TD 6: Certification & Vie privée

1 Certificats en `PyCa` et `OpenSSL`

Cet exercice a pour but de créer un certificat auto-signé en passant par l'intermédiaire d'une requête en signature du certificat (*certificate signing request*) en utilisant la librairie `Cryptography` de `Python` ainsi qu'avec `OpenSSL`.

1.1 En `Python`

(1) Commencez tout d'abord par créer une clé RSA de taille suffisante (au moins 1024 bits) et enregistrez-la sur le disque (extension `.pem`).

(2) En vous inspirant de la documentation, engendrez la requête en signature du certificat (*certificate signing request*) en remplissant bien les champs X509 et enregistrez-la (extension `.csr`).

(3) Générez le certificat auto-signé de la requête en signature du certificat (qui dépend de la clé RSA et du fichier `.csr` ou de son objet correspondant) et enregistrez-le (extension `.crt`).

1.2 Avec `OpenSSL`

(1) En utilisant la clé RSA enregistrée auparavant et le fichier `.csr`, engendrez le certificat auto-signé de la requête en signature du certificat et enregistrez-le sur le disque (extension `.crt` et sous un autre nom que celui généré avec `PyCa`).

(2) Observez les différences entre les deux fichiers en les affichant par la commande `OpenSSL` adéquate.

(3) Vérifiez vos certificats auto-signés par `OpenSSL`.

Que faudrait-il faire pour que ce certificat soit reconnu par votre système ou par votre navigateur?

La seconde partie de ce TP a pour objectif d'illustrer les notions de traçabilité et d'identification lors des navigations sur Internet.

2 Vie privée

2.1 Vous documenter...

Visitez et regardez comment protéger votre vie privée sur le site `https://www.eff.org/issues/privacy` pour trouver des informations relatives à la protection de la vie privée. Renseignez-vous aussi sur ce que signifie l'*intérêt légitime* qui vous est proposé dans les bannières de cookies, par exemple sur `https://www.cnil.fr/fr/les-bases-legales/interet-legitime`.
Vous pourrez aussi consulter l'article sur les traceurs sur le site du Monde.

2.2 Voir vos traces

Allez sur la page `http://www.anonymat.org/vostraces/index.php` et notez les informations relatives:

- à votre IP;
- à votre navigateur;
- les informations sur les pages visitées auparavant.

2.3 Où êtes-vous?

En utilisant votre adresse IP, tentez de vous géolocaliser en utilisant par exemple `https://www.geolocation.com/fr` et en interrogeant la base `whois` (accessible depuis le site de géolocalisation).

2.4 Etes-vous identifiable?

Visitez la page `https://amiunique.org` pour visualiser les informations relatives à votre navigateur et déduisez-en si vous êtes identifiable par l'empreinte de votre navigateur. Si c'est le cas, essayez de savoir pourquoi en retournant à la page de garde du site.
Vérifiez si vous autorisez les cookies tiers ou non. Désactivez les cookies tiers le cas échéant.
Vérifiez si vous avez une option "do not track" et si vous pouvez l'activer.
Faites un tour par la page "Statistics" pour voir où vous vous situez et regardez les conseils et outils pour améliorer votre vie privée.

2.5 Etes-vous traçable?

Visitez un site de presse. Avez-vous des contenus sponsorisés? Essayez de trouver par quelle agence et cherchez des informations sur celle-ci.
Essayez de visualiser le contenu des cookies. Voir par exemple pour Firefox ou pour chrome.
Si vous ne l'avez pas déjà fait, ajoutez le plugin "ghostery" ou "adBlock" à votre navigateur et refaites la visite précédente. Observez-vous une différence? Pouvez-vous dire combien de traceurs ont été bloqués?
Votre empreinte sur `https://amiunique.org` a-t-elle été modifiée?

2.6 Vous protéger

Bloquez tous les cookies, installez les plugins uBlock, Ghostery, Disconnect, Privacy Badger et vérifiez les résultats avant et après (ces plugins ne sont pas tous disponibles selon les navigateurs).
Attention aussi à l'évolution de ces plugins. Voir ici.
Vous pouvez également utiliser les navigateurs "Brave", "Iridium" ou "LibreWolf" qui contiennent beaucoup de ces protections de façon native, ou pour affiner votre choix vous référer au site de Privacytest.