



**ENTRUST**



# Entrust beschleunigt die Integration digitaler Zertifikate in Telefone von Polycom



## **GEMEINSAM MIT DEM PROFESSIONAL SERVICES TEAM UND DEN NSHIELD HSM VON ENTRUST VERBESSERT POLYCOM DIE VoIP-SICHERHEIT**

Polycom ist bekannt für seine charakteristischen dreieckigen Konferenztelefone. Das Unternehmen hat die geschäftliche Kommunikation in den frühen 1990er Jahren nachhaltig verändert, indem es die Zusammenarbeit unter Kollegen und Partnern weltweit einfacher, effizienter und angenehmer gemacht hat. Die Marke ist unter IT-Käufern weiterhin ein Synonym für Qualität, Übersichtlichkeit und Komfort. Der Markt für Voice-over-Internet-Protocol-Geräte (VoIP-Geräte) wächst stetig. Daher hat sich Polycom, die ein umfassendes Portfolio an VoIP-Telefonen vom Desktop bis hin zum Konferenzraum anbieten, entschlossen, seine Telefone zu verbessern. Diese sollten eine unverwechselbare Identität erhalten, so dass es einfacher ist, sie in Netzwerken von Kunden und Dienstleistern zu identifizieren und gleichzeitig mutmaßliche Fälscher und Betrüger abzuhalten. Wie funktioniert das? Mit digitalen Zertifikaten und kryptographischen Schlüsseln, die von nShield-®-Hardware-Sicherheitsmodulen (HSM) erstellt und gesichert werden.

„Unsere VoIP-Geräte können sich selbst mithilfe digitaler Zertifikate in einem Netzwerk authentifizieren“, erläutert Marek Dutkiewicz, Director of Product Management bei Polycom. „Da die Ausstellung der Zertifikate Teil des Herstellungsprozesses ist, können sich unsere Kunden und Partner einfacher authentifizieren und gleichzeitig potenzielle Fälscher oder Betrüger abhalten. Unser Erfolg beruht auf den nShield HSM von Entrust, die vom Entrust Professional Team bereitgestellt werden.“



**Entrust bot die nötige Fachkenntnis für die Entwicklung einer maßgeschneiderten, sicheren VoIP-Lösung. >>>**

- Marek Dutkiewicz, Polycom

**WEITERE INFORMATIONEN AUF [ENTRUST.COM/HSM](http://ENTRUST.COM/HSM)**

## **SICHERHEIT FÜR VoIP**

VoIP hat gegenüber traditioneller Telekommunikationstechnologie zwei Vorteile: geringere Kosten und die Möglichkeit zur Integration mit anderen IP-Anwendungen. Wie bei anderen Formen der internetbasierten Kommunikation gibt es jedoch auch Sicherheitsbedenken, wie z. B. die unsichere Identität von Geräten und Personen im Netzwerk.

VoIP-Telefone nutzen traditionell Passwörter zu Identifizierung. Dadurch war eine definitive Identitätsprüfung schwierig und führte zu längeren Einrichtungszeiten für Endbenutzer und Dienstanbieter. Darüber hinaus schützte dieses passwortbasierte Verfahren die Telefonhersteller nicht vor der Fälschung ihrer Geräte.

Dank digitaler Zertifikate konnten einige dieser Herausforderungen der passwortbasierten Sicherheit aus dem Weg geräumt werden. Anders als Passwörter eignen sich digitale Zertifikate für eine eindeutige Identifizierung. Dadurch können Geräte sich und das Netzwerk, das sie betreten, selbst authentifizieren. So kann ein Gerät mit einem gültigen Zertifikat beispielsweise verifizieren, ob es mit einem autorisierten Server verbunden ist, und der autorisierte Server kann im Gegenzug die Authentizität des Geräts überprüfen. Sicher erstellte und verteilte Zertifikate können nicht gefälscht werden. So ist es ganz einfach, Betrüger zu erkennen.

„Wenn Telefone manipuliert werden können, besteht das Risiko, dass Anrufe mit betrügerischer Absicht getätigt und fehlerhafte Rechnungen ausgestellt werden“, erklärt Dutkiewicz. „Polycom hat sich verpflichtet, Lösungen bereitzustellen, die die Bedürfnisse unserer Kunden erfüllen. Dazu gehört auch das Bedürfnis

nach Sicherheit. Indem wir Telefone anhand digitaler Zertifikate identifizieren, können wir die Sicherheitsrisiken deutlich senken. Uns wurde klar, dass wir eine Lösung benötigen, die uns erlauben würde, Zertifikate sowie einen dazugehörigen privaten Schlüssel zu erstellen, diese in die Telefone zu integrieren und dieses System während des gesamten Herstellungsprozesses beizubehalten.“

