pour transmettre ses informations, la société TBS INTERNET est susceptible d'utiliser :

- Les attributs de l'unité administrative à contacter
- Un champ de saisie supplémentaire amendant la politique de certification
- Une extension propriétaire ou l'extension patentée d'un fournisseur tiers

5.4 Publication des données des certificats révoqués

La société TBS INTERNET se réserve le droit de publier une LCR (liste des certificats révoqués) comme indiqué dans les présentes.

5.5 Obligation de vérification de l'exactitude des informations soumises

Dans tous les cas et pour tous les types de certificats TBS INTERNET, l'abonné a pour obligation à tout moment, de contrôler la véracité des informations soumises et de notifier TBS INTERNET de tout changement éventuel apporté à ces dites informations.

5.6 Publication des informations

Les informations critiques publiées pourront être mises à jour de temps en temps, conformément aux articles de la présente DPC. Les mises à jour seront indiquées par l'apposition du numéro de version et de la date de publication sur la nouvelle publication.

5.7 Ingérences sur l'installation de TBS INTERNET

Les abonnés, les parties utilisatrices et toutes autres parties concernées ne devront en aucun cas nuire au bon déroulement/faire de l'ingénierie inverse de l'installation technique de l'architecture PKI de la société TBS INTERNET ou de son opérateur technique, à savoir sur le processus de génération des clés, le site Internet public ainsi que les répertoires de la société TBS INTERNET, sauf mention contraire autorisée de manière explicite par la présente DPC ou après autorisation écrite de la part de la société TBS INTERNET. En cas de non-respect par l'abonné de cette obligation, le certificat numérique sera révoqué sans avis préalable à l'intention de l'abonné. L'abonné devra payer tous les frais impayés dans le cadre du présent contrat. En cas de non-respect de ceci par la partie utilisatrice, le contrat avec ladite partie utilisatrice sera résilié et cette dernière se verra retirer l'autorisation d'utiliser ou d'accéder au répertoire de la société TBS INTERNET, et d'utiliser un certificat numérique et de bénéficier d'une prestation fournie par la société TBS INTERNET.

5.8 Normes

La société TBS INTERNET considère que l'utilisation de logiciels clients compatibles avec le standard X.509v3 et avec toutes les autres normes applicables implique nécessairement la mise en application des conditions établies dans la présente DPC. À cet effet, la société TBS INTERNET ne peut garantir, par l'utilisation desdits logiciels par l'utilisateur, la prise en charge et l'application systématiques des conditions de contrôle exigés par la société. L'utilisateur devra demander conseil auprès de personnes concernées.

5.9 Limitations des partenariats avec TBS INTERNET

Les partenaires du réseau TBS INTERNET ne devront en aucun cas entreprendre d'action quelle qu'elle soit susceptible de compromettre, jeter le discrédit sur/ou diminuer la confiance accordée aux produits et services de la société TBS INTERNET. Ils devront particulièrement s'abstenir de chercher à s'associer à d'autres autorités de certification racine ou chercher à appliquer d'éventuelles procédures quelles qu'elles soient en provenance de ces dites autorités. En cas de non-respect de ceci, le contrat avec ladite partie utilisatrice sera résilié et cette dernière se verra retirer l'autorisation d'utiliser ou d'accéder au répertoire de la société TBS INTERNET, et d'utiliser un certificat numérique et de bénéficier d'une prestation fournie par la société TBS INTERNET.

5.10 Limitation des responsabilités de la société TBS INTERNET vis-à-vis de ses partenaires

Dans la mesure où le réseau TBS INTERNET comprend un certain nombre d'AE opérant selon les pratiques et procédures dictées par la société TBS INTERNET, cette dernière garantit l'intégrité de tous les certificats émis en son sein, dans les limites de sa politique de garantie.

5.11 Choix des méthodes cryptographiques

Les parties sont seules responsables de leur propre jugement et de la formation dont elles ont pu bénéficier quant au choix de matériel, logiciel de sécurité et algorithmes de signature numérique/cryptage, y compris concernant les paramètres de configuration choisis, les procédures et les techniques ainsi que la PKI adopté comme solution à leurs besoins en matière de sécurité.

5.12 Confiance vis-à-vis d'une signature numérique non vérifiée

Les parties invoquant un certificat numérique doivent vérifier l'authenticité de celui-ci, et ce à tout moment en comparant sa validité à la LCR publiée par la société TBS INTERNET. Les parties utilisatrices sont informées du fait qu'une signature numérique non vérifiée ne peut en aucun cas être assimilée à la signature valable de l'abonné.

Invoquer une signature numérique non vérifiée est source de risques que ni la partie utilisatrice, ni la société TBS INTERNET, ne sont en mesure d'assumer intégralement.

Par la présente, la société TBS INTERNET informe les parties utilisatrices des modalités d'utilisation et de validation des signatures numériques dictées par les DPC/autres documents publiés dans le répertoire public mis à disposition à l'adresse http://www.tbs-internet.com/CA/repository ou disponible en utilisant des moyens autres que les moyens de communication traditionnels, via l'adresse mél indiquée dans la section Rédaction du présent document de la DPC.

5.13 Demandes de certificat rejetées

La clé privée associée à une clé publique, et soumise dans le cadre d'une demande de certificat rejetée, ne peut en aucun cas être utilisée pour créer une signature numérique si l'objectif de ladite signature est de créer les mêmes conditions de confiance attendues à l'origine par la création du certificat rejeté. De même, cette clé privée ne peut être soumise à nouveau dans le cadre d'une nouvelle demande de certificat.

