Universell einsetzbare nShield®-Hardware-Sicherheitsmodule

ENTRUST

SECURING A WORLD IN MOTION

Inhalt

Sicherheit, der Sie vertrauen können

Die nShield-Hardware-Sicherheitsmodule (HSM) von Entrust sind verstärkte, manipulationssichere Geräte, welche die sensibelsten Daten Ihres Unternehmens schützen. Diese nach FIPS 140-2 zertifizierten Module führen kryptographische Funktionen wie das Erstellen sowie das Verwalten und Speichern von kryptographischen Schlüsseln- und Signierschlüsseln sowie sensible Funktionen innerhalb ihrer geschützten Bereiche aus.

Als leistungsstarke Ergänzung Ihres Sicherheitspakets unterstützen Sie die nShield-Hardware-Sicherheitsmodule dabei:

- einen höherer Grad an Datensicherheit und Vertrauen zu erreichen
- den wesentlichen Regulierungsstandards zu entsprechen und diese zu übertreffen
- ein hohes Serviceniveau und wirtschaftlicher Agilität aufrechtzuerhalten

Die nShield-Serie

Die nShield-Serie bietet für jede Umgebung die richtigen universell einsetzbaren HSM und umfasst die folgenden Modelle:

nShield Connect

Vernetzte Appliances

nShield-Connect-HSM stellen Verschlüsselungsdienste für Anwendungen innerhalb des gesamten Netzwerks bereit. Sie sind in zwei Serien erhältlich: die klassischen nShield-Connect+-HSM sowie die leistungsstarken nShield Connect XC.

nShield Edge

Tragbare USB-basierte Module

nShield-Edge-HSM sind einfach zu bedienende günstige Desktopgeräte. Sie eignen sich perfekt für Entwickler und unterstützen Anwendungen wie die Erstellung einer geringen Anzahl von Root-Schlüsseln.

nShield Solo

PCIe-Karten zur Einbettung in Geräte oder Server

Die Hardware-Sicherheitsmodule nShield Solo sind Niedrigprofil-PCI-Expresskartenmodule, die kryptographische Dienste für Anwendungen bereitstellen, welche auf einem Server oder einem Gerät gehostet werden. Sie sind in zwei Serien erhältlich: die klassischen nShield-Connect+-HSM sowie die leistungsstarken nShield Solo XC.

nShield-as-a-Service

Abo-basierte Lösung für den Zugriff auf nShield-HSM in der Cloud

nShield-as-a-Service stellt Zugang zu dedizierten, nach FIPS 140-2 Level 3 zertifizierten nShield-Connect-XC-HSM über ein Abonnementmodell bereit. Die Lösung bietet dieselben Funktionen wie On-Premises-HSM kombiniert mit den Vorteilen eines Cloud-Dienstes. So sind Kunden in der Lage, ihre in erster Linie auf die Cloud ausgerichteten Ziele zu erfüllen und die Wartung dieser Geräte den Experten von Entrust zu überlassen. Erhältlich als selbstverwaltete und vollständig verwaltete Service-Optionen.

Unterstützung für ein breitgefächertes Einsatzspektrum

Die Kunden von Entrust verwenden nShield-Hardware-Sicherheitsmodule als vertrauenswürdige Basis für verschiedene Unternehmensanwendungen, unter anderem Public Key Infrastructure (PKI), SSL/TLS-Schlüsselschutz, Code Signing, Digital Signing und Blockchain. Während das Wachstum des Internet-of-Things zu einer größere Nachfrage nach Geräte-IDs und Zertifikaten führt, untermauern die nShield-Hardware-Sicherheitsmodule weiterhin wichtige Sicherheitsmaßnahmen wie beispielsweise die Geräteauthentifizierung mithilfe von digitalen Zertifikaten.

nShield-Hardware-Sicherheitsmodule unterstützen außerdem ein breites Spektrum an kryptographischen Algorithmen, einschließlich der elliptischen Kurvenkryptographie, die Hochgeschwindigkeits-Transaktionen anbietet, welche perfekt für die heutigen kompakten Datenverarbeitungsumgebungen geeignet sind, sowie die in der Branche am häufigsten verwendeten Betriebssysteme und APIs.

