Processus de passage d'un site en HTTPS

Méthodologie pour mise en place

Afin planifier une action de passage d'un site en HTTPS :

1. Lire la guideline sur les certificats SSL au préalable
2. Le client dispose-t-il déjà d'un certificat en interne pour son NDD ?
3. Le cas contraire, quel type de certificat faut-il recommander pour le client (cf doc)
    a. Site à transaction bancaire ? (=> niveau de sécurité et assurance)
    b. 1 ou plusieurs sous domaines (www.domaine, api.domaine, crm.domaine, etc..) (=> simple, ou wildcard si supérieur à 1 sous domaine)

4. Chiffrer par un lead dev la mise en place du certificat sur le site en question
5. Deviser l'opération :
    - Achat certificat (client ou nous-même en deuxième recours)
    - Configuration serveur
    - Réplication du site vers un preprod pour testing
    - Développement et paramétrage du site en https
    - Application et configuration des règles SEO
    - Suivi et conseil
    - Mise en ligne
6. Planifier l'opération en s'assurant que chaque personne puisse intervenir
    a. Acheter le certificat avant de demander d'effectuer les opérations sur le serveur
    b. Configurer le serveur d'hébergement + PRERPOD avant de demander au dév de travailler dessus
    c. Demander au dev de traiter le HTTPS avant de tester
    d. Demander au CDP de configurer les règles SEO avant de tester
    e. Tester le site avec un crawler avant de demander la MEL
    f. S'assurer qu'un devops est disponible pour la MEL

Guideline du SSL / HTTPS

Pourquoi passer au https

> Pour répondre aux exigences de Google (et Firefox) : Depuis l'arrivée de Chrome 56 le 27 janvier 2017, la mention "Non Sécurisé" apparaît à côté de l'URL de la page de connexion si le domaine n'est pas sécurisé par un certificat SSL.

https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html

L'utilisation du protocole sécurisé HTTPS vous permet d'intégrer le flux Google Shopping.

Le HTTPS sera bientôt exigé pour créer des pages AMP valides.

> Pour sécuriser les données de vos sites

Les certificats SSL protègent l'échange de données entre les navigateurs et vos sites internet. Le vol d'informations et d'identifiants lors de la consultation d'espaces privés est impossible.

> Pour rassurer les internautes

Le cadenas présent à côté de l'URL d'un site internet est un indice de confiance pour 53% des utilisateurs.

> Pour améliorer votre référencement naturel

L'utilisation du protocole sécurisé HTTPS est un critère pris en compte par l'algorithme de Google dans le référencement naturel SEO. En résumé, Google accorde un bonus aux sites sécurisés dans le classement des résultats.

Obtenir un certificat

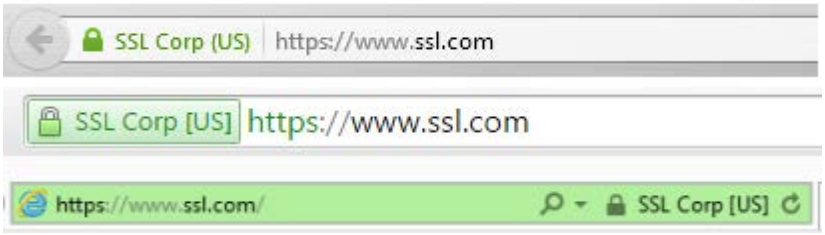
Il existe 3 types de certificats :

> Certificat à validation de domaine (DV) : l'autorité de certification vérifiera juste que vous êtes bien propriétaire du nom de domaine pour vous accorder le petit cadenas vert.

> **Certificat à validation de l'organisation (OV) :** vous devez prouver que vous êtes la personne morale détentrice du domaine à sécuriser et fournir des documents papier comme un extrait KBIS ou une attestation de domiciliation

> **Certificats à validation étendue (EV) :** Les informations que vous transmettrez sur votre organisation seront vérifiées (existence légale, physique, numéro de téléphone, adresse, activité, etc) et auditées chaque année.

Ce dernier type permet d'obtenir un affichage différent dans la barre du navigateur :



Activer le certificat sur l'hébergement

> Hébergement externe : faire une demande à l'hébergeur pour l'achat/l'activation/l'installation du certificat.
Par exemple ci-dessous la tarification de LinkByNet :

Installation d'un certificat SSL	80,00
Organisation SSL - 1 an	242 €
Organisation SSL - 2 ans	437 €
Organisation SSL Wildcard - 1 an	647 €
Organisation SSL Wildcard - 2 ans	1 166 €

> En interne : fournir la clé, le certificat, la durée de validité, le domaine pour mettre en place le certificat. Nous n'achetons pas le certificat, c'est au client de l'acheter. Le client peut se tourner vers komodo, globalsign let's encrypt, …

Opérations pour Mise en place

Checklist non exhaustive pour CDP

> Maillage interne des sites et modifications des URLS
> Modifier les urls sur les réseaux sociaux
> Recettage complet avec chrome de préférence (moins permissif)

SI e-commerce :
> Vérifier que les modules (per ex : Colissimo) ne comprennent pas d'URL à modifier.
> Modifications des URL dans la brique de paiement PREPROD/PROD (! aux urls de retours paiement)
> Refaire les tests de paiement test&prod.

