

Déclaration des Pratiques de Certification de TBS INTERNET

Version 1.14

1 mars 2023

www.tbs-internet.com

Historique des révisions

Version	Date	Action	Commentaire
V1.14		Révision finale	Suite à fin d'émission des certificats audités par TBS, le document a été simplifié pour renvoyer vers l'éditeur des produits opérés en marque blanche.
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

Version	Date	Action	Commentaire
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

Propriété

Ce document est la propriété de TBS Internet Limited. Tous droits réservés.
Les marques citées appartiennent à leurs propriétaires respectifs.

Notes

Document réalisé sous LibreOffice sous Linux

Table des matières

1 Généralités.....	7
1.1 TBS INTERNET.....	8
1.2 La DPC de TBS INTERNET.....	8
1.3 Autres Contrats & Déclarations de pratiques.....	8
1.4 Hiérarchie de la PKI TBS INTERNET (pour mémoire).....	9
1.4.1 Certificats mél.....	9
1.4.2 Certificats serveur standard.....	9
1.4.3 Certificats serveur Pro Hosting.....	9
1.4.4 Certificats client généraux.....	10
Rédaction du présent document.....	11

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/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 constituait la Déclaration des Pratiques de Certification (DPC) de la société TBS INTERNET et exposait les pratiques et principes juridiques, commerciaux et techniques employés par la société TBS INTERNET dans le cadre de ses prestations de délivrance de certificats.

Cette activité a pris fin définitivement le 30 septembre 2022 et ce document ne contient plus que des renvois. Certains produits continuent d'exister en marque blanche opérée par la société Sectigo. On pourra consulter les versions précédentes de notre DPC ici : <https://www.tbs-internet.com/CA/repository/>

Depuis le 1^{er} 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

Depuis le 30 septembre 2022 les certificats TBS INTERNET X509 client/email 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
X509 Email Novice TBS	Personal Authentication Certificate (Basic)
X509 Sign & Login TBS	
X509 Test Sign & Login TBS	
X509 Email Professionnel TBS	No longer available
X509 Test Email Professionnel TBS	
X509 Email Particulier TBS	
X509 Utilisateur TBS	EPKI Email

1.1 TBS INTERNET

La société TBS INTERNET a cessé son activité d'Autorité de Certification (AC) le 30 septembre 2022. Précédemment la société délivrait 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 occupait 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.

L'activité de courtier en certificats de TBS INTERNET se poursuit. 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 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

1.4 Hiérarchie de la PKI TBS INTERNET (pour mémoire)

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 (référéncés sous diverses appellations : UTN, AddTrust, USERTrust). La représentation de la PKI de TBS INTERNET ci-dessous illustre parfaitement la hiérarchie utilisée.

1.4.1 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 chaîne SSL (numéro de série = x, expiration = 1 an après la date d'émission)

1.4.2 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 chaîne SSL (numéro de série = x, expiration = 30 jours à 3 ans après la date d'émission)

1.4.3 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 chaîne SSL (numéro de série = x, expiration = 30 jours à 3 ans après la date d'émission)

1.4.4 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 chaîne 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 chaîne SSL (numéro de série = x, expiration = 30 jours à 6 ans après la date d'émission)

Ou pour les certificats 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 chaîne SSL (numéro de série = x, expiration = 30 jours à 4 ans après la date d'émission)

Ou pour les certificats 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 chaîne SSL (numéro de série = x, expiration = 30 jours à 6 ans après la date d'émission)

Rédaction du présent document

Ce document correspond à la version 1.14 de la DPC de TBS INTERNET, créée le 1 mars 2023 et signée par les membres de l'Autorité en charge de la politique de certification de TBS INTERNET.

Note de droits d'auteur

Copyright TBS INTERNET. Tous droits réservés.

Aucune partie de ce document ne peut être reproduite, inscrite ou introduite dans un système de consultation, voire transmise sous quelque forme que ce soit ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement ou autres) sans autorisation écrite de TBS INTERNET.