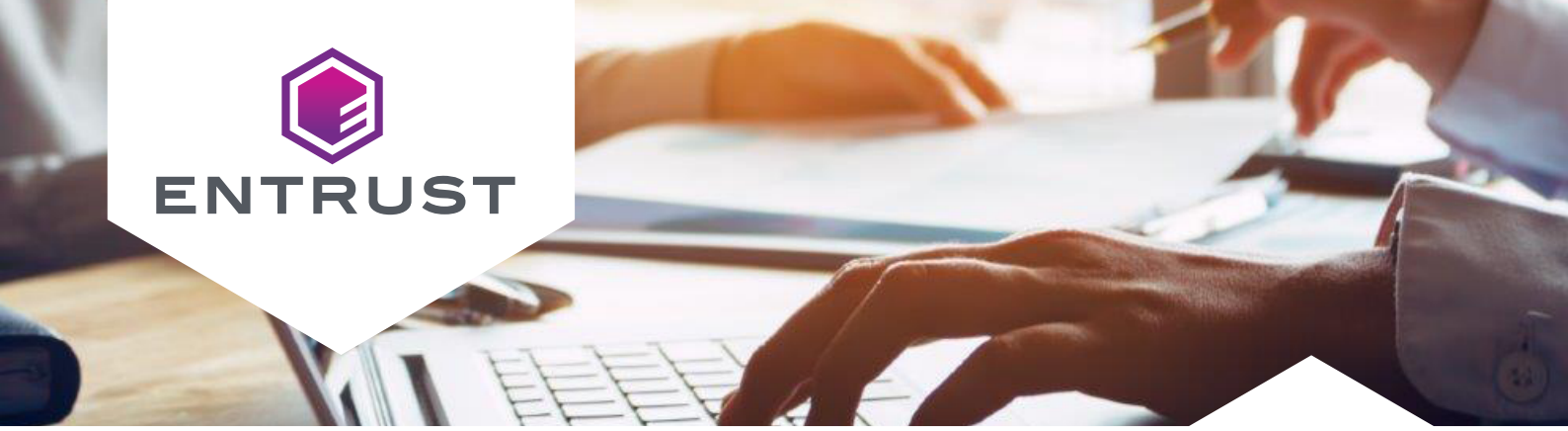

Code-Signing-Lösungen von Entrust

Hohe Sicherheit für Code Signing

ECKPUNKTE

- Sichert Urheberschaft, Veröffentlichungsdatum und Inhalt
- Gewährleistet Software-Integrität
- Schützt wertvolle Code-Signing-Schlüssel

Herausforderungen beim Versenden von Code

Die IT eines Unternehmens ist ein komplexes Gebilde. Um den Betrieb am Laufen zu halten, ist Software aus vielen unterschiedlichen Quellen erforderlich. Unternehmen, die Software für ihre Kunden oder den internen Gebrauch entwickeln, müssen geeignete Mechanismen finden, um die Authentizität dieser Software zu belegen. Das erreichen sie, indem sie:

- den Signaturprozess überprüfen, so dass nur der richtige Code durch die richtigen Schlüssel signiert wird
- den Diebstahl privater Signaturschlüssel verhindern, damit Kunden keine unautorisierten Versionen erhalten
- alle Signaturaktivitäten protokollieren

Was ist Code?

Code ist ein binäres Datenpaket, das von Zielplattformen genutzt oder ausgeführt wird. Beispiele sind ausführbare Pakete, Installationspakete, Firmwarepakete und eingebettete Umgebungen.

Entrust verfügt über umfangreiche Erfahrung in der Entwicklung und Umsetzung sicherer Code-Signing-Lösungen, die es Unternehmen ermöglichen, die Herausforderungen in Bezug auf Verfahren, Integrität, Autorisierung und den Schutz privater Schlüssel zu meistern, indem sie:

- das Risiko senken, dass Schlüssel gestohlen werden, Betrüger die Identität des Unternehmens nachahmen und die Software böswillig verändert wird
- dafür sorgen, dass Endbenutzer die Quelle und die Integrität der Software prüfen und Veränderungen oder das Einschleusen schädlichen Codes erkennen können
- verhindern, dass Benutzer die Installation nicht abschließen, weil sie eindeutige Warnmeldungen erhalten, dass es sich um unsignierte Software handele.
- den Zugriff auf sowie den Workflow, die Automatisierung und die Prüfung von Code-Signing-Verfahren kontrollieren

Zu diesem Zweck bietet Entrust zwei Code-Signing-Lösungen an, die auf nShield-Hardware-Sicherheitsmodulen als Vertrauensanker basieren. Diese Lösungen sind:

- Code Signing Gateway
- Code Signing mit direkter HSM-Integration

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Code-Signing-Lösungen von Entrust

Code Signing mit hsm von Entrust als Vertrauensanker

Code Signing bedeutet, dass Software mit digitalen Signaturen versehen wird. Mithilfe von Code Signing können Endbenutzer die Quelle und Integrität einer Software verifizieren, indem sie die Identität des Herstellers prüfen. Außerdem trägt es dazu bei, zu verhindern, dass Benutzer die Installation einer Software abbrechen, da sie Warnmeldungen des Betriebssystems erhalten, dass es sich um unsignierte Software handelt.

Mit Code-Signing-Lösungen kann der Endbenutzer mithilfe des öffentlichen bzw. privaten Schlüsselpaars des Urhebers der Software und einem digitalen Zertifikat den Code prüfen. Das Zertifikat enthält den öffentlichen Schlüssel des Urhebers und wurde von einer geeigneten Zertifizierungsstelle signiert. Zu Beginn dieses Verfahrens wendet der Urheber der Software eine Hash-Funktion an, um den Code zu senden, und signiert/verschlüsselt den Hash-Code mit seinen privaten Schüssel. Anschließend enthält der Endbenutzer ein Paket mit dem verschlüsselten Hash-Code, dem originalen Code sowie einem Zertifikat. Im letzten Schritt entschlüsselt der Endbenutzer mithilfe des öffentlichen Schlüssels des Urhebers der Software den Hash-Code und vergleicht den entsprechenden Hash mit einem neu erstellten Hash des erhaltenen Codes. Wenn beide identisch sind, ist der Code erfolgreich geprüft.

Der private Schlüssel ist wichtig für die Sicherheit des Code Signing Systems und darf unter keinen Umständen bekannt gemacht oder weitergegeben werden. Ein kompromittierter privater Schlüssel bringt das gesamte Vertrauenssystem zum Einsturz. Die Sicherheit privater Signaturschlüssel ist wichtiger Grundbaustein des gesamten Code-Signing-Prozesses.

Sensible Anwendungen wie Code Signing erfordern, dass der private Schlüssel stets geschützt ist – unabhängig davon, ob er gerade verwendet wird oder nicht. Nur dann sind diese Anwendungen sicher. HSM bieten eine zertifizierte manipulationssichere Umgebung, die Schlüssel über ihren gesamten Lebenszyklus schützt.

Code Signing Gateway

In großen Unternehmen muss das Verfahren zu Genehmigung von Software-Signaturen streng kontrolliert werden. Code Signing Gateway automatisiert den Workflow mithilfe flexibler und zentraler Funktionen, damit Softwareentwicklungsunternehmen strikte Sicherheitsanforderungen erfüllen können. Es handelt sich um einen zentralen, vom Kunden gehosteten Server, auf dem Workflow-Anwendungen von Entrust für das Code Signing ausgeführt werden.

Code Signing Gateway verwaltet den Workflow, akzeptiert Abfragen, benachrichtigt Genehmigungsberechtigte per E-Mail, verwaltet Auszeiten, bestätigt Genehmigungen und sendet signierten Code an den Bereitstellungsbereich.

Universell einsetzbare nShield HSM

nShield HSM sind zertifizierte, robuste und manipulationssichere Geräte, die eine sichere Umgebung für das Erstellen und den Schutz von Schlüsseln bereitstellen, die für eine Vielzahl an Anwendungen verwendet werden. Es gibt sie auch als as-a-Service-Modell, und sie sind in drei Formfaktoren erhältlich:

- nShield Connect unterstützt mehrere Anwendungen über ein Netzwerk (auch als a-a-Service-Modell erhältlich).
- nShield Solo ist eine PCIe-Karte für Anwendungen auf einem einzelnen Server.
- nShield Edge ist ein über USB angeschlossenen Desktop-Gerät für geringe Transaktionsvolumen.

Alle nShield HSM sind nach FIPS 140-2 Level 2 und Level 3 zertifiziert.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Code-Signing-Lösungen von Entrust

Code Signing Gateway unterstützt mehrere Benutzerrollen: Administratoren, Entwickler von Unternehmens-, Desktop-, IOT oder mobilen Anwendungen, Managementteam sowie zur Genehmigung von Code Signing Berechtigte. Die Autorisierung von Arbeitsgruppen und die Authentifizierung von Benutzern erfolgt mithilfe von Active Directory.

nShield HSM schützen den privaten Schlüssel, der zur Signierung des Codes verwendet wird. Die Signaturschlüssel werden im HSM aufbewahrt und dort in mehreren Signaturprofilen gruppiert, die in Code Signing Gateway erstellt werden.

