Horus metatime

Service d'horodatage

Lors d'échanges dématérialisés, internes ou avec leurs clients ou leurs partenaires, les organisations doivent pouvoir assurer que certaines transactions ou certains évènements ont eu lieu avant un instant donné. L'utilisation d'une contremarque de temps qui comporte une date et une heure sûres associées à un document apporte un élément de preuve. Atos, acteur européen de la sécurité, propose metatime, un service d'horodatage pour fournir des contremarques de temps.

Le succès des transactions dématérialisées et de l'archivage électronique repose sur un principe fondamental : la capacité de pouvoir démontrer avant quel instant des transactions ont eu lieu ou bien des documents ont été archivés.

Cette démonstration est possible grâce à l'usage de contremarques de temps constituées d'un ensemble de données signées comprenant :

- une date et une heure (UTC time);
- une empreinte calculée par une fonction de hachage (ex : SHA1, SHA256);
- l'identifiant de l'unité d'horodatage (TSU) qui a produit la contremarque de temps.

Une réponse à des contextes variés

Dans le cas de transactions électroniques signées, une contremarque de temps peut être apposée sur la signature électronique, ce qui permet de démontrer que celle-ci a été effectuée avant la date et l'heure figurant dans la contremarque de temps. Cette date et cette heure peuvent ensuite être comparées avec la date de fin de validité du certificat du signataire et, si le certificat a été révoqué, avec la date de révocation du certificat pour démontrer la validité de la signature électronique.

Dans le cas d'un archivage électronique de documents, une contremarque de temps peut être apposée sur le document afin de démontrer que celui-ci a bien été archivé avant la date et l'heure figurant dans la contremarque de temps. Une fois archivé, tout changement au document sera détecté.

Les contremarques de temps sont générées conformément à une politique d'horodatage qui définit principalement les fonctions de hachage acceptées et les algorithmes utilisés.

Metatime propose une ou plusieurs unités d'horodatage, gérées par une Autorité d'Horodatage et mettant en œuvre une politique d'horodatage. Pour fournir les contremarques de temps, metatime met en œuvre le protocole d'horodatage défini par la norme RFC 3161. La gestion de metatime se fait au moyen d'interfaces web, ce qui la rend accessible depuis tous les navigateurs web.

Atos, acteur européen de la sécurité

Leader européen de la sécurité intégrée, Atos a développé une expertise unique de la sécurité des systèmes d'information, conjuguant ses savoir faire de conseil, d'intégrateur et d'expert des technologies de confiance.

Les fonctionnalités de metatime

Les composants de metatime

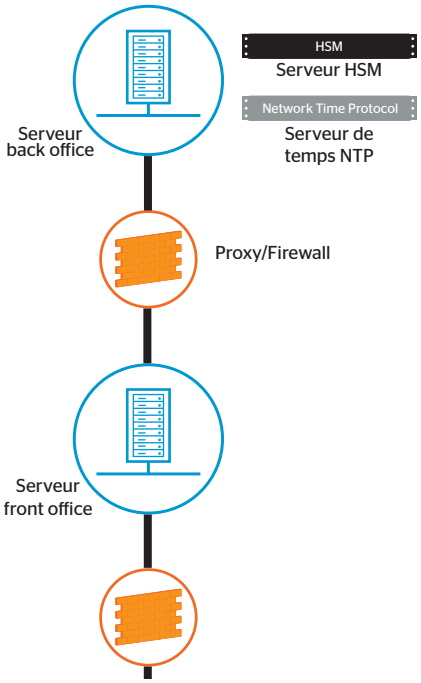
Metatime est composé d'un serveur front office et d'un serveur Back Office.

Le serveur front office

Le serveur front office sert d'interface avec les applications clientes et tient à jour un log des demandes et des réponses. La présence d'un serveur Front Office peut être optionnel lorsque le service n'est pas exposé sur Internet.