5.14 Refus d'émission d'un certificat

La société TBS INTERNET se réserve le droit de refuser d'émettre un certificat à l'intention d'une partie quelle qu'elle soit, selon son bon jugement, et sans obligation ou responsabilité pour les conséquences préjudiciables de perte ou de frais occasionnées par son refus. La société TBS INTERNET se réserve le droit de ne pas divulguer les raisons justifiant son refus.

5.15 Obligations de l'abonné

Sauf mention contraire dans les présentes, les abonnés et eux seuls sont dans l'obligation de :

- Limiter – en interne - les risques d'atteinte à l'intégrité de la clé privée en s'assurant de la formation et des compétences de son personnel en matière d'infrastructure PKI.

- Générer leurs propres paires de clés publique / privée à utiliser avec la demande de certificat soumise à la société TBS INTERNET ou à l'une des AE de TBS INTERNET.

- S'assurer que la clé publique soumise à la société TBS INTERNET ou à l'une des AE de la société TBS INTERNET correspond à la clé privée utilisée.
- S'assurer que la clé publique soumise à la société TBS INTERNET ou à l'une des AE de la société TBS INTERNET est la bonne clé.
- Fournir à la société TBS INTERNET ou à l'AE de la société TBS INTERNET des informations correctes et précises.

- Prévenir TBS INTERNET ou l'AE de la société TBS INTERNET si, à un moment ou à un autre durant la validité d'un certificat, les informations à l'origine soumises ont été modifiées depuis la toute dernière soumission à la société TBS INTERNET.
- Générer la nouvelle paire de clés sécurisées associée au certificat demandé à la société TBS INTERNET ou à l'une des AE de la société TBS INTERNET.

- Lire, comprendre et approuver l'ensemble des conditions générales de la présente DPC de la société TBS INTERNET ainsi que les politiques connexes publiées dans le répertoire de TBS INTERNET à l'adresse http://www.tbs-internet.com/CA/repository

- S'abstenir d'altérer sans autorisation un certificat de la société TBS INTERNET.
- Utiliser les certificats de la société TBS INTERNET à des fins légales et autorisées, conformément aux usages et pratiques suggérés dans la présente DPC.

- Cesser immédiatement d'utiliser un certificat TBS INTERNET si l'une des informations contenues dans ledit certificat est trompeuse, obsolète ou incorrecte.
- Cesser d'utiliser un certificat TBS INTERNET si ledit certificat a expiré et supprimer celui-ci de toute application et/ou périphérique sur lequel celui-ci a été installé.
- S'abstenir d'utiliser la clé privée d'un abonné correspondant à la clé publique d'un certificat émis par la société TBS INTERNET pour émettre un certificat numérique à l'intention d'une autre entité finale ou d'une AC secondaire.

- Faire, dans la mesure du raisonnable, tout son possible pour empêcher une éventuelle atteinte à l'intégrité, la perte, la divulgation, la modification, voire l'utilisation non autorisée de la clé privée associée à la clé publique publiée dans un certificat TBS INTERNET.
- Demander la révocation d'un certificat en cas d'évènement susceptible d'affecter matériellement l'intégrité d'un certificat TBS INTERNET.
- À cause et pour les actes et omission de la part de partenaires et d'agents qu'il utilise, générer, conserver, bloquer ou détruire les clés privées en leur détention.

5.16 Observations de l'abonné après acceptation d'un certificat

Après acceptation d'un certificat, l'abonné affirme à l'intention de la société TBS INTERNET et des parties utilisatrices que, au moment de l'acceptation, et jusqu'à nouvel ordre :

- Les signatures numériques créées à l'aide de la clé privée associée à la clé publique du certificat correspondent à la signature numérique de l'abonné ; en outre, que le certificat a été accepté et est parfaitement opérationnel au moment de la création de la signature numérique.

- À aucun moment une personne non autorisée n'a eu accès à la clé privée de l'abonné.
- Toutes les observations formulées par l'abonné à l'intention de la société TBS INTERNET et concernant les informations contenues dans le certificat sont exactes et complètes.

- Toutes les informations contenues dans le certificat sont, à la connaissance de l'abonné, exactes et complètes. Néanmoins, dans la mesure où l'abonné est informé de ces informations, il est de son devoir d'agir dans les plus brefs délais pour notifier la société TBS INTERNET de toute inexactitude éventuelle de ces informations.
- Le certificat est utilisé exclusivement à des fins autorisées et légales, en accord avec la présente DPC.
- L'abonné s'engage à utiliser un certificat uniquement en conjonction avec l'entité nommée dans le champ organisation du certificat numérique (le cas échéant).