Code Signing Gateway kann in übliche Signaturtools wie Oracle Jarsigner, Microsoft SignTool sowie in die Signing-Tool von Apple und Android integriert werden. Abbildung 1 zeigt das Prozessschema.

Außerdem können mehrere Signaturprofile für verschiedene digitale Zertifikate definiert werden. Diese Zertifikate unterstützen zentrale Protokolle, Dateiarchivierung, Integration in einen Zeitstempeldienst sowie Integration in Microsoft Defender zur Virenprüfung von Dateien vor dem Signieren.

Die Code Signing Gateway kann vom Professional Services Team von Entrust individuell an die Umgebung des Kunden angepasst werden.

Code Signing mit direkter HSM-Integration

Die direkte Integration in ein HSM eignet sich für eine kleine Anzahl an Entwicklern mit einfacher Aufgabentrennung. Sie wird in der Regle für einzelne Entwicklerarbeitsplätze oder entsprechende Code-Signing-Server genutzt. Das nShield HSM erstellt und schützt den privaten Schlüssel für das Code Signing.

Code Signing ist mit den üblichen HSM-API kompatibel, wie z. B. Java Cryptography Extension (JCE) sowie CAPI und CNG von Microsoft, und erstellt mittels Drittanbieter-Tools wie Jarsigner, SignTool und Open SSL Signaturanforderungen für das HSM.

Weitere Informationen

Mehr Informationen zu den nShield HSMs 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.

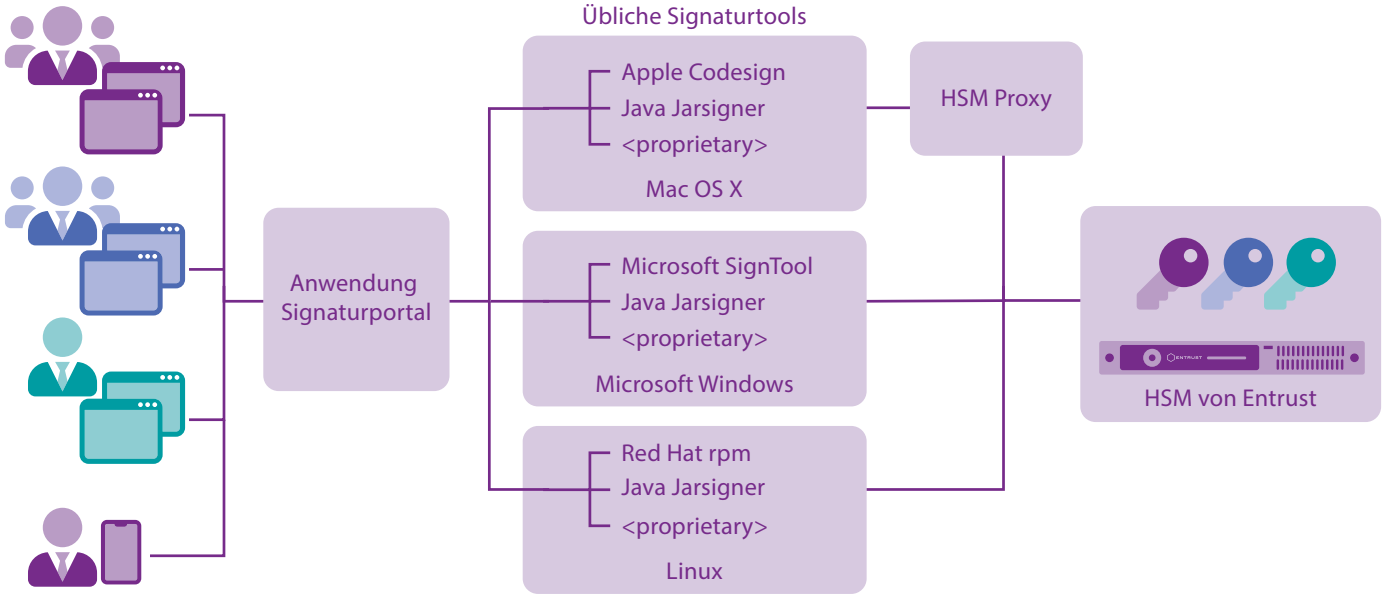

Abbildung: Schema von Code Signing Gateway.

Mehr Informationen zu Entrust nShield HSMs

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