Retour sur la version actuelle des signatures

Signature des fichiers par LoGeAs Web jusqu'à la version 9.4

Nos remerciements à Flavien FENET-GARDE pour le développement initial de cet outil dans le cadre de son stage final de “Titre Développeur Logiciel”, et pour le partage du texte de son rapport dont se document s'est inspiré

Problématique

La problématique initiale de la signature est d'authentifier avec certitude l'auteur d'une information et de s'assurer que celle-ci n'a pas été modifiée depuis sa création.
Pour cela on peut utiliser un algorithme de cryptographie à clef asymétrique : en effet ce type d'algorithme possède deux clefs, une clef privée et une clef publique. Le principe initial est de crypter avec la clef publique et de décrypter avec la clef privée, afin que tout le monde puisse envoyer des données cryptées, mais que seul le destinataire prévu puisse les lire. La signature utilise ces propriétés pour obtenir exactement l'inverse : Si on utilise la clef privée pour crypter et la clef publique pour décrypter, seul l'émetteur peut envoyer des données, mais tout le monde peut les lire. En effet, une clef publique n'étant associée qu'à une seule clef privée, qui n'est pas déductible depuis la clef publique, si l'émetteur d'une clef publique est connu, toute donnée décryptable avec cette clef a été encryptée avec sa clef privée, et il en est donc probablement l'émetteur (sauf cas particulier d'attaque cryptographique).

Choix technologique

L'algorithme utilisé par le logiciel de signature de Logeas est **RSA en 2048 bits en mode CBC (Cipher Block Chaining)** (Voir l'article Wikipédia), il serait difficile d'expliquer ici le fonctionnement de ce type de codage.

La signature mise en place ne concerne pas l'intégralité des données chiffrées, mais seulement leur empreinte. Signer un document entier serait la solution la plus simple, cependant ce n'est absolument pas optimisé, car une signature n'étant rien d'autre que des données encryptées, la taille de la signature serait égale à la taille des données encryptées. Insignifiant pour un fichier texte brut, mais inenvisageable pour des dossiers.
Le fait de rendre accessible directement les données encryptées pourrait également rendre l'intégrité de la signature vulnérable à une attaque cryptographique visant à forger une signature valide pour des données, à partir de signatures et de données existantes.
Pour contrer ces deux problèmes majeurs, une solution existe : le hachage. C'est une fonction réductrice qui nous permettra de calculer un « hash » qui est une empreinte des données qu'on lui a envoyé. En effet ce n'est qu'une empreinte, bien que la fonction soit déterministe, elle est impossible à inverser en raison d'une perte d'information induite volontairement.

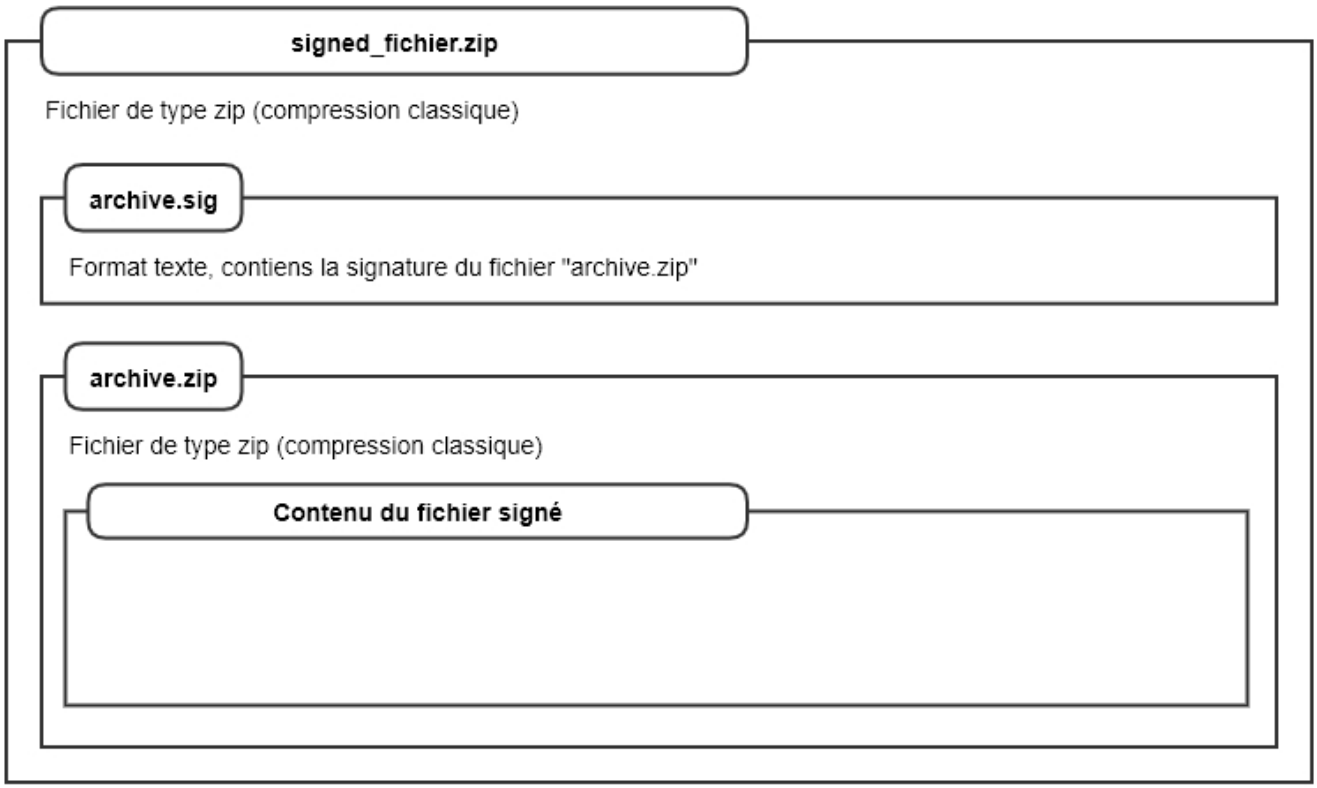
Bien que ce hash ne nous permette pas de récupérer les informations initiales, il va nous permettre de les identifier avec certitude : en effet les risques de collision (que deux données différentes