- L'abonné s'engage à garder à tout moment le contrôle de la clé privée, à utiliser un système sécurisé et fiable, et à prendre toutes les mesures raisonnables pour empêcher une éventuelle perte, divulgation, modification ou utilisation non autorisée.
- L'abonné est l'utilisateur final, et non une AC. De ce fait, il s'engage à ne pas utiliser la clé privée associée à la clé publique listée dans le certificat à des fins de signature d'un certificat quel qu'il soit (ou tout autre format de clé publique certifiée) ou d'une LCR, et d'exercer les fonctions d'une AC ou de toute autre autorité quelle qu'elle soit, sauf mention contraire expressément convenue par écrit entre l'abonné et la société TBS INTERNET.
- L'abonné accepte les conditions générales de la présente DPC, ainsi que les autres contrats et autres politiques de service clientèle de la société TBS INTERNET.
- L'abonné s'engage à respecter le droit applicable dans son pays ou le territoire qui lui est attribué, y compris les lois concernant la protection sur la propriété intellectuelle, les virus, l'accès aux systèmes informatiques, etc.
- L'abonné s'engage à se conformer à toutes les règlementations et lois sur l'exportation des biens à double usage lorsqu'elles s'appliquent.

5.17 Indemnisation par l'abonné

En acceptant un certificat, l'abonné s'engage à indemniser la société TBS INTERNET et la décharger, ainsi que ses agents, fournisseurs et opérateurs, de toute responsabilité vis-à-vis d'actes ou d'omissions ayant pour conséquences une obligation de réparer un quelconque préjudice, la perte ou les dommages occasionnés par ceux-ci ; décharger la société TBS INTERNET de toute action pénale et frais quels qu'ils soient, y compris les honoraires d'avocat aussi raisonnables qu'ils puissent être, que la société TBS INTERNET et les parties susmentionnées pourraient encourir, suite à l'utilisation ou à la publication d'un certificat, et occasionnés par :

- Des données erronées ou dénaturées fournies par l'abonné ou par un agent.

- Le défaut par l'abonné à divulguer un fait matériel, dans le cas où la déformation des informations ou l'omission de celles-ci font suite à une négligence ou sont dues à une intention de tromper l'AC, la société TBS INTERNET ou toute personne recevant ou invoquant le certificat.

- Le défaut de protection des données confidentielles de l'abonné, y compris la clé privée, ou le défaut à prendre, dans la limite du raisonnable, les précautions nécessaires pour empêcher la compromission, la perte, la divulgation, la modification ou l'utilisation non autorisée des données confidentielles de l'abonné.

- La violation du droit applicable dans son pays ou du territoire qui lui est attribué, y compris les lois

concernant la protection sur la propriété intellectuelle, les virus, l'accès aux systèmes informatiques, etc.

5.18 Obligations des Autorités d'Enregistrement de TBS INTERNET

Les AE de TBS INTERNET opèrent conformément aux politiques et aux pratiques spécifiées dans la présente DPC et conformément au contrat de distribution pour hébergeur,et au contrat pour titulaire d'un compte PKI PME. L'AE est liée par contrat à :

- Réceptionner les demandes de certificat TBS INTERNET conformément à la présente DPC.
- Effectuer toutes les opérations de vérification prescrites par les procédures de validation de la société TBS INTERNET et la présente DPC.

- Réceptionner, vérifier et transmettre à la société TBS INTERNET toutes les demandes de révocation des certificats TBS INTERNET conformément aux procédures de révocation de TBS INTERNET et la présente DPC.

- Agir selon la règlementation en vigueur et le droit applicable.
- Vérifier l'exactitude et l'authenticité des informations fournies par l'abonné lors d'un renouvellement ou d'une refabrication du certificat, conformément avec la politique de certification applicable.

5.19 Obligations de la partie utilisatrice

La partie utilisatrice invoquant un certificat TBS INTERNET accepte le fait que, pour pouvoir raisonnablement se fier à un certificat TBS INTERNET, elle doit :

- Minimiser les risques liés à l'invocation d'une signature numérique créée à partir d'un certificat non valide, révoqué, expiré ou rejeté. La partie utilisatrice doit avoir raisonnablement fait tout son possible pour acquérir suffisamment d'informations sur l'utilisation des certificats numériques et sur les infrastructures PKI.

- Étudier les limitations de l'utilisation des certificats numériques et prendre conscience, par la lecture du contrat de la partie utilisatrice, des valeurs maximales que peuvent atteindre les transactions susceptibles d'être effectuées à l'aide d'un certificat numérique TBS INTERNET.

- Lire et approuver les termes et conditions de la DPC de TBS INTERNET et du contrat de la partie utilisatrice.

- Vérifier la validité d'un certificat TBS INTERNET en consultant la LCR concernée et les LCR de l'AC intermédiaire et AC racine.

- Se fier à un certificat TBS INTERNET uniquement s'il est valable et s'il n'a pas été révoqué ou n'a pas expiré.

- Se fier à un certificat TBS INTERNET dans la limite du raisonnable, selon les circonstances énumérées dans cette section et les autres sections pertinentes de la présente DPC.

5.20 Légalité des informations

L'abonné est seul responsable de la légalité des informations qu'il présente ; informations qui seront utilisées dans les certificats émis dans le cadre de la présente DPC, et ce dans quelque compétence juridique que ce soit où ces informations sont susceptibles d'être utilisées ou consultées.

5.21 Responsabilité de l'abonné vis-à-vis des parties utilisatrices

Sans limite des obligations des autres abonnés énumérés dans la présente DPC, les abonnés sont responsables de toute déclaration fallacieuse faite concernant des certificats délivrés à des tierces parties ; tierces parties invoquant raisonnablement les observations contenues dans ces dits certificats et ayant vérifié une ou plusieurs signatures numériques associées aux dits certificats.

