Conditions particulières - Certificats SSL/TLS (Boxis)

Version : 28.12.2025

La présente CP complète les Conditions générales de service (« CGS »). En cas de contradiction, la hiérarchie prévue à l'Article 1.4 des CGS s'applique.

> IMPORTANT - Hors périmètre / facturation Toute demande hors périmètre (p.ex. configuration, assistance applicative, migration, sécurité, coordination tiers, restauration/réversibilité, etc.) est traitée en Services Professionnels (CGSP) et facturée au temps passé selon le tarif et les modalités de l'Annexe - Frais de service, plus coûts tiers au réel.

Conformément à l'Article 5.7 des CGS, certaines actions demandées via Support peuvent être considérées comme sensibles (p.ex. révocation, ré-émission, changement de CSR/clé, changements d'éligibilité/validation) et nécessiter une approbation explicite avant exécution.

1. Objet / rôles

Les présentes CP s'appliquent à la fourniture de certificats SSL/TLS (p.ex. DV/OV/EV selon disponibilité) pour des noms de domaine et/ou services définis à la Commande.

Boxis agit en tant qu'intermédiaire ; l'émission, la validation et la révocation dépendent d'une Autorité de Certification (« AC ») et de ses politiques.

2. Validation / dépendance AC

Le Client fournit des informations exactes et réalise les validations requises (p.ex. validation de contrôle du domaine, vérification d'organisation, approbations email/DNS/HTTP selon le type de certificat).

L'AC peut refuser, suspendre, ou retarder une émission (p.ex. incohérence, suspicion de fraude, exigences supplémentaires, listes de blocage). Boxis n'est pas responsable des décisions et délais imposés par l'AC ou par un tiers habilité.

3. Clés privées / CSR / sécurité

Le Client génère et protège ses clés privées, CSR, mots de passe et fichiers associés. Le Client reste seul responsable de toute compromission (p.ex. vol de clé privée, serveur compromis) et des conséquences (p.ex. révocation, ré-émission, indisponibilité).

4. Installation / compatibilité

Le Client est responsable de l'installation et de la configuration du certificat sur ses systèmes (p.ex. serveurs web, reverse-proxy, load balancer, applications). Il lui appartient de vérifier la compatibilité (p.ex. chaîne/intermédiaires, SNI, protocoles/ciphers) et de maintenir ses systèmes à jour.

Toute assistance (installation, troubleshooting, configuration serveurs, tests) est susceptible d'être facturée en Services Professionnels (CGSP).

5. Renouvellement / expiration

Le Client est responsable du renouvellement et du maintien des moyens de paiement. Un certificat expiré peut entraîner une indisponibilité fonctionnelle (p.ex. alertes navigateur, refus de connexion). Les notifications éventuelles ne constituent pas une garantie.

6. Révocation / ré-émission / non-remboursement

En cas de révocation liée au Client (p.ex. informations inexactes, compromission, usage abusif), aucun remboursement

n’est dû. Sauf droit impératif, aucune annulation/remboursement n’est dû une fois l’opération initiée ou exécutée auprès de l’AC.