Signer mes articles avec PGP

Jacques BEHAEGEL, le 11 oct. 2026

Après l'article de Baptiste sur les usages de PGP sur le média Sans Dépendances, j'avais envie de voir comment l'utiliser concrètement pour signer mes propres articles.

Quand je publie sur mon blog ou ici, mon nom apparaît sous le titre et l'adresse du site permet de savoir où je me trouve. Mais ça ne prouve pas grand-chose techniquement. Une page peut être copiée, un compte WordPress compromis ou un texte modifié après sa publication.

Je me suis demandé si je pouvais utiliser ma clé PGP pour apporter une garantie supplémentaire. Pas pour empêcher quelqu'un de reprendre mes articles, mais pour permettre aux lecteurs de vérifier qu'un document correspond bien à celui que j'ai écrit.

Donner un usage à ma clé

J'avais déjà une clé PGP associée à mon compte Proton. Je l'utilise pour mes échanges et mes signatures, mais je n'avais pas encore trouvé d'usage particulier pour mon blog.

Ajouter simplement une mention sous mes articles n'aurait rien prouvé. Il me fallait une vraie signature cryptographique, vérifiable indépendamment de WordPress.

Le principe est assez simple, je signe un document avec ma clé privée, puis n'importe qui peut vérifier cette signature avec la clé publique correspondante. Si le document est modifié après la signature, la vérification échoue.

Pourquoi passer par un PDF ?

Mon blog est sous WordPress. Les articles sont donc des pages web, avec leur mise en forme, le thème et les différents éléments ajoutés par le site.

Signer directement une page HTML serait assez contraignant. WordPress peut en modifier la structure par une mise à jour du thème par exemple, et le contenu affiché dans le navigateur ne correspond pas forcément à un fichier stable que je pourrais faire vérifier.

J'ai donc choisi de conserver mes articles en ligne et de leur associer une version PDF signée.

Je pars de mon document original, je l'exporte en PDF, puis je vérifie le résultat avant de le signer. Le PDF garde une présentation stable et reste facile à lire ou à télécharger. C'est aussi un fichier que le lecteur peut conserver sur son ordinateur et vérifier plus tard, même si la page web a changé.

La signature ne porte pas directement sur la page WordPress. Elle concerne le PDF que je mets à disposition. Si je modifie ensuite l'article en ligne, je dois aussi mettre à jour le PDF et sa signature pour que les deux versions restent cohérentes.

Signer avec Kleopatra

Je n'ai pas eu besoin de programmer quoi que ce soit pour réaliser cette opération. J'utilise Kleopatra, l'interface graphique qui permet notamment de gérer ses clés PGP et de signer des fichiers.

Je sélectionne le PDF, je choisis ma clé et je lance une signature détachée, sans chiffrement. Le document reste donc lisible par tout le monde.

Kleopatra produit alors un fichier de signature séparé, avec l'extension .sig. Je conserve les deux fichiers : le PDF et sa signature.

La signature est liée au contenu exact du document au moment ou j'effectue l'opération.
Si quelqu'un modifie le PDF, même sans changer son apparence de manière évidente, la vérification ne fonctionnera plus. Le lecteur n'a pas besoin de me faire confiance sur parole, il peut effectuer lui-même le contrôle avec ma clé publique.

Comment vérifier un article signé ?

Le lecteur télécharge le PDF et le fichier .sig, puis vérifier la signature à partir des deux fichiers.



Le logiciel indique si la signature correspond au document et quelle clé a servi à la produire. Si le PDF a été modifié depuis sa signature, le contrôle échoue.

Il reste une question, comment savoir si la clé utilisée est bien la mienne ?

Une signature valide prouve une chose, que le fichier a été signé avec la bonne clé privée. Mais elle ne prouve pas à elle seule que cette clé m'appartient vraiment.

C'est pour ça que j'affiche aussi l'empreinte de ma clé publique sur mon site et ma page Masto. Elle permet de vérifier qu'on utilise bien la clé que j'annonce. Pour aller plus loin, on peut comparer cette empreinte avec une source indépendante, par exemple la clé publique associée à mon adresse Proton.

C'est d'ailleurs là que touchent les limites d'un contrôle fait uniquement sur le site. Si un pirate prend la main sur mon blog, il peut très bien remplacer mon PDF, le signer avec sa propre clé et afficher son empreinte à la place de la mienne. Pour quiconque vérifie uniquement les fichiers du site, la signature aura l'air parfaitement valide.

D'où l'intérêt d'une source externe. En cas de doute, vous pouvez directement vérifier l'empreinte de ma clé via mon adresse Proton (que j'utilise aussi hors du blog) ou sur mon compte Masto. Et pour que ce soit vraiment carré, le mieux reste que je vous réponde par un mail lui-même signé avec cette même clé PGP.

Ce que ça garantit, et ce que ça ne garantit pas

Il ne faut pas non plus lui faire dire plus qu'elle ne peut.

La signature garantit seulement l'intégrité du PDF, pas la véracité de ce que j'écris.

Elle ne prouve pas non plus la date réelle de publication et ne protège pas mon site contre un piratage. Si je corrige une coquille dans WordPress sans refaire le PDF et sa signature, les deux versions ne correspondront plus.

C'est une façon de vérifier l'origine d'un document et de détecter une modification, rien de plus.

Une étape de plus à chaque publication

Pour le moment, je dois exporter le PDF, le signer avec Kleopatra, puis publier le document et sa signature dans WordPress. Ce n'est pas automatique, mais la procédure reste raisonnable pour un article que je souhaite conserver comme référence.

Je ne cherche pas à imposer cette vérification à tout le monde. Les lecteurs peuvent continuer à lire mes articles comme avant. Ceux qui veulent vérifier le document disposent simplement de deux fichiers et de ma clé publique.

C'est un petit usage supplémentaire de ma clé PGP, et une façon assez concrète de mettre en pratique un outil dont on parle souvent sans forcément savoir quoi en faire.

Si le sujet vous intéresse ou vous donne envie de partager votre expérience, venez en discuter avec moi dans les commentaires ou directement sur mes réseaux. Je serai ravi d'échanger avec vous !