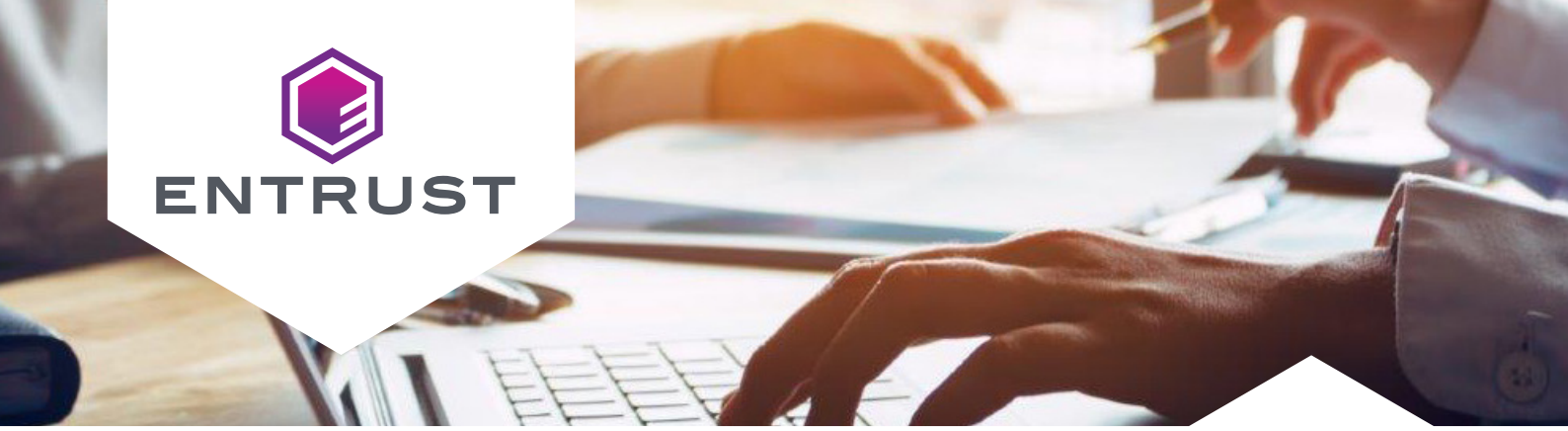

Les solutions de signature de code Entrust

Un niveau de sécurité élevé pour la signature de code

CARACTÉRISTIQUES

- Garantie de la paternité, de la date de publication et du contenu
- Assurance de l'intégrité des logiciels
- Protection des clés de signature de code importantes

Les défis de la distribution des codes

L'informatique d'entreprise est complexe et utilise des logiciels venant de différentes sources afin de faire fonctionner une organisation. Les entreprises qui développent des logiciels, que ce soit pour un usage interne ou pour les vendre à leurs clients, doivent créer ou maintenir des mécanismes qui prouvent l'authenticité de leurs logiciels. Assurer cette sécurité nécessite de :

- Valider le processus de signature, afin que seul le bon code soit signé par les bonnes clés
- Gérer les clés de signature privées afin qu'elles ne soient pas volées, permettant ainsi à des versions non autorisées d'atteindre leurs clients
- Fournir une piste d'audit de toutes les activités de signature

Entrust possède une expertise significative dans le développement et la mise en œuvre de solutions de signature de code sécurisées qui résolvent les problèmes de processus, d'intégrité, d'autorisation et de protection des clés privées en fournissant les fonctionnalités suivantes :

- Réduit le risque de vol de clés, l´usurpation d'entreprise et l'altération de logiciels malveillants
- Permet aux utilisateurs finaux de vérifier la source et l'intégrité des logiciels et de détecter l'altération ou l'insertion de codes malveillants
- Contribue à éviter que les utilisateurs n'abandonnent l'installation en raison des dialogues d'avertissement forts des systèmes d'exploitation pour les logiciels non signés
- Fournit un contrôle d'accès, un processus d'approbation, des capacités d'automatisation et d'audit pour les opérations de signature de code

Pour offrir ces fonctionnalités, Entrust propose deux solutions de signature de code qui sont basées sur les modules matériels de sécurité (HSM) nShield® comme racine de confiance. Ces solutions sont les suivantes :

- Code Signing Gateway
- Signature de code avec intégration directe de HSM

Qu'est-ce qu'un code ?

