cpl.thalesgroup.com/de

Code Signing

Code Signing

Beim Code Signing werden PKI-Technologien wie Schlüssel, Zertifikate und digitale Signaturen verwendet, um die Identität und Integrität von Software sicherzustellen. Technologieunternehmen teilen und verteilen Code über Netzwerke mit inkonsistenten und unterschiedlichen Sicherheitsrichtlinien, wodurch der Code potenziell Risiken durch Manipulation, Korruption oder Diebstahl ausgesetzt ist.

Viele Software-Anbieter stellen ihre Produkte inzwischen über das Internet zur Verfügung. Daher ist es zwingend erforderlich, dass der im Internet veröffentlichte Code vom Benutzer, der ihn herunterlädt, als vertrauenswürdig angesehen wird. Viele Browser weisen zwar darauf hin, die Authentizität des Codes zu überprüfen. Jedoch kann kein Browser feststellen, ob der Code vor der Auslieferung manipuliert wurde. Daher ist ein aktiverer Ansatz erforderlich, um das Internet zu einem zuverlässigen Medium für den Softwarevertrieb zu machen.

Digitale Signaturen helfen dabei, die elektronische Integrität und Authentizität eines Codes aufrechtzuerhalten, indem sie ihn mit der eindeutigen Signatur eines Softwareanbieters verknüpfen. So ist der Vertrieb von Software über das Internet kein anonymer Vorgang mehr, da digitale Zertifikate die Nachvollziehbarkeit sicherstellen, genau wie es der Markenname eines Herstellers auf der Software-Verpackung tut.

Digitale Zertifikate

Ein Zertifikat ist ein Datensatz, der eine Entität vollständig identifiziert und von einer Zertifizierungsstelle (Certification Authority, CA) ausgestellt wird. Dieser Datensatz enthält den öffentlichen kryptographischen Schlüssel der Entität. Wenn der Absender einer Nachricht diese mit seinem privaten Schlüssel signiert, kann der entsprechende Empfänger den öffentlichen Schlüssel des Absenders (abgerufen aus dem Zertifikat, das entweder mit der Nachricht gesendet wurde oder möglicherweise an anderer Stelle im Verzeichnisdienst verfügbar ist) verwenden, um dessen Identität zu überprüfen.

Vorteile von Thales

- Geprüfte Sicherheit mit Zertifizierung gemäß FIPS 140-2 Level 3 und Common Criteria
- Das einzige HSM, das echte Hardware-Schlüsselerstellung und Speicherfunktionen für die Notfallwiederherstellung bietet
- Multifaktor-Authentifizierung für Verwaltung und Management
- Überlegene Performance: Ein einzelnes Thales-Luna-HSM ist in der Lage, bis zu 20.000 ECC- und 10.000 RSA-Operationen pro Sekunde durchzuführen
- Aufgabentrennung mit mehrstufiger Zugriffskontrolle für alle Schlüssel der Zugriffsverwaltung
- Cloud-basiertes HSM on Demand

Problemstellung des Kunden

Die Verhinderung von Produktfälschungen war für Softwareanbieter schon immer eine Herausforderung. Im Laufe der Zeit wurden Sicherheitsmaßnahmen wie manipulationssichere Verpackungen und eindeutige Lizenzschlüssel entwickelt, um die Zahl der Raubkopien und unautorisierte Kopien der auf Disketten vertriebenen Software so gering wie möglich zu halten. Dem Internet fehlt die subtile Sicherheit, die durch Verpackung, Regalplatz, Schrumpffolie und dergleichen gegeben ist. Ohne sich der Integrität der Software sicher zu sein und ohne zu wissen, wer sie veröffentlicht hat, ist es für Endbenutzer schwierig, zu beurteilen, inwieweit sie einer Software vertrauen können. Darüber hinaus verlangen Windows, Java und Apple, dass der Code ihren Anforderungen an digitale Signaturen entspricht. Wenn der Code keinem bekannten Anbieter zugeordnet ist, wird eine Sicherheitswarnung mit dem Hinweis „Unbekannter Herausgeber" angezeigt, die den Benutzer auffordert, das Programm zunächst zu autorisieren, bevor er es auf seinem Computer ausführen kann. Aus diesem Grund sehen sich die Softwarehersteller einem erhöhten Druck ausgesetzt, den Code zu signieren.

Sicherheitsbedrohung

- Das Vertrauen in die Marke geht verloren.
- Schädliche Malware wird oft als legitime Software getarnt. So kann sie leicht verbreitet werden, um ahnungslose Desktops mit Viren zu infizieren oder Anwendungen zu installieren, die betrügerische Aktivitäten ermöglichen.
- Code muss vor Viren geschützt werden, um Vertrauen in die Authentizität zu schaffen.

Die Rolle des Hardware-Sicherheitsmoduls

Um ein Zertifikat von einer Zertifizierungsstelle zu erhalten, muss ein Softwarehersteller die Kriterien für ein kommerzielles Veröffentlichungszertifikat erfüllen. Es wird empfohlen, dass Antragsteller ihren privaten Schlüssel mit einer dedizierten Hardwarelösung, die ein HSM sein kann, erzeugen und speichern.

Ein Hardware-Sicherheitsmodul (HSM) schützt die Identität, egal ob es sich um den Server, den Virtualisierungsserver oder den Benutzer handelt. Luna-HSM von Thales gehen in Sachen Sicherheit noch einen Schritt weiter, indem sie das Signiermaterial in einem Hardware-Gerät speichern und so die Authentizität und Integrität einer Code-Datei sicherstellen.

Luna-HSM

Schützen Sie sensible Daten und kritische Anwendungen, indem Sie kryptographische Schlüssel in Luna-Netzwerk-HSM speichern, schützen und verwalten. Setzen Sie auf diese hochsicheren, manipulationssicheren und gemäß FIPS 140-2 Level 3 zertifizierten netzwerkgebundenen Geräte mit einer Leistung, die am Markt ihresgleichen sucht.

