Des sites en https au pic ?

Qu'est-ce que https ?

Un site web en https offre une meilleure sécurité à ses utilisateurs, parce que :

- Les communications sont cryptées
- Qui dit cryptage dit clés de cryptage. Le serveur va donc nous faire parvenir ses clés de cryptage, en utilisant le cryptage asymétrique[1]. Mais comment être sûr que nous ayons la clé du serveur, et pas la clé d'un méchant pirate qui va nous espionner ? (« homme du milieu »[2]). Le serveur doit être authentifié, et cela se fait en utilisant des « certificats électroniques ».

Pourquoi un certificat ?

Si je veux être sûr de l'identité de la personne à qui je vais confier un secret, je vais lui demander sa carte d'identité. Je vais vérifier les informations qu'elle contient, en particulier la date de fin de validité. Je fais confiance à l'exactitude des renseignements se trouvant sur la carte, parce que je fais confiance à l'État qui en assure la gestion[3] L'État joue ici le rôle de « tiers de confiance » : un tiers qui s'invite dans la relation entre deux personnes, en qui les deux ont confiance, et grâce à qui elles se font mutuellement confiance.

De même, un certificat électronique est « certifié » par une autorité de certification, c'est-à-dire une personne, en l'occurrence souvent une société commerciale[4], qui gère de manière rigoureuse les certificats de ses « clients ». Le certificat permet d'assurer au navigateur que le site qu'il visite est bien celui correspondant au nom de domaine.

Le certificat, comme une carte d'identité, a une date de péremption.

Pour que les sites du pic puissent fonctionner en https, il nous faudra certifier tous les noms de domaines correspondants. Il faudrait donc un certificat pour le site https://truc.le-pic.org et un autre pour le site https://machin.le-pic.org, plus un pour https://www.bidule.fr (si ce site est hébergé par le pic) ?

C'est là que ça se complique : pour des raisons techniques liées à apache, il n'est pas possible d'installer plusieurs certificats sur un même serveur web. Il faudra donc disposer d'un seul certificat, multi domaines (capable de garantir l'authenticité de plusieurs domaines). Ce qui signifie qu'à chaque fois qu'on ajoute un nom de domaine (une nouvelle association par exemple) il faut refaire le certificat ! Tout ça est bien compliqué et coûte cher. Sauf qu'il y a depuis peu une nouvelle possibilité.

---

1 https://fr.wikipedia.org/wiki/Cryptographie_asym%C3%A9trique
2 https://fr.wikipedia.org/wiki/Attaque_de_l'homme_du_milieu
3 je sais par ailleurs qu'il est possible que la carte d'identité soit un faux, mais dans les situations de la vie courante j'accepte ce risque).
4 l'internet est un truc international, il n'est pas chapeauté par un État

Pour quoi faire et pourquoi maintenant ?

Le fait que la liaison soit cryptée empêche les éventuels « indiscrets » de lire vos communications: pas très utile lorsqu'il s'agit d'un site web public, mais important lorsque vous envoyez des articles sur votre CMS… et tout particulièrement au moment où vous tapez votre mot de passe ! Encore plus important si vous utilisez des outils comme galette ou autres logiciels de gestion en ligne.

Les « géants » de l'internet (google et Cie) essaient actuellement de pousser les fournisseurs d'accès internet vers le https : par exemple Google a annoncé récemment qu'il accorderait plus d'importance aux sites en https lors du référencement de sites[5]. Bref, « c'est la tendance », le web de l'avenir sera (sans doute) essentiellement https, pourquoi attendre ?

Des adhérents au PIC nous l'ont demandé à l'Assemblée Générale 2015

Une nouvelle Autorité de Certification vient d'apparaître : letsencrypt[6], automatique et gratuite (parce qu'automatique). Donc tout ça devrait pouvoir se simplifier et ne pas ruiner le pic !

letsencrypt est-elle digne de confiance ?

Letsencrypt est soutenu par les « grands noms » de l'internet[7], ce n'est pas « un truc de geeks ». Pour google, c'est un des outils qui permettra que l'ensemble du web devienne crypté.

Bien qu'automatisée, l'autorité de certification essaie de s'assurer qu'elle ne génère pas des certificats pour « n'importe qui » :

- Vérification que le demandeur contrôle bien le nom de domaine
- Limites très strictes du taux de certificats produits pour un domaine donné (5 pour un délai de 7 jours glissants actuellement !)
- Les certificats sont valides 90 jours, donc si par malchance un certificat « pirate » est émis, cela ne devrait pas durer trop longtemps.

Propositions de règles pour le pic :

Dans un premier temps, le mode https sera proposé **seulement** aux associations qui en feront la demande.

Seules la ou les adresses « de production » seront associées à un certificat :

- asso.le-pic.org possède un certificat, https://asso.le-pic.org fonctionne donc normalement
- https://asso-v1.le-pic.org n'en possède pas : le navigateur enverra une fenêtre d'alerte sur cette adresse car il ne peut pas s'assurer de l'authenticité de cette adresse, mais le cryptage sera quand-même effectif.

Le serveur sera configuré de manière que l'ancienne adresse http://asso.le-pic.org fonctionne

5 http://www.zdnet.fr/actualites/google-ameliore-le-referencement-des-sites-en-https-39804689.htm
6 https://letsencrypt.org
7 https://letsencrypt.org/sponsors/

toujours : elle générera tout simplement une redirection vers l'adresse https[8]

Les certificats seront renouvelés tous les 60 jours : un script sera exécuté toutes les nuits, et le certificat sera renouvelé dès lors qu'il ne lui restera plus que 30 jours à vivre, ou moins

Les appels à letsencrypt seront intégrés aux scripts de création de sites web, afin que les administrateurs du pic puissent s'approprie facilement les commandes.

Attention, letsencrypt est encore en version bêta, nous n'avons pas de recul dessus. Pour l'instant ça marche, mais nous ne pouvons pas garantir qu'il n'y aura jamais aucun problème ! Les associations doivent en être conscientes.

8 Allez donc visiter le site : http://www.le-pic.org