

Certificats SSL Wildcard

Les certificats Thawte® SSL Wildcard assurent le cryptage et l'authentification de plusieurs hôtes partageant le même niveau de sous-domaine (par exemple thawte.com, support.thawte.com et mail.thawte.com). Comparée à l'acquisition et au déploiement d'un certificat différent pour chacun de vos sous-domaines, l'utilisation de certificats Thawte Wildcard offre une solution simple, économique et d'une très grande souplesse. C'est pourquoi nous vous invitons à capitaliser sur ces certificats pour garantir à vos clients un transfert de données sécurisé en continu, quel que soit le sous-domaine auquel ils accèdent.

Avant d'opter pour l'efficacité d'un certificat Wildcard, il est important de bien comprendre les avantages d'un tel dispositif, mais également ses inconvénients et les risques potentiels associés. Pour déterminer si un certificat Wildcard correspond à vos besoins et s'intégrera parfaitement à votre environnement, vous devez tenir compte des éléments suivants :

- Les pages Web nécessitant l'utilisation de la technologie SSL EV (Extended Validation) ne peuvent pas être protégées à l'aide d'un certificat Wildcard. À la place, Thawte recommande d'utiliser des certificats SSL EV pour serveur Web sur les pages impliquant la saisie de mots de passe, d'informations d'identification personnelle, ou qui contiennent des composants d'e-commerce (panier d'achat, validation de commande, paiement, etc.).
- Le déploiement d'un même certificat Wildcard sur plusieurs sous-domaines et serveurs présente un risque inhérent : si l'intégrité d'un serveur ou d'un sous-domaine venait à être compromise, celle de tous les autres pourrait l'être également. Assurez-vous que votre environnement est doté d'un dispositif de sécurité multiniveau contre les menaces internes et externes.
- Le fait de n'avoir qu'un seul certificat simplifie sans aucun doute la gestion, mais les certificats Wildcard ne réduisent en rien les tâches d'administration liées au déploiement sur plusieurs sous-domaines ou serveurs. Par exemple, en cas de révocation d'un certificat Wildcard, les risques mentionnés précédemment persisteront jusqu'à ce qu'il ait été supprimé de tous les sous-domaines et serveurs sur lesquels il a été déployé.

Principaux avantages

Réduction des coûts d'administration et de déploiement grâce à la possibilité d'utiliser un seul certificat SSL pour plusieurs sous-domaines

Simplification extrême de l'installation et de la gestion des certificats en protégeant un nombre illimité de sous-domaines partageant un même de nom de domaine

Déploiement immédiat de la technologie SSL sur de nouveaux sous-domaines ou sur des sous-domaines qui ne bénéficient pas encore d'une protection, éliminant ainsi l'attente liée à l'émission de nouveaux certificats pour les serveurs correspondants tout en fournissant une solution pérenne

Réponse aux besoins d'administration des environnements riches en fonctionnalités qui nécessitent des communications client-serveur et serveur-serveur sécurisées, à l'intérieur comme à l'extérieur du pare-feu

Sérénité et confiance renforcée des utilisateurs grâce à l'authentification complète de l'entreprise identifiée sur le certificat

Prise en charge optimale de plus de 99 % des navigateurs pour PC et appareils mobiles, ce qui évite l'affichage de messages d'erreur susceptibles d'entamer la confiance des utilisateurs

Hausse de la valeur ajoutée grâce aux fonctionnalités exceptionnelles des certificats Thawte SSL : niveau de cryptage pouvant atteindre 256 bits, équipe de support avenante et assidue, et réémissions gratuites illimitées pendant toute la durée de vie du certificat

- Les certificats Wildcard imposent des limites sur le nombre de noms de domaine et de serveurs couverts. Pour protéger plusieurs domaines (par exemple thawte.com et thawte.fr), Thawte recommande l'utilisation de l'un de ses trois types de certificats SSL SAN (Subject Alternative Name). De plus, la licence d'un certificat Thawte SSL Wildcard permet de le déployer sur plusieurs sous-domaines, mais pas sur plusieurs serveurs ; une nouvelle licence est nécessaire pour chaque serveur supplémentaire.
- Certains navigateurs plus anciens ne prennent pas en charge les certificats Wildcard, ni le standard de cryptage de session SSL à 128 bits. Pour assurer la prise en charge des navigateurs plus anciens, Thawte recommande d'utiliser ses certificats SGC Supercerts afin d'étendre la protection SSL au plus grand nombre de visiteurs possible.

Pour en savoir plus, contactez nos conseillers commerciaux :

- Par téléphone
 - France : +33 1 57 32 42 68
 - Royaume-Uni : +44 203 450 5486
 - Afrique du Sud : +27 21 819 2800
 - Allemagne : +49 69 3807 89081
- E-mail : sales@thawte.com
- Visitez notre site Web à l'adresse : <https://www.thawte.fr>

Protégez votre entreprise et inspirez confiance à vos clients grâce à la sécurité renforcée des certificats numériques signés Thawte, pionnière de la sécurité en ligne à l'échelle planétaire. Stabilité, fiabilité, infrastructure éprouvée, support client irréprochable... en 17 ans, Thawte a su s'imposer comme le partenaire international de choix pour les entreprises du monde entier.