5.22 Obligation vis-à-vis des agents de contrôle

L'abonné s'engage à maîtriser et être responsable des données que son agent fournit à la société TBS INTERNET. Il s'engage à notifier dans les plus brefs délais l'émetteur de ces données, de toute déformation des informations et omissions faites par cet agent. L'obligation du présent article s'applique en permanence.

5.23 Utilisation d'un agent

Concernant les certificats émis à la demande d'un agent de l'abonné, l'agent et l'abonné s'engagent tous deux conjointement et séparément à indemniser la société TBS INTERNET, ainsi que ses agents et ses fournisseurs.

5.24 Conditions d'utilisation du répertoire et du site Internet de la société TBS INTERNET

Les parties (comprenant les abonnés et les parties utilisatrices) accédant au répertoire de la société TBS INTERNET (http://www.tbs-internet.com/CA/repository) et au(x) site(s) Internet officiel(s) approuvent les dispositions de la présente DPC et toute autre condition d'utilisation que la société TBS INTERNET est susceptible de mettre en application.

Les parties font la preuve de leur acceptation des conditions d'utilisation de la DPC en utilisant un certificat émis par la société TBS INTERNET.

En cas de non-respect des conditions d'utilisation des répertoires et du site Internet de la société TBS INTERNET, cette dernière pourra décider de mettre un terme à ses relations avec la partie concernée.

5.25 Exactitude des informations

La société TBS INTERNET, reconnaissant sa position en tant qu'interlocuteur de confiance, s'engage à faire raisonnablement tout son possible pour garantir que les parties accédant à ces répertoires bénéficient d'informations fiables, correctes et actualisées. Elle ne peut cependant accepter aucune responsabilité en dehors des limites définies dans la présente DPC et la politique de garantie de la société TBS INTERNET.

En cas de non-respect des conditions d'utilisation des répertoires et du site Internet de la société TBS INTERNET, cette dernière pourra décider de mettre un terme à ses relations avec la partie concernée.

5.26 Obligations de la société TBS INTERNET

Dans les limites spécifiées dans les sections concernées de la DPC, la société TBS INTERNET s'engage à :

- Se conformer à la présente DPC, ainsi qu'à ses procédures et politiques internes ou publiées.
- Respecter la règlementation et le droit applicable.
- Fournir des prestations d'infrastructure et de certification, comprenant mais non limitées à celles-là, la mise en place et le fonctionnement du site Internet et du répertoire TBS INTERNET pour la délivrance des prestations de la PKI.
- Fournir des mécanismes de confiance, à savoir un mécanisme de génération de clé, un système de protection des clés et des procédures de partage de secret concernant sa propre infrastructure.
- Avertir dans les plus brefs délais en cas d'atteinte à l'intégrité d'une ou de plusieurs clés privées.
- Mettre à disposition et valider les procédures de demandes pour les divers certificats que la société est susceptible de distribuer publiquement.
- Émettre des certificats numériques conformément à la présente DPC et satisfaire à ses obligations, spécifiées dans les présentes.
- À réception d'une demande de la part d'une AE opérant au sein du réseau TBS INTERNET, agir rapidement en vue d'émettre un certificat de TBS INTERNET conformément à la présente DPC.
- À réception d'une demande de révocation de la part d'une AE opérant au sein du réseau TBS INTERNET, agir rapidement en vue de révoquer un certificat de TBS INTERNET conformément à la présente DPC.
- Publier les certificats acceptés conformément à la présente DPC.
- Procurer une assistance aux abonnés et aux parties utilisatrices conformément aux instructions de la présente DPC.
- Révoquer les certificats conformément à la présente DPC.
- Organiser l'expiration et le renouvellement des certificats conformément à la présente DPC.
- Mettre à disposition des parties qui le demandent, un exemplaire de la présente DPC et des politiques en vigueur.

- Garantir l'exactitude des informations publiées sur un certificat qualifié émis conformément aux consignes de la Directive Européenne 99/93.

- Garantir le fait que le signataire détient la clé privée au moment de l'émission d'un certificat émis conformément aux conditions portant sur les certificats qualifiés selon la Directive Européenne 99/93.

L'abonné convient également que la société TBS INTERNET n'a pas d'autres obligations dans le cadre de la présente DPC.

5.27 Aptitude à un but particulier

La société TBS INTERNET rejette toute garantie et obligation de quelque type que ce soit, y compris la garantie d'aptitude à un but particulier, et toute garantie concernant l'exactitude des informations fournies non vérifiées, à l'exception de celles contenues dans les présentes et de celles ne pouvant être exclues par le droit applicable.

5.28 Autres garanties

À l'exception des éléments susceptibles d'avoir été spécifiés dans le cadre des certificats qualifiés émis conformément aux conditions de la Directive Européenne 99/93, la société TBS INTERNET ne garantit pas :

- L'exactitude, l'authenticité, l'intégralité ou l'aptitude des informations non vérifiées quelles qu'elles soient contenues dans les certificats, voire rassemblées, publiées ou disséminées par/pour le compte de la société TBS INTERNET, à l'exception des informations susceptibles d'être communiquées dans la description des produits concernés ci-dessous dans la présente DPC et dans la politique de garantie de la société TBS INTERNET.

- L'exactitude, l'authenticité, l'intégralité ou l'aptitude des informations quelles qu'elles soient, contenues dans les certificats TBS INTERNET Email Novice de classe 1, les versions gratuites, de test ou de démonstration.