Le code peut être considéré comme un pack binaire d'informations qui est consommé ou exécuté par les plateformes cibles. Les exemples de code comprennent les packs exécutables, les packs d'installation, les packs de microprogrammes et les environnements intégrés.

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Les solutions de signature de code Entrust

Signature de code avec les HSM d´Entrust comme racine de confiance

La signature de code est l'application des signatures numériques à l'édition de logiciel. La signature de code permet aux utilisateurs finaux de vérifier la source et l'intégrité des logiciels en authentifiant l'identité de l'éditeur ; elle contribue également à empêcher les utilisateurs d'abandonner les installations de logiciels car les systèmes d'exploitation présentent des dialogues d'avertissement robustes pour les logiciels non signés.

Les solutions de signature de code utilisent la paire de clés publiques/privées du créateur du logiciel et un certificat numérique. Ce dernier comprend la clé publique du créateur du logiciel et est signé par une AC appropriée, pour permettre à l'utilisateur final de vérifier le code. Le processus commence lorsque l'auteur du logiciel hachera le code à distribuer, et utilisera sa clé privée pour signer/chiffrer le hachage. L'auteur distribue ensuite le hachage chiffré et le code original, ainsi que le certificat numérique, dans un pack à l'utilisateur final. Enfin, l'utilisateur final utilise la clé publique de l'auteur du logiciel pour déchiffrer le code chiffré et haché et compare le hachage obtenu avec un hachage régénéré du code reçu. Si les hachages sont identiques, le code est vérifié.

La clé privée est essentielle à la sécurité du système de signature de code et ne doit jamais être révélée ou partagée. Si la clé privée est compromise, le système de confiance échoue. La sécurité de la clé de signature privée est indispensable pour le processus de signature de code.

Pour les applications sensibles telles que la signature de code, la protection de la clé privée, qu'elle soit utilisée ou non, est essentielle pour créer une solution sécurisée. Les HSM offrent un environnement certifié inviolable pour sécuriser les clés tout au long de leur cycle de vie.

Code Signing Gateway

Pour les grandes organisations qui ont besoin d'un processus d'approbation de signature de logiciels hautement contrôlé, Code Signing Gateway offre une gamme de fonctions d'automatisation des processus flexibles et centralisés qui aident les organisations de développement de logiciels à répondre à des exigences de sécurité strictes. Code Signing Gateway est un serveur centralisé, hébergé par le client, qui exécute les applications de processus de signature de code Entrust.

Code Signing Gateway gère le processus, accepte les demandes, notifie les approbateurs par e-mail, gère les intervalles de temporisation, accuse réception des approbations, enregistre l'activité et livre le code signé à la zone de transit. Plusieurs rôles d'utilisateur peuvent être pris en charge, y compris, par exemple : les administrateurs de Code Signing Gateway, les développeurs d'applications d'entreprise, de bureau, d'IoT ou mobiles, l'équipe de gestion et les approbateurs de la signature de code. L'intégration d'Active Directory est utilisée pour l'autorisation des groupes de travail et l'authentification des utilisateurs.

Les HSM polyvalents nShield

Les HSM nShield sont des dispositifs certifiés, renforcés et inviolables qui offrent un environnement sécurisé pour générer et protéger les clés utilisées pour une variété d'applications. Les HSM nShield sont également disponibles en tant que service, sous trois formes :

- nShield Connect, un appareil servant de multiples applications sur un réseau ; également disponible en tant que service
- nShield Solo, une carte PCIe servant des applications sur un seul serveur
- nShield Edge, un appareil de bureau à connexion USB pour les transactions à faible volume

Les HSM nShield sont certifiés FIPS 140-2 niveau 2 et 3.

Les solutions de signature de code Entrust

Les HSM nShield sont utilisés pour protéger la clé privée utilisée pour signer le code. Les clés de signature résident dans les HSM et sont mises en relation avec plusieurs profils de signature qui peuvent être créés dans Code Signing Gateway.

Code Signing Gateway s'intègre aux outils de signature standard tels que Oracle Jarsigner, Microsoft SignTool, l'outil de signature de code d'Apple et le service de signature de code d'Android. Le schéma du processus est illustré sur la Figure 1.