donnent le même hash) sont faibles, et les mêmes données donneront toujours le même hash. Afin de réduire la taille de notre signature, nous allons donc hasher les données avant de signer le hash final, ceci nous permettra effectivement de confirmer l'intégralité du document sans nécessairement conserver l'intégralité des données du document original.

Logeas utilise comme fonction de **hachage l'algorithme SHA-384**. Celle-ci fait partie de la famille SHA-2 (Secure Hash Algorithm) qui ont été conçues par la National Security Agency des États-Unis (NSA), sur le modèle des fonctions SHA-1 et SHA-0, elles-mêmes fortement inspirées de la fonction MD4 de Ron Rivest (qui a donné parallèlement MD5). Telle que décrite par le National Institute of Standards and Technology (NIST), elle comporte les fonctions, SHA-256 et SHA-512 dont les algorithmes sont similaires mais opèrent sur des tailles de mot différentes (32 bits pour SHA-256 et 64 bits pour SHA-512), SHA-224 et SHA-384 qui sont essentiellement des versions des précédentes dont la sortie est tronquée, et plus récemment SHA-512/256 et SHA-512/224 qui sont des versions tronquées de SHA-512. Le dernier suffixe indique le nombre de bits du haché (Voir l'article de Wikipédia).

Architecture des fichiers signés par LoGeAs Signature

Un fichier signé par LoGeAs Signature est un conteneur au format zip dont la structure est.



(le format source de cette image est dans le dossier de certification)

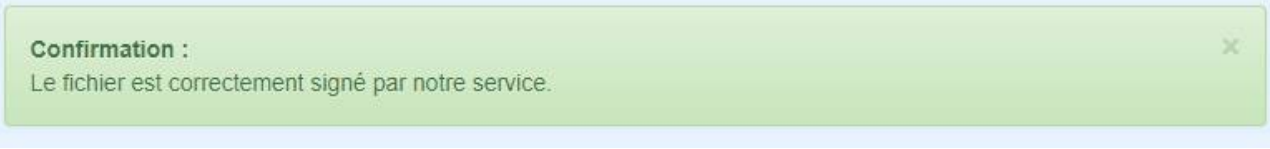
Architecture des fichiers signés par LoGeAs Signature

Manipulation des fichiers signés

Vérifier que le fichier est conforme à sa signature

1. se connecter sur l'interface https://monespace.logeas.fr en utilisant votre compte habituel
2. sur la page d'accueil vous trouverez un bloc "Signature"

3. Il suffit d'utiliser le bouton "choisir un fichier" pour le charger puis sur "Vérifier"
4. Après vérification la plate-forme donne la réponse en haut de l'écran



Extraire la partie "utile"

LoGeAs Web dispose d'un menu permettant d'extraire facilement la partie utile d'une archive signée "Administration\Exporter l'archive d'un fichier signé par LoGeAs-Signature"

Récupération des certificats