Merkmale der nShield-Serie

Cloud-freundliche Web-Service-Schnittstellen

Die optionale Web-Services-Optionspaket von nShield optimiert die Schnittstelle zwischen Ihren Anwendungen und den Hardware-Sicherheitsmodulen, indem sie Befehle über Web-Service-Aufrufe ausführt. Dieser innovative Ansatz erleichtert die Bereitstellung, da es nicht mehr erforderlich ist, Anwendungen direkt mit nShield zu integrieren, und beseitigt die Abhängigkeit von Betriebssystemen und der Wahl des Architekturdesigns. Das Web-Services-Optionspaket, eine Cloud-kompatible Lösung, verbindet Anwendungen, die in der Cloud wie auch in herkömmlichen Rechenzentren gehostet werden.

Containerisierter Support On-Premises oder in der Cloud

Das nShield Container Option Pack ermöglicht die nahtlose Entwicklung und Bereitstellung von containerisierten Anwendungen oder Prozessen, die durch die hochsicheren Hardware-Sicherheitsmodule von Entrust unterstützt werden. Diese Option bietet eine Reihe vorkonfigurierter Skripte an, die die Integration von nShield-HSM in eine Container-Anwendungsumgebung erheblich vereinfachen und gleichzeitig die dynamischen, skalierbaren Anforderungen von Kundenanwendungen und containerisierten Hosts unterstützen.

Leistungsstärkere Schlüsselverwaltung für Ihre Cloud-Daten mit nShield-BYOK

nShield-BYOK (Bring Your Own Key) ermöglicht es Ihnen, in Ihren On-Premises installierten nShield-HSM starke Schlüssel zu erstellen und sicher in Ihre Cloud-Anwendungen zu exportieren, unabhängig davon, ob Sie Amazon Web Services, Google Cloud Platform, Microsoft Azure oder alle drei verwenden. Mit nShield-BYOK stärken Sie die IT-Sicherheit Ihrer Schlüsselverwaltung, erhalten mehr Kontrolle über Ihre Schlüssel und stellen sicher, dass Sie zur Sicherheit Ihrer Daten in der Cloud beitragen.

nShield-BYOK bietet Ihnen die folgenden Vorteile:

- Sicherere Schlüsselverwaltungspraktiken, welche die Sicherheit Ihrer sensiblen Daten in der Cloud erhöhen
- Stärkere Schlüsselerstellung mithilfe des hoch-Entropie Zufallszahlengenerators von nShield, geschützt durch FIPS-zertifizierte Hardware
- Größere Kontrolle über Schlüssel: verwenden Sie Ihre eigenen nShield-Hardware-Sicherheitsmodule in Ihrer eigenen Umgebung, um Ihre Schlüssel zu erstellen und sicher in die Cloud zu exportieren

Verwenden Sie nCipher BYOK mit Microsoft Azure, um für höchste Sicherheit und strikte Kontrolle des Transports und der Verwendung kryptographischer Schlüssel zu sorgen. Wenn Sie vor Ort Unterstützung bei Integration und Bereitstellung benötigen, wählen Sie das BYOK Deployment Services Pack. Dieses Paket umfasst nShield Edge, eine vom Entrust Professional Services Team umgesetzte Integration sowie ein Jahr Wartung.

Verwenden Sie das Cloud Integration Option Pack (CIOP) von Entrust für BYOK in Amazon Web Services und Google Cloud Platform. Das Optionspaket enthält alles, was Sie benötigen, um Ihre lokalen nShield HSM zur Erstellung und Vermietung der Schlüssel für Amazon Web Services oder die Google Cloud Platform zu verwenden. Zusätzlich bietet CIOP Unterstützung für den neuen offenen Plattformmechanismus Microsoft Azure BYOK.

