Signatures cryptographiques

Une signature permet d'identifier que quelqu'un a bien écrit quelque chose. Une signature doit être authentique, non falsifiable, non réutilisable. De même, un document signé ne peut pas être modifié et une signature ne peut pas être reniée.

Il faut pouvoir faire toutes ces propriétés dans les signatures numériques (cryptographiques).

Avec de la cryptographie symétrique

Pour faire un système de signature avec une seule clé secrète, il faut trois acteurs, le signataire, le destinataire et un tiers de confiance. C'est le tiers de confiance qui donne toute sa sécurité à la structure.

Chaque acteur partage une clé avec le tiers de confiance. Ainsi lorsque le signataire va partager le document avec sa clé au tiers de confiance.

Le tiers de confiance peut donc confirmer la signature puisque qu'il connait la clé secrète. Le tiers de confiance peut donc ajouter une certification sur le document et le signer en utilisant la clé partagée avec le destinataire.

Le destinataire peut donc ensuite valider que le tiers de confiance a authentifié la signature et donc considérer la signature comme correcte, car le tiers de confiance a utilisé sa clé.

Le problème ici est que toute la sécurité du système réside dans le tiers de confiance, donc si le tiers de confiance est compromis, toutes les signatures sont compromises.

Avec de la cryptographie asymétrique

Avec de la cryptographie asymétrique, on a uniquement besoin du signataire et du destinataire. Le destinataire connait la clé publique du signataire. Le rôle d'un potentiel tiers de confiance ici est seulement d'authentifier le propriétaire de la clé (cela n'a donc besoin d'être fait qu'une seule fois).

Nous avons vu que lorsque quelque chose est chiffré avec une clé publique, seule la clé privée peut la déchiffrer. Mais à l'inverse, lorsque quelque chose est signé avec une clé privée, elle peut être validée par les clés publiques.

La procédure de signature équivaut globalement à appliquer l'algorithme de déchiffrement sur le texte à signer. Ainsi, il suffira au destinataire de chiffrer le résultat pour retrouver le texte d'origine.

Systèmes de confiances

Certificats numériques X509

Les certificats numériques x509 lient une clé publique à une identité (nom de domaine, adresse email, etc) en utilisant une signature cryptographique.

Toute personne faisant confiance au tiers connait la clé publique de ce dernier afin de pouvoir vérifier les certificats. C'est notamment cela qui est utilisé sur internet pour vérifier les connexions HTTPS. Le navigateur possède une liste de clés publiques de tiers de confiances pour vérifier les certificats.

Certains tiers de confiances offrent leurs services de vérification gratuitement, c'est par exemple le cas de "Let's Encrypt", cependant la vaste majorité sont payants, mais ont l'avantage d'offrir une vérification beaucoup plus rigoureuse.

Let's Encrypt ne fait que vérifier que la demande de certificat est bien faite depuis une machine sous le nom de domaine demandé, alors que d'autres tiers de confiance vont aller se renseigner sur l'entreprise et l'appeler pour avoir une confirmation de l'authenticité de la demande.

Système de PGP (Pretty Goog Privacy)

C'est un système à clé publique sans tiers de confiance. L'identité des personnes est garantie de manière transitive.

Ainsi, si Alice connait Bob, elle peut certifier sa clé publique en la signant. Bob peut alors partager la clé signée par Alice. De cette manière, toute personne faisant confiance aux fréquentations d'Alice pourra faire confiance à Bob en vérifiant la signature.

Revision #2
Created 6 January 2024 17:26:08 by SnowCode
Updated 6 January 2024 17:48:48 by SnowCode