Les HSM (module matériels de sécurité) polyvalents nShield®

ENTRUST

SECURING A WORLD IN MOTION

Sommaire

Une solution de sécurité sur laquelle vous pouvez compter

Les modules matériels de sécurité (HSM) nShield de Entrust sont des appareils renforcés et inviolables qui protègent les données critiques de votre entreprise. Ces modules certifiés FIPS 140-2 FIPS et CC de réaliser des opérations de chiffrement telles que la génération, la gestion et le stockage de clés de chiffrement et de signature, ainsi que des fonctions sensibles au sein de leurs limites protégées.

Éléments indispensables à la sécurité de votre organisation, les HSM nShield vous permettent de :

- Atteindre de meilleurs niveaux de sécurité des données et de confiance
- Respecter et surpasser les principales normes réglementaires
- Maintenir des niveaux élevés de service et de réactivité commerciale

La gamme nShield

Afin de mieux correspondre à votre environnement spécifique, la gamme de HSM polyvalents nShield comprend les modèles suivants :

nShield Connect

Appareils connectés au réseau

Les HSM nShield Connect fournissent des services de chiffrement aux applications réparties sur le réseau.

nShield Edge

Modules mobiles USB

Les HSM nShield Edge sont des appareils de bureau conçus pour être pratiques et abordables. Edge est l'outil idéal pour les développeurs, et prend en charge des applications telles que la génération de clés racines en faible volume.

nShield Solo

Cartes PCIe à intégrer dans des appareils ou des serveurs

Les HSM nShield Solo sont des modules de cartes PCI-Express de petite taille qui fournissent des services de chiffrement aux applications hébergées sur serveur ou appareil.

nShield as a Service

Accès grâce à un abonnement aux HSM nShield Connect XC dans le cloud

nShield as a Service permet d'avoir accès par abonnement aux HSM nShield Connect XC certifiés FIPS 140-2 de niveau 3. Cette solution offre les mêmes caractéristiques et fonctionnalités que les HSM sur site, auxquelles s'ajoutent les avantages d'un déploiement dans le cloud. Cela permet aux clients d'atteindre leurs objectifs en matière de stratégies basées essentiellement sur le cloud, tout en confiant la gestion de ces appareils aux équipes de Entrust. Disponible sous forme de services auto-gérés par le client ou entièrement gérés par Entrust.

Un large éventail d'utilisations

Les clients de Entrust utilisent les HSM nShield comme base de confiance pour toute une série d'applications d'applications du marché, notamment pour les infrastructures à clé publique (PKI), la protection des clés de chiffrement SSL/TLS, la signature de code, la signature numérique et la blockchain. Alors que le développement de l'Internet des Objets stimule une plus forte demande d'identifiants et de certificats pour les pour les équipements, les HSM nShield continueront à prendre en charge des mécanismes de sécurité essentiels tels que l'authentification des appareils à l'aide de certificats numériques.

Les HSM nShield prennent également en charge un large éventail d'algorithmes de chiffrement, notamment les algorithmes de chiffrement à courbe elliptique qui permettent des transactions à grande vitesse parfaitement adaptées aux environnements informatiques compacts d'aujourd'hui, ainsi que les systèmes d'exploitation et les API les plus utilisés.

Caractéristiques de la gamme nShield

Des interfaces de services web compatibles avec le cloud

Le pack d'options de services web nShield simplifie les interactions entre vos applications et les HSM en exécutant des requêtes par le biais d'appels de services web. Cette approche novatrice simplifie les déploiements en évitant de devoir intégrer les applications directement au sein de nShield, et permet de ne plus dépendre d'un système d'exploitation ou d'une architecture en particulier. Le pack d'options de services web peut interagir aussi bien avec des applications hébergées sur le cloud qu'au sein de centres de données classiques.