Cloud-HSM on Demand

Zusätzlich zu unseren On-Premises-HSM-Lösungen bietet Thales auch eine Cloud-HSM-Lösung namens Data Protection On Demand (DPoD) an. DPoD bietet ein As-a-Service-Abrechnungsmodell, bei dem keine Hardware bereitgestellt und gewartet werden muss.

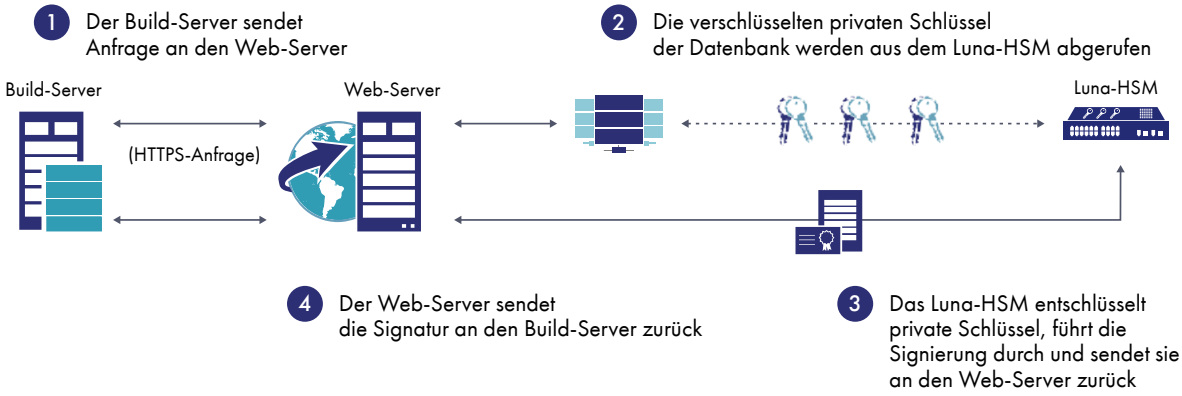
Anwendungsfall

Ein Software-Anbieter hat sein Geschäft darauf ausgerichtet, günstige und benutzerfreundliche Software über das Internet anzubieten. Mit der Veröffentlichung von Microsoft Windows Vista kam die Anforderung, dass heruntergeladener Code vor der Ausführung signiert werden muss. Wenn der Code nicht signiert war, wurde eine Warnmeldung ausgegeben, sobald potenzielle Kunden versuchten, die Software des Herstellers zu installieren. Laut dieser Meldung fehlten dem Download digitale Code-Signierungszertifikate, um die Quelle der Software zu authentifizieren. Die Folge war, dass viele Interessenten der Echtheit der heruntergeladenen Software nicht trauten und die Verkäufe über das Internet ins Stocken gerieten.

Um den Kunden zu versichern, dass er vertrauenswürdige Inhalte bereitstellt, suchte der Anbieter nach einer Lösung, um seinen Code mit privaten und öffentlichen Schlüsseln zu signieren. Die Lösung bestand in der Implementierung einer unternehmensweiten Public Key Infrastructure (PKI) mit VeriSign als Zertifizierungsstelle und einem Luna-HSM für die Speicherung der kryptografischen Schlüssel. Das Luna-HSM war die richtige Wahl, da es eine Zertifizierung gemäß FIPS 140-2 Level 3 und Common Criteria in einem manipulationssicheren Hardware-Gerät bot.

Mit der PKI haben potenzielle und bestehende Kunden die Gewissheit, dass die Inhalte, die sie herunterladen, authentisch sind und ihnen vertraut werden kann. Der Softwarehersteller konnte das Vertrauen der Benutzer in seine Marke stärken, Sicherheitswarnmeldungen beseitigen und den Internetverkauf seiner Software steigern.

Code Signing



Gewonnene Vorteile

Erhöhter Schutz der Umsatzerlöse

- Reduziert das Risiko interner/externer Kompromittierung und schützt so den Ruf der Marke und verhindert, dass Kosten für die Reparatur infizierter Rechner der Benutzer entstehen.
- Gewährleistet die Authentizität des Unterzeichners, die Integrität der Daten und die Nichtabstreitbarkeit von Dokumenten/Code

Erhöhte Kontrolle und einfaches Softwaremanagement

- Vereinfachte Schlüsselverwaltung zur Kontrolle der Verteilung der Software im Internet
- Benutzer können nur signieren, wenn sie Teil des Systems sind, das aus der Ferne verwaltet werden kann
- Kann von mehreren Build-Systemen aus aufgerufen werden

Erhöhte Sicherheit

- Trennung von Daten und Schlüsseln
- Private Schlüssel und andere notwendige Signaturberechtigungen werden in einer robusten Anwendung gespeichert

Geringere Kosten und verbesserte Compliance-Auditierbarkeit

- Vereinfachte Compliance – alle Aktionen sind auditierbar
- Kann zur unternehmensweiten Verschlüsselung verwendet werden – Konsolidierung und Vereinfachung der Verschlüsselung im gesamten Unternehmen

Umfangreiches Partner-Ökosystem

- Thales arbeitet mit vielen Code-Signing-Anbietern zusammen, darunter American Megatrends Inc., Adobe, Device Authority, Keyfactor, Microsoft und Venafi, und bietet Zertifikats- und Schlüssellebenszyklusdienste sowohl on-premises als auch in der Cloud an.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.

> cpl.thalesgroup.com/de <

Kontaktieren Sie uns – alle Geschäftsstellen und Kontaktangaben finden Sie auf cpl.thalesgroup.com/de/contact-us