- En outre, n'accepte aucune responsabilité concernant les communications d'informations contenues dans un certificat, à l'exception des informations susceptibles d'être contenues dans la description des produits concernés de la présente DPC.

- Ne garantit pas la qualité, les fonctions ou les performances des logiciels ou des périphériques matériels.

- Bien que la société TBS INTERNET soit responsable de la révocation d'un certificat, elle ne peut être tenue pour responsable de la non-exécution de la révocation en cas de circonstances indépendantes de sa volonté.

- La validité, l'intégralité ou la disponibilité des répertoires de certificats émis par une tierce partie (y compris un agent) sauf mention contraire spécifiquement indiquée par la société TBS INTERNET.

5.29 Informations non vérifiées de l'abonné

Nonobstant les limitations de garantie énumérées dans la section produits de la présente DPC, la société TBS INTERNET ne pourra être tenue pour responsable des informations non vérifiées de l'abonné qui lui sont soumises, ou qui sont soumises au répertoire de TBS INTERNET, ou soumises avec l'attention d'inclure celles-ci dans un certificat, à l'exception des éléments susceptibles d'être spécifiés dans le cadre des certificats qualifiés émis conformément aux conditions de la Directive Européenne 99/93.

5.30 Exclusion de certains éléments des pertes et préjudices

En aucun cas (sauf en cas de tromperie ou de mauvaise conduite volontaire) la société TBS INTERNET ne pourra être tenue responsable de :

- Dommages directs, accessoires ou indirects
- Manque à gagner.
- Perte de données.
- Dommages indirects, immatériels ou dissuasifs provenant de l'utilisation, la livraison, la patente, les performances ou manque de performance des certificats ou de signatures numériques.
- Des autres opérations ou prestations offertes dans le cadre de la présente DPC.
- Des autres préjudices, à l'exception de ceux subis à la suite de la confiance envers les informations apparaissant sur un certificat, et sur les informations vérifiées sur un certificat.
- Toute obligation de réparer les conséquences préjudiciables dans ces circonstances ou dans toute autre circonstance si la faute concernant ces informations vérifiées fait suite à une tromperie ou une mauvaise conduite volontaire de la part du demandeur.
- Toute obligation de réparer un préjudice provenant de l'utilisation d'un certificat n'ayant pas été émis ou utilisé en accord avec la présente DPC.
- Toute obligation de réparer un préjudice suite à l'utilisation d'un certificat non valable.
- Toute obligation de réparer un préjudice suite à l'utilisation d'un certificat ayant dépassé les limitations en termes d'utilisation, valeur et transaction définies sur celui-ci ou dans la DPC.
- Toute obligation de réparer un préjudice en rapport avec la sécurité, la facilité d'utilisation, l'intégrité des produits, y compris le matériel et le logiciel que l'abonné utilise.
- Toute obligation de réparer un préjudice suite à l'atteinte à l'intégrité de la clé privée de l'abonné.

La société ne limite ni n'exclut sa responsabilité en cas de décès ou de préjudices corporels.

5.31 Plan de garantie d'un certificat

Sauf en cas de mauvaise conduite volontaire, la responsabilité cumulée maximale acceptée par la société TBS INTERNET dans le cadre de l'émission d'un certificat contenant des informations non valables, vis-à-vis de l'abonné d'un certificat ; certificat ayant été validé par l'utilisation des méthodes correspondant à la classe et/ou au type de certificat, est exposée ci-dessous.

5.31.1 Certificat Standard

La responsabilité cumulée de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices dans le cadre de l'utilisation d'un certificat Standard ne pourra dépasser 50 $US (cinquante dollars américains).

5.31.2 Certificat Ecommerce

La responsabilité cumulée de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices dans le cadre de l'utilisation d'un certificat Ecommerce ne pourra dépasser 2 500 $US (deux mille cinq cents dollars américains).

5.31.3 Certificat Premium

La responsabilité cumulée de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices dans le cadre de l'utilisation d'un certificat Premium ne pourra dépasser 10 000 $US (dix mille dollars américains).

5.31.4 Certificat Omnidomaine

La responsabilité cumulée de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices dans le cadre de l'utilisation d'un certificat Omnidomaine ne pourra dépasser 10 000 $US (dix mille dollars américains).

5.31.5 Certificat Email Professionnel, Utilisateur PKI PME

Aucune responsabilité de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices, n'est rattachée à ce type de certificat.

5.31.6 Certificat Email Particulier

Aucune responsabilité de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices, n'est rattachée à ce type de certificat.

5.31.7 Certificat Sign & Login, Multiples-Sites

Aucune responsabilité de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices, n'est rattachée à ce type de certificat.

5.31.8 Certificat Test, Test Sign & Login, Email Novice

Aucune responsabilité de la société TBS INTERNET vis-à-vis des demandeurs, abonnés et parties utilisatrices, n'est rattachée à ce type de certificat.

5.32 Limitations financières par rapport à l'utilisation d'un certificat

Les certificats TBS INTERNET peuvent être utilisés uniquement en rapport avec des transferts de données et des transactions d'une valeur en dollars américains ($ US) inférieure au niveau de garantie associé au certificat concerné ; niveau de garantie spécifiée dans la section 5.31 de la présente DPC.