Conteneurisation sur site ou sur le cloud

Le pack d'options de conteneur nShield permet le développement et le déploiement en continu d'applications ou de processus conteneurisés grâce aux HSM matériels de sécurité haute protection de Entrust. Ces options comprennent un ensemble de scripts prépackagés qui simplifient considérablement l'intégration des HSM nShield au sein d'un environnement d'application conteneurisé tout en prenant en charge les besoins dynamiques et évolutifs des applications et des hébergeurs conteneurisés des clients.

Gestion renforcée des clés pour vos données sur le cloud avec nShield BYOK

nShield BYOK (Bring Your Own Key ou « apportez votre propre clé ») vous permet de générer des clés fortes au sein de vos HSM nShield sur site et de les exporter en toute sécurité vers vos applications cloud, qu'elles soient hébergées sur les services web d'Amazon, la plateforme cloud de Google, Microsoft Azure, ou bien les trois à la fois. Avec nShield BYOK, vous renforcez la sécurité de vos méthodes de gestion des clés, vous maîtrisez mieux vos clés et vous vous assurez de partager la responsabilité du maintien de la protection de vos données dans le cloud.

nShield BYOK comporte les avantages suivants :

- Des pratiques de gestion des clés plus sécurisées qui renforcent la sécurité de vos données sensibles au sein du cloud
- Génération de clés plus performantes grâce au générateur de nombres aléatoires à haute entropie du HSM nShield, protégé par un matériel certifié FIPS
- Un meilleur contrôle des clés : vous utilisez vos propres HSM nShield au sein de votre environnement pour créer et exporter vos clés en toute sécurité sur le cloud

Utilisez nCipher BYOK avec Microsoft Azure pour bénéficier d'une protection optimale et de contrôles stricts concernant le transport et l'utilisation des clés de chiffrement. Si vous avez besoin d'une assistance sur place pour l'intégration et le déploiement, choisissez notre pack de service de déploiement BYOK. Ce pack comprend un nShield Edge, l'intégration assurée par l'équipe des services techniques de Entrust, et un an de maintenance.

Pour la solution BYOK dans les services web Amazon et la plateforme Google Cloud, choisissez le pack d'options d'intégration dans le Cloud (CIOP) de Entrust. Ce pack d'options contient tout ce dont vous avez besoin pour utiliser vos HSM nShield sur site pour générer et louer vos clés aux services web d'Amazon ou à Google Cloud Platform. En outre, CIOP est compatible avec la nouvelle plate-forme ouverte Microsoft Azure BYOK.

Opérations simplifiées grâce à la gestion et au suivi à distance

Le suivi et la gestion à distance sont tous deux disponibles pour les HSM nShield Solo et nShield Connect avec nShield Monitor et nShield Remote Administration. Ils vous permettent de diminuer vos coûts opérationnels tout en restant informés et aux commandes de votre parc de HSM 24 heures sur 24, et 7 jours sur 7.

Le suivi et la gestion à distance de Entrust vous permet de :

- Optimiser les performances du HSM, la planification de l'infrastructure et son temps de fonctionnement en utilisant nShield Monitor pour informer votre personnel sur les tendances de la charge, les statistiques d'utilisation, les événements de sabotage, les avertissements et les alertes
- Diminuer les frais de déplacement et gagner du temps en gérant les HSM grâce à l'interface performante et sécurisée de nShield Remote Administration

Configuration à distance

Les HSM nShield Connect XC disposent d'une console qui simplifie l'installation physique du HSM pour le montage en rack, le câblage et l'alimentation électrique. Toutes les autres configurations de HSM et du réseau peuvent alors être effectuées à distance. Cela facilite le déploiement et le redéploiement, ce qui permet d'éviter de devoir revenir au centre de données. Cette fonction prend en charge un modèle fournisseur/locataire dans lequel le fournisseur contrôle la configuration du réseau et le locataire a le contrôle total de son matériel stratégique.

Une architecture très souple grâce à Security World

nShield Security World fournit aux HSM nShield de Entrust un environnement unique et évolutif pour la gestion des clés. Avec nShield Security World, vous pouvez combiner différents modèles de HSM nShield pour construire un écosystème unifié et évolutif qui vous permettra d'équilibrer les charges et de bénéficier d'un basculement transparent.

