nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

CodeSafe: exécution de code dans un environnement sécurisé

- Vise à préserver l'intégrité via la signature numérique et la vérification du code
- Propose un environnement sécurisé pour la gestion de clés via l'application de politiques de sécurité
- Permet un contrôle d'accès fort par l'association de clés et de certificats uniques aux applications
- Propose une solution utile et pratique grâce aux outils CodeSafe à distance

nCipher Security CodeSafe®

Protection matérielle certifiée pour vos applications sensibles

nCipher Security CodeSafe®

CodeSafe est un ensemble d'outils permettant aux développeurs d'écrire et d'exécuter des applications sensibles au sein de l'environnement sécurisé des HSM nShield certifiés FIPS. Les applications exécutées dans cet environnement peuvent chiffrer, déchiffrer et traiter des données, ainsi que bénéficier de la mise en œuvre, par les HSM, des stratégies de gestion des clés des applications.

LARGE PANEL D'APPLICATIONS

CodeSafe peut être utilisé pour protéger tous types d'applications. Des exemples incluent la cryptographie et la logique métier associée à des banques, mesures intelligentes, agents d'authentification, agents de signature numérique et processus de chiffrement personnalisés.

INTÉGRITÉ DE L'APPLICATION CODESAFE

CodeSafe fournit des outils de signature numérique des applications exécutées dans l'environnement sécurisé de nShield de Permettant la vérification de leur intégrité au moment de l'exécution.

CONTRÔLE D'ACCÈS ET APPLICATION DE STRATÉGIES CODESAFE

CodeSafe permet au propriétaire du logiciel de définir les stratégies régulant l'utilisation des données de l'application (y compris les clés et certificats) et de mettre en œuvre ces stratégies afin de procurer un environnement sécurisé pour la gestion des clés. CodeSafe met également en place une association unique des clés et certificats avec les applications concernées afin d'assurer un fort contrôle d'accès.

TERMINAUX SSL/TLS SÉCURISÉS

Les développeurs d'applications utilisant CodeSafe peuvent intégrer la bibliothèque OpenSSL au sein de leur application afin de fermer des sessions SSL/TLS au sein du HSM nShield, facilitant ainsi le chiffrement de bout en bout, renforçant la sécurité de la couche de transport des données et réduisant l'exposition aux attaques.

DÉPLOIEMENT ET MISES À JOUR À DISTANCE

Les administrateurs peuvent déployer des applications depuis un emplacement centralisé, évitant ainsi le besoin d'accéder physiquement aux HSM.

COMPATIBILITÉ NSHIELD

CodeSafe est disponible avec les HSMs certifiés FIPS 140-2 niveau 3 nShield Solo (PCI-e) et nShield Connect (boîtier réseau). Les modèles compatibles incluent tous les HSMs nShield Solo et Connect, y compris les versions XC.

ENVIRONNEMENT DE DÉVELOPPEMENT DES HSM

CodeSafe est compatible avec les applications de programmation suivantes:

- langages de programmation C et C++ pour applications intégrées
- C, C++ et Java sur serveur hôte

DÉBUTER AVEC CODESAFE

Les éléments suivants sont requis pour utiliser CodeSafe :

- Kit du développeur CodeSafe
- HSM nShield Solo ou Connect certifié FIPS 140-2 niveau 3
- Licence d'activation CodeSafe

Le kit du développeur CodeSafe inclut des tutoriels, de la documentation et des exemples de programmes pour vous assister dans l'intégration de votre application au sein des HSM nShield. À cette fin, la solution nCipher Advanced Solutions Group (ASG) vous fournit également des services professionnels adéquats.

EN SAVOIR PLUS

Pour découvrir comment nCipher Security incorpore confiance, intégrité et contrôle aux informations et applications critiques de votre entreprise, accédez à ncipher.com