5.33 Limitations en termes de dommages et pertes

En aucun cas (excepté en cas de tromperie ou de mauvaise conduite volontaire) la responsabilité cumulée de la société TBS INTERNET vis-à-vis de toutes les parties comprenant mais non limitées à celles-ci, les abonnés, les demandeurs, les destinataires, ou les parties utilisatrices pour toutes les signatures numériques et les transactions en rapport avec le certificat émis ne pourra être supérieure au plafond de responsabilité applicable dans le cas dudit certificat, plafond mentionné dans le plan de garantie de la société TBS INTERNET et détaillé en section 5.31 de la présente DPC.

5.34 Conflit de règlements

Lorsque la présente DPC entre en conflit avec les autres règlements, consignes ou contrats, la DPC, datant du 6 juin 2006, prime et lie l'abonné et les autres parties, à l'exception des autres contrats :

- Antérieurs à la première parution publique de la version actuelle de la DPC.
- Remplaçant expressément la présente DPC, lesdits contrats étant applicables sur les parties des présentes, et dans les limites autorisées par la loi.

5.35 Droits de propriété intellectuelle de la société TBS INTERNET

La société TBS INTERNET ou ses partenaires ou associés détiennent la totalité des droits de propriété intellectuelle associés aux bases de données, aux sites Internet, aux certificats numériques de TBS INTERNET et aux autres publications en provenance de la société TBS INTERNET, y compris la présente DPC.

5.36 Violation et autres éléments de préjudice

Les abonnés de la société TBS INTERNET déclarent et garantissent que, à la soumission des informations à la société TBS INTERNET et dans l'utilisation d'un nom de domaine et d'un nom distinctif (et de la totalité des informations soumises dans le cadre d'une demande de certificat), ils s'engagent à ne pas enfreindre ou

transgresser les droits quels qu'ils soient d'une tierce partie dans quelque juridiction que ce soit, concernant la marque de commerce, la marque de service, la dénomination commerciale, le nom de société ou à l'encontre de tout autre droit de propriété intellectuelle de ladite tierce partie. Ils s'engagent à ne pas chercher à utiliser le nom de domaine et le nom distinctif à des fins illicites y comprenant mais non limités à celles-ci, une éventuelle ingérence de caractère tortueux sur un contrat, ou un avantage commercial éventuel, une concurrence déloyale, l'intention de nuire à la réputation d'un tiers, tromper ou induire en erreur une personne, qu'elle soit morale ou physique.

Bien que la société TBS INTERNET fasse, dans la limite du raisonnable, tout son possible, pour apporter le cas échéant son assistance, les abonnés s'engagent à décharger, exempter, indemniser la société TBS INTERNET de toute responsabilité pour les pertes et préjudices résultants de ces ingérences et de ses violations, et sont responsables de défendre les intérêts de la société TBS INTERNET.

5.37 Propriétés

Les certificats sont la propriété de la société TBS INTERNET. La société TBS INTERNET autorise la reproduction et la distribution des certificats de manière non exclusive, sans droits d'auteur dans la mesure où ceux-ci sont reproduits et distribués dans leur totalité. La société TBS INTERNET se réserve le droit de révoquer un certificat à tout moment.

Les clés publiques et les clés privées sont la propriété des abonnés qui dans leur bon droit les ont émises et les détiennent.
Toutes les parties secrètes (éléments distribués) de la clé privée de la société TBS INTERNET restent la propriété de cette dernière.

5.38 Droit applicable

La présente DPC est régie et interprétée selon la loi française. Ce choix du droit applicable a été fait de manière à garantir une interprétation homogène de la présente DPC, quel que soit le lieu de résidence ou le lieu d'utilisation des certificats numériques TBS INTERNET ou des autres produits et services de la société. La loi française s'applique à l'ensemble des relations contractuelles de la société TBS INTERNET, pour lesquelles s'applique la présente DPC, ou pour lesquelles la DPC est mentionnée implicitement ou explicitement en relation avec les produits et services TBS INTERNET, et pour lesquelles la société TBS INTERNET exerce les fonctions de fournisseur, prestataire, bénéficiaire, destinataire ou autre.

5.39 Compétence juridique

Chacune des parties, y compris les partenaires de la société TBS INTERNET, les abonnés et les parties utilisatrices, conviennent irrévocablement du fait que les tribunaux français et en première instance le tribunal de commerce de Caen possèdent la juridiction exclusive pour entendre et décider de toute poursuite, action ou procédure judiciaire, et pour régler tout litige quel qu'il soit susceptible d'avoir lieu du fait de la DPC ou en rapport avec la DPC, ou concernant la prestation des services de PKI de la société TBS INTERNET.

5.40 Règlement des litiges

Avant de recourir à un mécanisme de règlement des litiges quel qu'il soit, à savoir une décision judiciaire ou tout type de règlement extrajudiciaire de conflits (y compris et sans exception, arbitrage, avis d'expert liant les parties en cause, etc.), les parties s'accordent à notifier la société TBS INTERNET du litige, en vue de chercher le règlement anticipé de celui-ci.

5.41 Ayant droits et ayant cause

La présente DPC engage les ayant droits, les exécuteurs testamentaires, les héritiers, les représentants, les administrateurs des biens et les ayant cause, qu'ils soient explicites, implicites ou évidents, des parties. Les droits et obligations mentionnés dans la présente DPC sont transférables par les parties, par effet de la loi (y compris des suites d'une fusion ou d'un transfert de majorité des titres avec droit de vote) ou autres, dans la mesure où ce transfert est en accord avec les articles de la présente DPC concernant la terminaison et la cessation d'activité ; et dans la mesure où ce transfert n'affecte pas la novation des autres dettes ou obligations que la partie affectée doit aux autres parties à l'heure du transfert.