« Les HSM nShield de nCipher sont des appareils de pointe qui nous ont permis d'intégrer une puce plus élaborée et plus sécurisée à notre technologie. »

Bill Kavadas, Responsable des systèmes d'information, Memjet

nShield Security World vous procure l'interopérabilité, que vous déployiez un ou des centaines de HSM, il vous permet de gérer un nombre illimité de clés, et il sauvegarde et restaure tout matériel associé à une clé automatiquement et à distance.

nShield Security World vous permet de :

- Adapter facilement votre parc de HSM nShield en fonction de vos besoins
- Préserver la résilience du système
- Gagner du temps en évitant les sauvegardes HSM qui prennent beaucoup de temps

CodeSafe - L'environnement d'exécution sécurisé de nShield

Les HSM nShield Solo et nShield Connect ne se contentent pas de protéger vos clés sensibles : ils fournissent également un environnement sécurisé pour vos applications propriétaires. CodeSafe vous permet de développer et d'exécuter du code au sein de nShield conformément aux exigences de la norme FIPS 140-2 de niveau 3 et Critères Communs, protégeant ainsi vos applications contre les attaques potentielles.

CodeSafe vous permet de :

- Garantir un niveau d'assurance élevé en exécutant des applications sensibles et en protégeant les points de terminaison des données d'application au sein d'un environnement certifié
- Protéger les applications critiques contre les risques, tels que les attaques internes, les logiciels malveillants et les menaces persistantes avancées
- Empêcher que les applications ne soient modifiées sans autorisation préalable ou infectées par des logiciels malveillants grâce à la signature de code

Des partenariats avec les principaux acteurs du marché

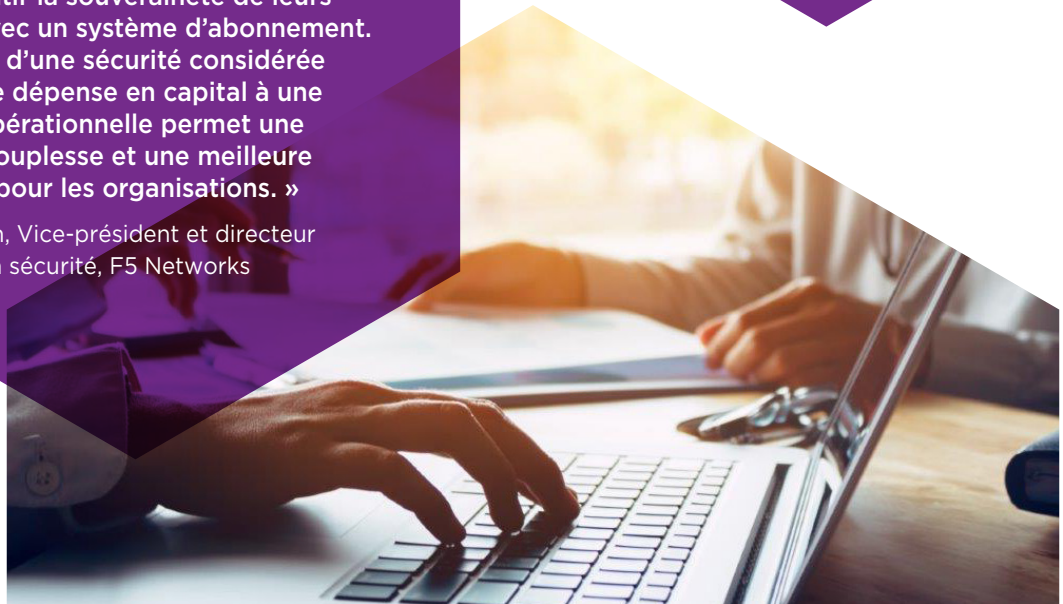
Entrust s'associe aux principaux fournisseurs de technologies de pointe afin de vous fournir des solutions élaborées qui répondent à un large éventail de défis en matière de sécurité et d'aider vos clients à atteindre leurs objectifs de transformation numérique. Dans le cadre de son programme de partenariat technologique, Entrust travaille avec ses partenaires pour intégrer les HSM nShield à toute une série de solutions de sécurité, notamment l'authentification et la PKI, la sécurité des bases de données, la signature de code, les signatures numériques, la gestion des comptes privilégiés, la fourniture d'applications, mais aussi le traitement des données dans le cloud et des données volumineuses. Les HSM nShield prennent en charge les applications de sécurité de nos partenaires afin que nous puissions leur fournir le meilleur chiffrement, la meilleure protection des clés et la meilleure gestion des clés possibles, et ce, tout en facilitant leur mise en conformité avec les réglementations en vigueur des autorités publiques et du marché en matière de sécurité des données.

