Sécurité - TP n°2 - Exercice 3

1 - Quelle est la différence technique entre les certificats X509v3 et les couples de clés GNUPG ?

Le différence est que dans le système de toile de confiance, un certificat peut être signé par plusieurs autres pairs de confiance. X509 gère une chaine de confiance, ou chaque certificat est signé par un pair de plus haut niveau.

La seconde est que la confiance dans GNUPG n'est pas "transitive". C'est à dire que si A fait confiance à B, et B fait confiance à C. A ne fera pas confiance à C. Contrairement à X509, si l'on fait confiance au certificat racine, on fait alors confiance à tout les certifiacts qu'il aura signé, ou tout ceux qui possèdent ce certificat racine dans leur chaine de confiance.

2 - Quel mécanisme permet de vérifier l'authenticité d'un certificat X509v3 ?

Les certificats X509v3 reposent sur une chaine de confiance. C'est à dire que chaque certificat est signé par avec le certificat d'une autorité de certification. Ce certificat de l'autorité de certification peut être lui même signé par un certificat de plus haut niveau. Cela forme une chaine de confiance. À la base de la chaine, on retrouve les certificats racines. Ces certificats racine sont des clés publiques non-signés ou auto-signés. Les logiciels gardent en mémoire une copie de ces certificats pour vérifier l'autenticité des certificats de plus bas niveau.

3 - Quelles sont les limites d'utilisation et les contextes d'usage de GnuPG ?

GnuPG a du sens pour une utilisation personnelle. Chiffré des échanges personnels, des documents, etc... La principale limite est le mécanisme de la toile de confiance derrière les certificats. En effet, pour qu'un certificat soit considéré comme "de confiance", il faut que l'utilisateur définisse manuellement à quels autres utilisateurs il fait confiance (dont il aurrait vérifié que l'identité corresponde à sa clé publique). Ce système n'est pas très pratique quand il sagit d'échanger avec des acteurs "inconnus", comme des site web par exemple.

4 - Quels sont les différentes contextes d'utilisation d'un certificat X509v3 ?

Au contraire, les certificats X509v3 se basent sur une chaine de confiance. Ce qui a beaucoup de sens pour les usages comme l'envoi de mail ou la navigation sur internet.

5 - Quelle confiance peut-on accorder à l’usage des certificats X509v3?

La confiance repose entièrement sur l'authenticité des certificats racine enregistré dont dispose l'utilisateur. Dans le cas ou ces certificats seraient corrompu, il ne pourrait plus avoir de confiance avec tout le reste des certificats.

6 - Que penser de Let's Encrypt ? Avantages/inconvénients/limites.

Let's encrypt permet de générer des certifiacts signés facilement. L'inconvénient principal est que l'on ajoute un acteur à qui faire confiance en plus : let's encrypt. En ajoutant un outil supplémentaire, on est pas sur que celui-çi est de confiance. Cela reste utile pour un petit site internet, afin de le configurer rapidement.