5.42 Dissociabilité

Si une disposition quelle qu'elle soit de la présente DPC ou l'application de celle-ci s'avère, pour quelque raison que ce soit et dans quelque mesure que ce soit, non valable ou non exécutoire, les parties restantes de la DPC (et l'application de la disposition non valable ou non exécutoire à d'autres personnes ou dans d'autres circonstances) seront interprétées de manière à affecter l'intention d'origine des parties.

Chaque disposition de la présente DPC, prévoyant une limitation de la responsabilité, un déni de responsabilité ou la limitation des garanties ou des autres obligations, où l'exclusion de dommages et intérêts est considérée comme séparable et indépendante de toute autre disposition et devra être appliquée en tant que telle.

5.43 Interprétation

La présente DPC devra être interprétée sans exception, dans le cadre des pratiques commerciales, du caractère raisonnable de l'activité commerciale selon les circonstances et l'usage voulu du produit ou du service. Dans l'interprétation de la DPC, les parties devront également prendre en compte l'aspect et la mise en œuvre au plan international des services et des produits de la société TBS INTERNET ; et son réseau international d'Autorités d'Enregistrement ainsi que le principe de bonne foi lorsqu'il est appliqué dans les transactions commerciales.

Les en-têtes de section, les sous-titres et les autres titres de la présente DPC ne sont insérés que par commodité et par référence et de ce fait, ne devront pas être utilisés pour interpréter, traduire ou mettre en application les dispositions de la DPC.

Les annexes et définitions de la DPC sont, pour tout ce qui a trait à elles, parties intégrantes et contraignantes de la DPC.

5.44 Sans dispense

La présente DPC sera appliquée dans sa totalité. À cet effet, le non-respect par une personne quelle qu'elle soit, d'une disposition de la DPC ne pourra être considérée comme une dispense, à l'avenir, de l'exécution desdites dispositions ou de toute autre disposition.

5.45 Avis

La société TBS INTERNET accepte la réception d'un avis en rapport avec la présente DPC au moyen de messages signés numériquement ou sous la forme papier. À réception d'un accusé de réception valable, signé numériquement de la part de TBS INTERNET, l'expéditeur considéra le message comme envoyé et réceptionné. L'expéditeur devra recevoir cet accusé de réception dans les cinq (5) jours. Dans le cas contraire, un avis par écrit doit être envoyé sous forme papier par le biais d'un service postal confirmant la livraison ou par lettre recommandée avec accusé de réception, ou par lettre avec affranchissement payé par anticipation, ou par courrier avec accusé de réception exigé, adressé à :

TBS INTERNET Limited

Britannia House, Athol Street
Douglas, Isle of Man
IM1 1JD
British Isles

Tél : +44-330-684-0000

À l'attention du Service juridique

Mél : legal@tbs-internet.com

Cette DPC, les accords connexes et les Politiques de Certification référencés dans ce document sont disponibles en ligne à l'adresse http://www.tbs-internet.com/CA/repository.

5.46 Honoraires

La société TBS INTERNET facture des honoraires à l'abonné pour certains de ses services de certification, à savoir l'émission, le renouvellement et la ré-émission des certificats (conformément à la politique de ré-émission de TBS INTERNET, en section 5.7 de la DPC). Ces honoraires sont renseignés sur les sites Internet officiels de la société TBS INTERNET (www.tbs-internet.com. www.tbs-certificats.com et www.tbs-x509.com).

La société TBS INTERNET ne facture aucun honoraire pour la révocation d'un certificat ou pour qu'une partie utilisatrice puisse vérifier le statut de validité d'un certificat émis par la société TBS INTERNET par le biais des listes de certificats révoqués.

La société TBS INTERNET se réserve le droit de modifier ces honoraires. Les partenaires de la société TBS INTERNET à savoir les distributeurs, les partenaires hébergeurs, et les titulaires de comptes PKI PME seront en

temps voulu informés des modifications de prix dans les contrats de partenariat les concernant.

5.47 Politique de ré-émission de la société TBS INTERNET

La société TBS INTERNET pratique une politique de ré-émission sur 30 jours. Pendant cette période de 30 jours (qui commence dès l'émission d'un certificat), l'abonné a la possibilité de demander la ré-émission d'un certificat, qui n'est pas facturée. Si des informations autres que la clé publique nécessitent une modification, et nécessitent un nouveau processus de validation, la société TBS INTERNET se réserve le droit de refuser la ré-émission gratuite. Le cas échéant, le certificat d'origine pourra être révoqué et l'abonné remboursé.

La société TBS INTERNET n'est pas tenue de re-émettre gratuitement un certificat après que la période de ré-émission de 30 jours ait expiré.

5.48 Politique de remboursement de la société TBS INTERNET

La société TBS INTERNET ne pratique pas de politique de remboursement.

Un demande de certificat n'ayant pas abouti (à l'émission d'un certificat) peut être annulée dans les 30 jours suivant la demande initiale. Un remboursement à 90% pourra être demandé, les 10% restant étant facturés.

La société TBS INTERNET n'est pas l'agent, le mandataire, le fiduciaire, ou un autre représentant des abonnés ou des parties intéressées.

