Les certificats SSL

Par Patrick Sentinel – 29a.ca

Les types de certificats SSL : Qui protège vraiment votre site web ?

Aujourd'hui, si votre site web n'a pas de certificat SSL, c'est un peu comme se balader en caleçon sur Internet. *Google* vous juge, vos utilisateurs prennent peur, et les hackers préparent déjà le barbecue pour vos données. Heureusement, le monde merveilleux des certificats SSL est là pour vous aider. Mais lequel choisir ? Plongeons dans cette jungle sécurisée avec humour !

1. Le certificat SSL DV (*Domain Validation*) – *Le fast-food* de la sécurité

- Validé en quelques minutes, sans vérification approfondie;
- Coût : pas cher, voire gratuit;
- Idéal pour les blogs, les petits sites vitrines et les pages perso.

Le **certificat DV** est l'équivalent du *fast-food* : rapide, pratique, mais pas franchement élaboré. Il suffit de prouver que vous possédez le domaine (généralement par un courriel ou un fichier à ajouter sur le serveur), et hop ! Votre site a droit à son petit cadenas vert. Mais attention, aucune vérification d'identité ici : un hacker pourrait aussi bien en obtenir un pour un site frauduleux. C'est mieux que rien, mais ce n'est pas la totale.

2. Le certificat SSL OV (*Organization Validation*) – La carte d'identité du web

- Vérification de l'entreprise nécessaire;
- Coût : modéré;
- Idéal pour les PME et les sites qui veulent un minimum de crédibilité.

Le **certificat OV** est comme une pièce d'identité officielle. L'autorité de certification (CA) vérifie que votre entreprise existe réellement avant de délivrer le certificat. Ça prend un peu plus de temps que le DV (quelques jours), mais au moins, vos visiteurs savent qu'ils ne sont pas sur un site louche monté en 5 minutes dans un sous-sol humide.

3. Le certificat SSL EV (*Extended Validation*) – La *Rolls-Royce* de la sécurité

- Vérification ultra-stricte de l'entreprise et de son existence légale;
- Coût : élevé;
- Idéal pour les banques, e-commerces et sites qui gèrent des transactions sensibles.

Avec un **certificat EV**, votre barre d'adresse affichera fièrement le nom de votre entreprise en vert (sur certains navigateurs). C'est un peu comme rouler en limousine blindée avec des vitres teintées : tout le monde sait que vous êtes sérieux. L'obtention de ce certificat implique une enquête minutieuse (presque aussi longue qu'un contrôle fiscal), mais finalement, vos visiteurs auront une totale confiance.

4. Le certificat SSL *Wildcard* – Le passe-partout de la sécurité

- Protège un domaine et tous ses sous-domaines;
- Coût : plutôt raisonnable;
- Idéal pour les sites avec plusieurs sous-domaines (blog, boutique, support…).

Si vous avez un site avec plein de sous-domaines (comme **blog.monsite.com**, **shop.monsite.com**, **support.monsite.com**), alors le **certificat *Wildcard*** est votre meilleur ami. Il couvre tout ce petit monde sous une seule et même protection, évitant ainsi d'acheter 50 certificats différents. C'est un peu comme un abonnement *Netflix* familial : tout le monde en profite sans payer plein tarif.

5. Le certificat Multi-Domaines (SAN) – La sécurité polyamoureuse

- Protège plusieurs domaines différents;
- Coût : un peu plus cher, mais rentable;
- Idéal pour les entreprises qui gèrent plusieurs sites.

Vous avez plusieurs domaines à sécuriser, comme **monsite.com**, **monautresite.net** et **encoreunsite.org** ? Plutôt que d'acheter un certificat pour chacun, optez pour un **certificat SAN (*Subject Alternative Name*)**, qui protège plusieurs domaines à la fois. C'est un peu comme avoir une seule clé qui ouvre toutes les portes de votre maison, de votre bureau et de votre cabane au fond du jardin.

6. Le certificat SSL Auto-Signé – L'arnaque maison

- Gratuit, mais sans validation officielle;
- Coût : 0 $ (mais coûte votre crédibilité);
- Idéal pour… euh, personne en fait.

Le **certificat auto-signé** est le certificat SSL du bricoleur du dimanche. Créé par votre propre serveur, il ne garantit absolument rien et déclenche une énorme alerte rouge sur les navigateurs, mettant vos visiteurs en panique totale. C'est un peu comme écrire soi-même son propre diplôme de médecine et essayer d'opérer des patients… Franchement, c'est le truc 'cheapo' des certificats, je ne recommande pas ce type de certificat.

Conclusion : Quel certificat SSL choisir ?

Tout dépend de vos besoins :

- **Un simple blog ou site perso ?** Un **DV** suffit.
- **Un site d'entreprise ?** Passez à l'**OV**.
- **Un site e-commerce ou bancaire ?** L'**EV** est recommandé.
- **Beaucoup de sous-domaines ?** Un ***Wildcard*** fera l'affaire.
- **Plusieurs sites à sécuriser ?** Optez pour un **Multi-Domaines (SAN)**.

Dans tous les cas, évitez l'auto-signé (sauf si vous aimez voir vos visiteurs fuir en courant). Bref, choisissez bien votre bouclier numérique et évitez de finir en caleçon sur Internet !