Webmarketing

1. SEO
    a. Redirections http vers https
        i. Pages
        ii. Images
        iii. Js, …
        iv. Sur WordPress : https://es.wordpress.org/plugins/really-simple-ssl/
    b. Sitemap https avec uniquement les URLs https
    c. Robots.txt https
    d. Canonical de la version http vers https
        i. et vérifier que les autres sont en place : non-www vs. www; slash vs. non-slash…
    e. Search Console
        i. Mise en place version https et la définir comme favorite
        ii. Conserver la Search Console du http
        iii. Créer un groupe http + https pour suivre trafic global
        iv. Envoi du sitemap https dans la SC https
        v. Si besoin soumission de la Home Page pour accélérer l'exploration et l'indexation
        vi. S'il y en avait pour le http, reconfigurer les paramètres pour la version https
        vii. Paramétrage geolocal si pertinent
        viii. Si fichier de désaveu pour http, le resoumettre sur la SC Https
    f. Mise en place du suivi de positions https
    g. Maillage
        i. interne à modifier / vérifier

ii. externe à modifier si besoin (et si on a du temps vendu sur le sujet, sur un Top 10-20)

h. Crawler le site après migration pour vérifier les éventuelles erreurs, et vérifier la bonne indexation

2. Social Media
   a. Modifications des pages de profils media sociaux
      i. Ex. Youtube : Creator studio > Channel > Advanced
   b. Paramétrages Boutons de partage (Facebook and Google+ n'agrègent pas les Like des page HTTP et HTTPS)

3. Analytics : Reparamétrage du suivi : propriété + vue

4. Autres leviers à mettre à jour
   c. SEA
   d. Affiliés
   e. Campagnes en cours : display, …

Ressources :

http://www.journaldunet.com/solutions/seo-referencement/1192830-risque-benefices-migration-https/
https://www.theguitarlesson.com/guitar-lesson-blog/theguitarlessoncom-news/https-migration/
https://www.slideshare.net/AysunAkarsu1/https-the-road-to-a-more-secure-web-seocamp-paris
https://fr.semrush.com/blog/comment-reussir-sa-migration-seo/
https://www.semrush.com/blog/http-vs-https-how-security-affects-your-seo/
http://www.aleydasolis.com/en/search-engine-optimization/http-https-migration-checklist-google-docs/

Actions à mener sur les sites

Généralités

> Rediriger en HTTPS (301) via htaccess :
http://stackoverflow.com/questions/32805448/htaccess-redirect-domain-to-https-subdomain-with-parameter-to-http

> Changer toutes les URLs dans votre base de données en HTTPS. Attention aux données sérialisées, un simple search&replace cassera la serialisation

> Vérifier et remplacer si besoin tous les appels à des services externes (ex : vidéo embed youtube, code de tracking, …). Toutes les urls doivent également être en https pour respecter la same origin policy :

https://developer.mozilla.org/fr/docs/Web/JavaScript/Same_origin_policy_for_JavaScript

> Tester votre site en HTTPS (plutôt sur chrome car moins permissif que Firefox à l'heure actuelle, vérifie notamment en plus les actions des formulaires)

> Activer HTTP Strict Transport Security (HSTS):

Intime à l'agent utilisateur de remplacer automatiquement tous les liens non sécurisés par des liens sécurisés

Strict-Transport-Security: max-age=16000000; includeSubDomains; preload

> Inscription HSTS preload list :

On peut inscrire son nom de domaine sur une liste de pré-chargement HSTS preload list pour demander son inclusion dans cette liste. Cette liste est utilisée par les navigateurs modernes. En clair, si votre site est dans cette liste, les navigateurs utiliseront HTTPS de suite et quoi qu'il arrive.

https://hstspreload.org/

Prestashop

Préférences > SEO > URL puis dans URL DE LA BOUTIQUE, dans le champ DOMAINE SSL rajouté l'url de votre site sans le HTTPS uniquement : www.votresite.tld

Rendez-vous ensuite dans Préférences > Paramètres Généraux

Puis tout en haut dans Activer le SSL cliquez sur : "Cliquez ici pour utiliser le protocole HTTPS avant d'activer le mode SSL."

Une page s'ouvrira avec votre site en HTTPS.

Retournez dans Préférences > Paramètres Généraux et mettre sur OUI : -- Activer le SSL -- Forcer l'utilisation de SSL pour toutes les pages

Wordpress

TYPO3