6 Procédure générale d'émission

6.1 Généralités - TBS INTERNET

La société TBS INTERNET propose différents types de certificats qui font appel à la technologie SSL et S/MIME ; certificats destinés à sécuriser les transactions en ligne et les échanges par mél. Avant d'émettre un certificat, la société TBS INTERNET valide une demande conformément aux dispositions de la DPC ; validation pouvant impliquer, pour elle, d'exiger auprès des demandeurs la délivrance d'un certain nombre de documents officiels susceptibles d'étayer la demande.

Les certificats TBS INTERNET sont émis à l'intention des organisations ou des individus.

La période de validité des certificats TBS INTERNET varie selon le type de certificats, mais en règle générale, un certificat est valable pendant 1 à 6 ans. La société TBS INTERNET se réserve le droit, à sa seule discrétion, d'émettre des certificats susceptibles de dépasser ces périodes définies.

6.2 Certificats émis à des individus et des organisations

La demande de certificat peut être faite en utilisant l'un des procédés suivants :

Mode connecté : par Internet (https). Le demandeur soumet sa demande en cliquant sur un lien sécurisé, sur Internet, selon une procédure donnée par la société TBS INTERNET. Un certain nombre de documents supplémentaires chargés d'étayer la demande pourront être exigés, de manière à ce que la société TBS INTERNET puisse vérifier l'identité du demandeur. Le demandeur soumet ces documents supplémentaires à la société TBS INTERNET. Après vérification de l'identité du demandeur, la société TBS INTERNET émet le certificat et envoie un avis au demandeur. Le demandeur télécharge et installe le certificat sur son périphérique. Il doit alors avertir TBS INTERNET en cas d'inexactitude ou d'anomalies du certificat, et ce dans les plus brefs délais après réception du certificat, ou informer plus rapidement la société TBS INTERNET de l'éventuelle nécessité d'inclure un contenu informationnel supplémentaire dans le certificat.

La société TBS INTERNET pourra, à sa seule discrétion, accepter les demandes via mél.

6.3 Contenu

Le contenu habituel des informations publiées sur un certificat comprend, mais n'est pas limité aux éléments d'information suivants :

6.3.1 Certificats Serveur

- Nom de domaine complet du demandeur,
- Nom de l'organisation du demandeur,

- Code du pays du demandeur,
- Nom de l'unité administrative, adresse, rue, ville, état/région,
- Autorité d'enregistrement émettrice (TBS INTERNET),
- Clé publique du demandeur,
- Signature numérique de TBS INTERNET,
- Type d'algorithme,
- Période de validité du certificat numérique,
- Numéro de série du certificat numérique.

6.3.2 Certificat Client Email

- Adresse mél du demandeur,
- Nom du demandeur,
- Code du pays du demandeur,
- Nom de l'organisation, nom de l'unité administrative, adresse, rue, ville, état/région,
- Clé publique du demandeur,
- Autorité d'enregistrement émettrice (TBS INTERNET),
- Signature numérique de TBS INTERNET,
- Type d'algorithme,
- Période de validité du certificat numérique,
- Numéro de série du certificat numérique.

6.4 Délai nécessaire pour confirmer les données soumises

La société TBS INTERNET s'engage à prendre toutes les mesures raisonnables pour confirmer les informations saisies lors des demandes de certificats, et émettre le certificat numérique dans un délai raisonnable. Le délai dépend grandement du temps nécessaire à l'abonné pour fournir les documents et/ou les informations nécessaires. À réception de ces documents et/ou informations, la société TBS INTERNET vise à confirmer les données soumises dans le cadre de la demande et à compléter le processus de validation, et émettre/rejeter la demande de certificat dans les 3 jours ouvrés.

De temps en temps, un évènement indépendant de la volonté de la société TBS INTERNET peut retarder le

processus d'émission. Cependant, la société fera, dans la limite du raisonnable, tout son possible pour respecter les délais et pour renseigner promptement le demandeur de tout facteur susceptible d'affecter le délai d'émission.

6.5 Procédure d'émission

Voici ci-dessous les différentes étapes constituant les évènements marquants de l'émission d'un certificat Serveur :

a) Le demandeur remplit le questionnaire de demande en ligne sur le site Internet de TBS INTERNET et soumet les informations nécessaires : la demande de signature de certificat (CSR), les coordonnées de son organisation, d'un contact administratif, d'un contact technique et les informations de paiement.

b) Le demandeur accepte le contrat d'abonnement en ligne.

c) Le demandeur délivre les informations requises à la société TBS INTERNET.

d) Le demandeur paye les frais de certification.

e) La société TBS INTERNET vérifie les informations soumises à partir de bases de données tierces et les archives publiques.

f) Après que les informations aient été validées, la société TBS INTERNET est en mesure d'émettre le certificat à l'intention du demandeur. Si la demande devait être rejetée à ce stade, la société en informerait le demandeur.

g) Le renouvellement s'effectue conformément aux procédures décrites dans la présente DPC et sur les sites Internet officiels de la société TBS INTERNET.

h) La révocation du certificat s'effectue conformément aux procédures décrites dans la présente DPC.

Rédaction du présent document

Ce document correspond à la version 1.13 de la DPC de TBS INTERNET, créée le 14 septembre 2021 et signée par les membres de l'Autorité en charge de la politique de certification de TBS INTERNET.