Entrust CodeSafe®

Zertifizierter Hardwareschutz für sensible Anwendungen

HIGHLIGHTS

CodeSafe: Führen Sie Code in einer sicheren Umgebung aus

- Schützt sensible Anwendungen, indem es diese in manipulationssicheren Hardware-Sicherheitsmodulen (HSM) ausführt
- Garantiert Integrität durch digitale Signaturen und die Prüfung von Code
- Setzt Richtlinien für die Bereitstellung einer sicheren Umgebung für die Schlüsselverwaltung um
- Sorgt für strikte Zugriffskontrolle, indem es Anwendungen eindeutige Schlüssel und Zertifikate zuweist
- Bietet bequemen Fernzugriff dank entsprechender CodeSafe-Tools

CodeSafe ist eine Zusammenstellung verschiedener Tools, mit denen Entwickler sensible Anwendungen innerhalb der manipulationssicheren Grenzen FIPS-zertifizierter nShield-HSM schreiben und ausführen können. In dieser sicheren Ausführungsumgebung können Anwendungen Daten verschlüsseln, entschlüsseln und verarbeiten. Außerdem sorgen die HSM für die Durchsetzung der Richtlinien für die Nutzung der entsprechenden Schlüssel.

Eine Vielzahl an Anwendungen

CodeSafe schützt jede Art von Anwendung. Beispiele umfassen Kryptographie und hochwertige Geschäftslogik im Zusammenhang mit Banking, intelligenter Verbrauchsmessung, Authentifizierungsagenten, digitalen Signaturen und benutzerdefinierten Verschlüsselungsprozessen

Mit CodeSafe die Integrität von Anwendungen gewährleisten

CodeSafe stellt Tools bereit, mit denen Sie die Anwendungen, die in der sicheren Umgebung von nShield ausgeführt werden, digital signieren und ihre Integrität mithilfe des HSM während der Laufzeit prüfen können.

Entrust CodeSafe®

WICHTIGE FUNKTIONEN UND VORTEILE

Richtliniendurchsetzung und Zugriffskontrolle mit CodeSafe

Mit CodeSafe kann der Eigentümer einer Software Richtlinien für die Nutzung der Anwendungsdaten einschließlich Schlüssel und Zertifikate definieren und durchsetzen und so eine sichere Umgebung für die Schlüsselverwaltung bereitstellen. CodeSafe unternimmt zudem eine eindeutige Zuweisung der Zertifikate und Schlüssel zu bestimmten Anwendungen, um eine strikte Zugriffskontrolle zu garantieren.

Sichere SSL/TLS-Endpunkte

Mit CodeSafe können Entwickler die OpenSSL-Bibliothek in ihre Anwendungen einbetten und so SSL-/TLS-Sitzungen innerhalb der nShield-HSM beenden. Dadurch sind eine End-to-End-Verschlüsselung, eine sicherere Datentransportschicht und die Verringerung der Angriffsoberfläche möglich.

Bereitstellung und Aktualisierungen per Fernzugriff

Administratoren können Anwendungen von einem zentralen Ort aus bereitstellen, ohne dass sie physisch auf die HSM zugreifen müssen.

nShield-Kompatibilität

CodeSafe ist mit FIPS 140-2 Level 3 zertifizierten nShield-Solo-PCIe und netzwerkgebundenen nShield-Connect-HSM erhältlich. Zu den kompatiblen Modellen gehören alle nShield-Solo- und Connect-HSM einschließlich der XC-Produktlinie.

HSM-Entwicklungsumgebung

CodeSafe ist mit den folgenden Programmieranwendungen kompatibel:

- C- und C++-Programmiersprachen für Embedded-Anwendungen
- C, C++ und Java auf dem Host-Server

CodeSafe: Erste Schritte

Für CodeSafe benötigen Sie:

- Nach FIPS 140-2 Level 3 zertifizierte nShield-Solo- oder Connect-HSM
- CodeSafe-Entwickler-Toolkit
- CodeSafe-Aktivierungslizenz

Das CodeSafe-Entwickler-Toolkit enthält Tutorials, Dokumentation und Beispielprogramme, die Sie dabei unterstützen, Ihre Anwendung mit nShield-HSM zu integrieren. Außerdem ist das Professional-Services-Team von Entrust Ihnen gerne bei der Integration behilflich.

Weitere Informationen

Auf Anfrage erhalten Sie von uns ein Whitepaper zu CodeSafe, das sich eingehender mit der zugrunde liegenden Technologie befasst. Mehr Informationen zu den nShield HSM von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com