« Nous sommes ravis des possibilités que les nouvelles fonctionnalités compatibles avec le cloud de nShield offrent à nos clients, notamment nShield as a Service. Ces nouvelles fonctionnalités reflètent l'évolution du marché qui reconnaît le fait que les organisations ont pleinement besoin des performances des HSM dans le cloud afin de stimuler l'innovation et d'en tirer tous les avantages commerciaux possibles. »

Ed Wood, Directeur de la gestion des produits, Cryptomathic

« Le déploiement de nShield as a Service de Entrust a permis aux clients de F5 de bénéficier d'options de sécurité renforcées et de garantir la souveraineté de leurs données avec un système d'abonnement. Le passage d'une sécurité considérée comme une dépense en capital à une dépense opérationnelle permet une meilleure souplesse et une meilleure rentabilité pour les organisations. »

John Morgan, Vice-président et directeur général de la sécurité, F5 Networks



Une polyvalence et des performances exceptionnelles

Les HSM nShield Connect et nShield Solo sont disponibles dans 3 niveaux de performance pour s'adapter à votre environnement, par exemple si vos volumes de transactions sont modérés ou si votre application exige un débit élevé. nShield as a Service, notre solution sur abonnement permettant d'accéder aux HSM nShield, est renforcée par les HSM haute performance nShield Connect XC.

Des solutions certifiées conformes aux normes en vigueur

Entrust respecte les normes les plus strictes, ce qui vous aidera à démontrer votre conformité dans les environnements réglementés tout en bénéficiant de l'intégrité et de la sécurité des HSM nShield. Vous trouverez ci-dessous une liste non exhaustive des normes que nous respectons. Une liste complète est disponible sur notre site web et dans nos brochures.

FIPS 140-2

Reconnue mondialement, la norme FIPS 140-2 est une norme du NIST, agence du Département du Commerce des États-Unis, qui atteste de la fiabilité des modules de chiffrement. Tous les HSM nShield de Entrust sont certifiés FIPS 140-2 de niveau 2 et de niveau 3.

FIPS Level 3 Validated 140-2

Common Criteria

Critères communs et conformité au règlement eIDAS

Les HSM nShield XC et nShield + HSM sont certifiés Critères Communs et reconnus comme dispositifs qualifiés de création de signature (QSCD), conformément au règlement eIDAS. De plus, les HSM nShield Solo XC et Connect XC sont conformes au profil de protection des critères communs EN 419 221-5 intitulé « Modules de chiffrement pour les services de confiance ». Les HSM de nShield constituent ainsi les piliers de sécurité du processus de dématérialisation pour les entreprises et les administrations de l'Union Européenne. Cela comprend la mise en place de systèmes nationaux et transfrontaliers d'identification, de services pour la signature de documents électroniques et de transactions, ainsi que de services d'authentification, d'horodatage, de sécurisation des e-mails et de conservation à long terme des documents. Bien que ces normes aient été établies dans le cadre d'un règlement européen, elles sont adoptées par de nombreux pays dans le monde.

Pour en savoir plus

Consultez la page **entrust.com/fr/hsm**. pour découvrir comment nous pouvons protéger les données et applications critiques de votre organisation, que ce soit dans vos propres locaux, sur le cloud ou bien au sein d'environnements virtuels.

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 portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2500 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/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com