Optimierter Betrieb mithilfe von Remote-Überwachung und Verwaltung

nShield Monitor und nShield Remote Administration sind für die Hardware-Sicherheitsmodule nShield Solo und Connect verfügbar. Sie tragen dazu bei, Ihre Betriebskosten zu reduzieren. Gleichzeitig sind Sie stets informiert und haben jederzeit die Kontrolle über Ihre Hardware-Sicherheitsmodule.

- Die Remote-Überwachung und -Verwaltung von nCipher bietet die folgenden Vorteile:
- Optimierung der Leistung der Hardware-Sicherheitsmodule, der Infrastrukturplanung und der Betriebszeit mithilfe von nShield Monitor, um Ihr Personal über Lasten-Trends, Nutzungsstatistiken, Manipulationsversuche, Warnungen und Alarmmeldungen zu informieren.
- Reduzierung von Fahrtkosten und -zeit durch die Verwaltung der Hardware-Sicherheitsmodule über die leistungsfähige und sichere Schnittstelle der nShield Remote Administration

Fernkonfiguration

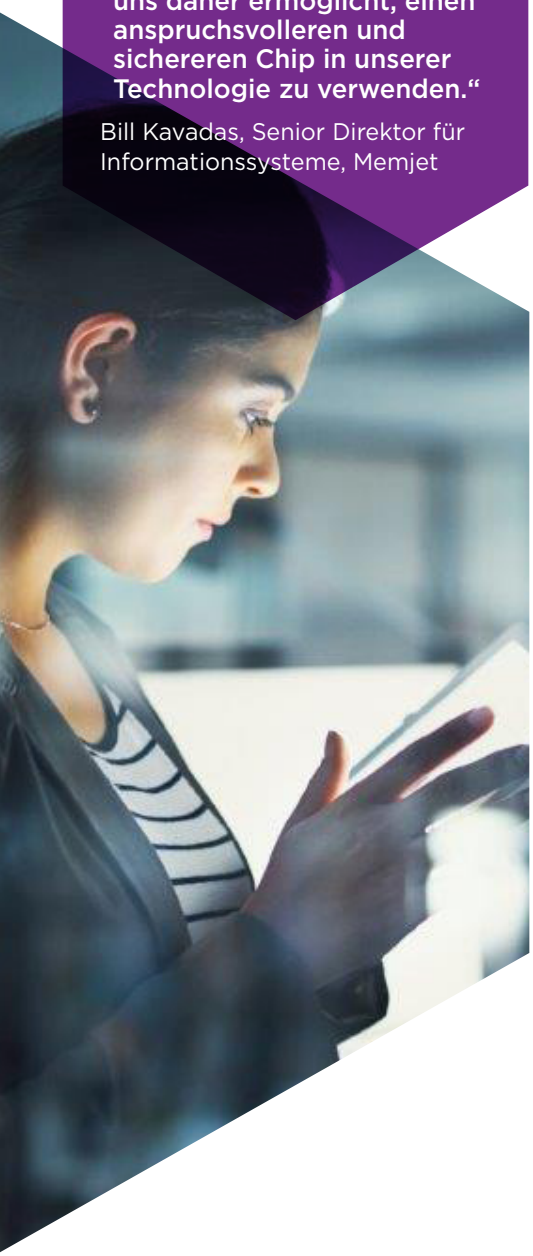
nShield Connect XC-Modelle bieten eine serielle Konsolenoption, welche die physische Installation des HSM für Racks, Verkabelung und Stromversorgung vereinfacht. Alle anderen HSM- und Netzwerkkonfigurationen können dann extern durchgeführt werden. Dies ermöglicht eine einfache Bereitstellung und Neuverteilung, ohne dass ein erneuter Besuch im Rechenzentrum erforderlich ist. Diese Funktion unterstützt ein Anbieter/Mieter-Modell, bei dem der Anbieter die Netzwerkkonfiguration kontrolliert und der Mieter die volle Kontrolle über sein Schlüsselmaterial hat.