Le serveur back office

Le serveur back office produit des contremarques de temps en conformité avec une politique d'horodatage. Il utilise un HSM (Hardware Security Module), pour protéger la clé privée de signature, et une référence de temps synchronisée avec le temps UTC (Universal Time Coordinated).

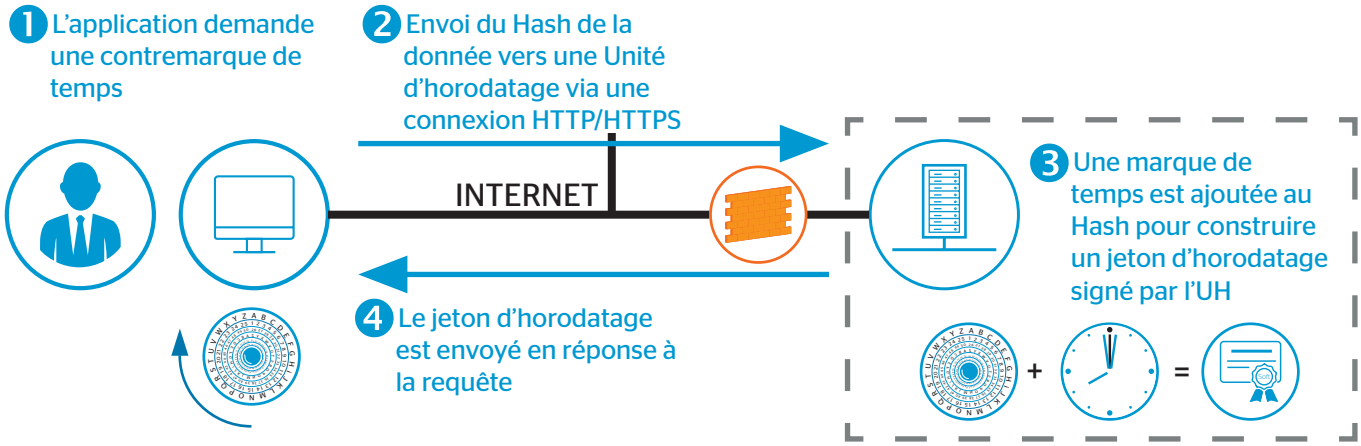


L'administration de metatime

Metatime permet de définir tous les paramètres des politiques d'horodatage. Chacune d'entre elles est supportée par une Unité d'Horodatage qui devient opérationnelle lorsque son certificat a été produit par une Autorité de certification (AC) et installé dans metatime. Le certificat peut être fourni par metapki la solution de Atos, ou d'autres solutions de PKI. Les contremarques de temps sont archivées dans une base de données située dans le serveur back office. Les accès au serveur front office peuvent optionnellement être authentifiés.

Accompagnement

Atos fournit des services de conseil afin de définir une ou plusieurs politiques d'horodatage en accord avec les besoins de l'organisation.



Caractéristiques techniques

Serveurs front office et back office

- Plateforme Linux (c-à-d RedHat ou SuSE)
- Composants Open source internation aux fournis avec metatime : Apache, Open SSL, PostgreSQL et PHP

HSM

- Tout HSM disposant d'une interface d'accès PKCS#11 pour la signature des contremarques de temps et en particulier les suivants : Trustway crypt2pay profil Protect, TrustWay Proteccio®
- Production de couples de clés avec exportation des clés publiques

La référence de temps

- Metatime permet le choix entre une référence GPS et/ou une référence DCF 77

Normes et standards
(conforme à la directive européenne 1999/93/CE et au réglement eIDAS)

- IETF RFC 3161
- ETSI TS 101 861 (un profil de RFC 3161)
- X.509 v3 ou RFC 5280 pour les certificats des unités d'horodatage
- KCS#11 pour l'interface avec le HSM
- HTTP ou HTTPS pour la fourniture des contremarques de temps
- HTTPS pour l'administration

Veuillez trouver plus d'information sur
https://atos.net/fr/produits/cybersecurite/digital-identities/metatime

CT_180928_LPM_Fs-Horus_metatime_fr4