Les fonctionnalités supplémentaires comprennent plusieurs profils de signature qui peuvent être définis pour utiliser un certain nombre de certificats numériques prenant en charge plusieurs profils de signature, la journalisation centralisée, l'archivage des fichiers, l'intégration avec un service d'horodatage ainsi que l'intégration avec Microsoft Defender pour vérifier l'absence de virus dans les fichiers avant la signature.

Code Signing Gateway d'Entrust est une solution personnalisée pour l'environnement unique de chaque client par l'équipe des services professionnels Entrust.

Signature de code avec intégration directe de HSM

L'intégration directe avec un HSM nShield offre une solution pour un petit nombre de développeurs avec une simple séparation des tâches. Elle est généralement utilisée pour les postes de travail des développeurs individuels ou les serveurs dédiés à la signature de code. La clé privée utilisée pour la signature du code est générée et protégée par le HSM nShield.

La signature de code s'intègre au HSM en utilisant des API standard, par exemple Java Cryptography Extension (JCE) et Microsoft CAPI et CNG et utilise des outils tiers tels que Jarsigner, SignTool et Open SSL pour créer des demandes de signature à exécuter par le HSM.

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur **entrust.com/fr/HSM** Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

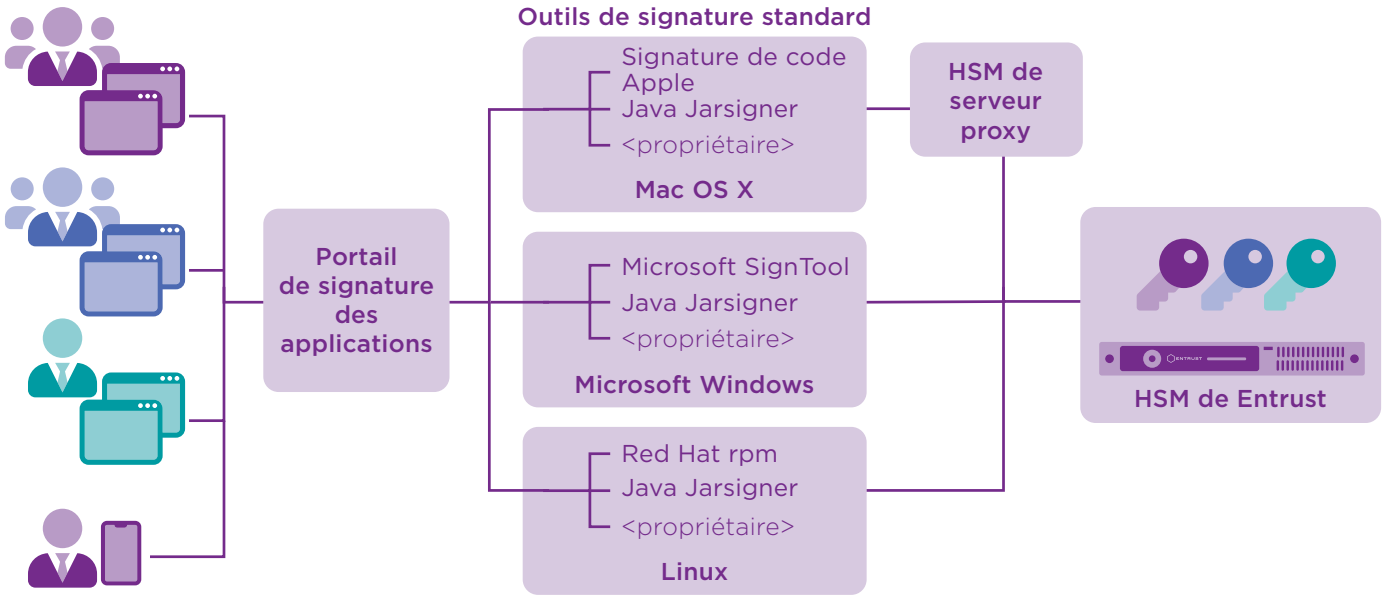

Figure 1 : Schéma de Code Signing Gateway

Pour en savoir plus sur les HSM nShield de Entrust

HSMinfo@entrust.com

entrust.com/fr/HSM

À PROPOS DE LA SOCIÉTÉ ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre gamme unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2 500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/fr/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com