Äußerst flexible Architektur von Security World

nShield Security World unterstützt die nShield HSM von Entrust, indem es eine einzigartige, flexible Umgebung für die Schlüsselverwaltung schafft. Mit nShield Security World können Sie verschiedene nShield-HSM-Modelle zu einem einheitlichen Ökosystem kombinieren, das Skalierbarkeit, nahtlosen Failover und Lastenausgleich bietet.

„Die Entrust nShield HSMs sind auf dem neuesten Stand der Technik und haben es uns daher ermöglicht, einen anspruchsvolleren und sichereren Chip in unserer Technologie zu verwenden.“

Bill Kavadas, Senior Direktor für Informationssysteme, Memjet



nShield Security World bietet Interoperabilität, unabhängig davon, ob Sie ein Hardware-Sicherheitsmodul oder hunderte bereitstellen, und ermöglicht Ihnen die Verwaltung einer unbegrenzten Anzahl von Schlüsseln sowie deren automatische und ferngesteuerte Sicherung und Wiederherstellung.

nShield Security World bietet die folgenden Vorteile:

- Sie können Ihre nShield-Hardware-Sicherheitsmodule bei zunehmendem Bedarf ganz einfach skalieren.
- Die Widerstandsfähigkeit Ihres Systems ist gewahrt.
- Sie sparen Zeit, da zeitraubende HSM-Backups nicht länger erforderlich sind.

CodeSafe: die sichere Ausführungsumgebung von nShield

Zusätzlich zum Schutz Ihrer sensiblen Schlüssel bieten die nShield-HSM Solo und Connect auch eine sichere Umgebung für die Ausführung Ihrer proprietären Anwendungen. Die CodeSafe-Option ermöglicht Ihnen das Entwickeln und Ausführen von Codes innerhalb der Grenzen der nach FIPS 140-2 Level 3 zertifizierten HSM und schützt Ihre Anwendungen so vor möglichen Angriffen.

CodeSafe unterstützt Sie dabei:

- Höhere Sicherheit bei der Ausführung sensibler Anwendungen zu erreichen und Datenendpunkte von Anwendungen innerhalb einer zertifizierten Umgebung zu schützen
- Sicherheitssensible Anwendungen vor Gefahren wie Insider-Angriffen, Malware und anhaltenden Bedrohungen zu schützen
- Das Risiko nicht-autorisierter Anwendungsänderungen oder Malware-Infektionen mithilfe von Code Signing zu beseitigen

Kooperation mit Branchenführern

Entrust arbeitet mit führenden Technologieanbietern zusammen, um verbesserte Lösungen für ein breites Spektrum von Sicherheitsherausforderungen bereitzustellen, mit denen sich die Branche konfrontiert sieht, und die Kunden beim Erreichen Ihrer Ziele in Bezug auf die digitale Transformation zu unterstützen. Im Rahmen seines Technologiepartnerprogramms arbeitet Entrust mit verschiedenen Partnern zusammen, um nShield-HSM in eine Vielzahl von Sicherheitslösungen zu integrieren, darunter Credentialing und PKI, Datenbanksicherheit, Code Signing, digitale Signaturen, Verwaltung privilegierter Konten, Anwendungsbereitstellung sowie Cloud- und Großdatenintelligenz. nShield-HSM unterstützen die Sicherheitsanwendungen unserer Partner, um die stärkste kryptographische Verarbeitung, den besten Schlüsselschutz und die beste Schlüsselverwaltung zu bieten und gleichzeitig die Einhaltung von staatlichen und branchenspezifischen Datensicherheitsvorschriften zu erleichtern.

„Wir sind von den Möglichkeiten begeistert, die die neuen Cloud-freundlichen Funktionen von nShield, einschließlich nShield-as-a-Service, unseren Kunden bieten. Diese neuen Funktionen verdeutlichen, dass sich der Markt verändert hat und dass Unternehmen die Fähigkeiten von Full-Service-HSMs in der Cloud benötigen, um die verfügbaren Innovationen und kommerziellen Vorteile freizusetzen.

Ed Wood, Direktor für Product Management, Cryptomathic

„Die Einführung von nShield-as-a-Service von Entrust bietet den Kunden von F5 erweiterte Sicherheitsoptionen und die Möglichkeit, Daten-Souveränität auf einem Abo-basierten Modell zu erreichen. Sicherheit fällt nicht länger unter die Investitionen sondern unter die Betriebsausgaben. Das ermöglicht Organisationen eine größere Flexibilität und Kosteneffizienz".

John Morgan, VP & GM für Security, F5 Networks

Vielseitigkeit und hohe Leistung

nShield Connect und Solo HSMs sind in drei Leistungsstufen erhältlich. Sie haben die Möglichkeit, passend zu Ihrer Umgebung die richtige Lösung auszuwählen, unabhängig davon, ob Ihre Transaktionsraten niedrig sind oder Ihre Anwendung einen hohen Durchsatz erfordert. nShield-as-a-Service, unsere abonnementbasierte Lösung für den Zugriff auf nShield- HSM in der Cloud, wird durch unsere leistungsstarken nShield Connect XC unterstützt.

Zertifizierung nach Branchenstandards

Entrust erfüllt strenge Normen und unterstützt Sie dabei, die Vorgaben in regulierten Umgebungen einzuhalten. Darüber hinaus sorgen wir für ein hohes Maß an Vertrauen in die IT-Sicherheit und die Integrität der nShield-Hardware-Sicherheitsmodule. Nachfolgend sehen Sie einen Auszug der Liste der Normen, die wir erfüllen. Die vollständigen Listen können Sie unserer Website und unseren Datenblättern entnehmen.

FIPS 140-2

FIPS 140-2 ist ein NIST-Standard der US-Regierung, der die Sicherheitsstabilität von Verschlüsselungsmodulen validiert. Alle nShield-HSM von Entrust sind nach FIPS 140-2 Level 2 und Level 3 zertifiziert.

FIPS Level 3 Validated 140-2

Common Criteria

Einhaltung von Common Criteria und eIDAS

nShield XC und nShield + HSMs sind nach Common Criteria EAL 4+ zertifiziert und als qualifizierte Signaturerstellungseinheiten (QSCDs) gemäß der eIDAS-Verordnung anerkannt. Darüber hinaus entsprechen nShield-Solo-XC und Connect-XC-HSM dem Common-Criteria-Schutzprofil EN 419 221-5 „Cryptographic Modules for Trust Services“. nShield HSMs können daher als Sicherheits-Backbone für die Digitalisierung von EU-Mitgliedsstaaten und Unternehmen dienen. Dazu gehören nationale ID-Systeme und grenzüberschreitende Dienste, Dienste für elektronische Dokumente und Transaktionssignierung sowie für Authentifizierung, Zeitstempel, sichere E-Mail und langfristige Dokumentenaufbewahrung. Obwohl diese Zertifizierungen als Teil einer europäischen Verordnung eingeführt wurden, werden sie von vielen Ländern auf der ganzen Welt übernommen.

Weitere Informationen

Auf unserer Website **entrust.com/HSM** zeigen wir Ihnen, wie wir Ihre geschäftskritischen Informationen und Anwendungen schützen – On-Premises, in der Cloud und in virtuellen Umgebungen.

Mehr Informationen zu Entrust nShield HSM

HSMinfo@entrust.com
entrust.com/HSM

ÜBER ENTRUST CORPORATION

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com