## **SUCHE NACH DEM RICHTIGEN PARTNER**

Sobald das Konzept feststand, machte sich Polycom auf die Suche nach der richtigen Lösung und einem Partner für die Umsetzung. Das Unternehmen besprach seine Optionen mit verschiedenen Technologieanbietern und Lösungsentwicklern, aber nur einer bot an, was Polycom suchte: erprobte Technologie, Erfahrung mit der Erstellung von kryptographischen Schlüsseln und der Ausstellung digitaler Zertifikate während der Fertigung sowie die Fähigkeit, einen sicheren End-to-End-Prozess zu entwickeln. Dieser Anbieter war das Professional Services Team von Entrust. Das Team machte deutlich, wie die nShield HSM von Entrust die Verfahren bei der Ausstellung digitaler Zertifikate und der Erstellung von Schlüsseln sichern. Das Wichtigste war jedoch, dass das Team zudem in der Lage war, eine Lösung zu entwickeln und umzusetzen, die in den Fertigungsprozess von Polycom integriert werden konnte.

„Wir haben uns also für nShield HSM von Entrust entschieden und unsere Lösung mit der Unterstützung des Professional Services Teams von Entrust umgesetzt“, erläutert Dutkiewicz. „Entrust bot die nötige Fachkenntnis für die Entwicklung einer maßgeschneiderten, sicheren VoIP-Lösung.“

« **Das Team von Entrust hat uns bei der Entwicklung und Implementierung eines Prozesses unterstützt, der die Anrufe unserer Kunden sowie unser Unternehmen vor Betrügern schützt.** »

- Marek Dutkiewicz, Polycom

## **ENTWICKLUNG EINES EFFEKTIVEN PROZESSES**

Das Professional Services Team von Entrust hat in enger Zusammenarbeit mit den Mitarbeitern von Polycom an der Entwicklung eines Prozesses gearbeitet, der die Bedürfnisse von Polycom eins zu eins erfüllt. Polycom gab vor, wie die Zertifikate in den Fertigungsprozess integriert werden sollten und das Professional Services Team von Entrust arbeitete ein detailliertes System mit den gewünschten Fähigkeiten aus.

Die Berater von Entrust entwickelten eine Lösung, die Schlüssel erstellt und mithilfe einer Zertifizierungsstelle (CA) von Microsoft digitale Zertifikate im Rechenzentrum von Polycom in Nordamerika signiert. Die Schlüsselerstellung und das Signieren der Zertifikate finden vollständig innerhalb der HSM-Umgebung statt. Anschließend werden die Schlüssel und Zertifikate auf die nShield HSM von Entrust in der Fertigungsanlage von Polycom in Thailand übertragen. Dort werden die Schlüssel und Zertifikate verschlüsselt gespeichert, bis sie in ein neu gefertigtes VoIP-Telefon implementiert werden.

„Wir wollten Schlüssel und Zertifikate in unserem Rechenzentrum erstellen und sicher zu der Fertigungsanlage und in neue Geräte transferieren“, erklärt Dutkiewicz. „Das wurde von Entrust wie gewünscht und benötigt umgesetzt. Das Team von Entrust hat uns bei der Entwicklung und Implementierung eines Prozesses unterstützt, der die Anrufe unserer Kunden sowie unser Unternehmen vor Betrügern schützt.“

## **SICHERE AUSFÜHRUNG**

Das Professional Services Team von Entrust verwendete nShield CodeSafe, die sichere Ausführungsumgebung innerhalb der nShield HSM, um die Erstellung, Übertragung und Implementierung von Schlüsseln und Zertifikaten umfassend zu schützen. CodeSafe ermöglicht es den nShield HSM von Entrust, eine Vielzahl an Prozessen in einer sicheren Umgebung auszuführen. Das Professional Services Team machte sich dieses zunutze, indem es Code schrieb, der Schlüsselpaare für Telefone erstellt, die Signierung von Zertifikaten anfordert und das verschlüsselte Paket an die Fertigungsanlage von Polycom überträgt. Das Team hat darüber hinaus ein Verfahren entwickelt, das eine Secure-Sockets-Layer-Verbindung (SSL-Verbindung) mit dem HSM am Fertigungsstandort initiiert, die im neu gefertigten Telefon endet. Diese Verbindung ermöglicht die sichere Bereitstellung von Schlüsseln und Zertifikaten in den Telefonen.

„Unsere nShield HSM von Entrust speichern die Zertifikate und privaten Schlüssel, mit denen Telefone sicher identifiziert werden können. nShield CodeSafe wiederum schützt den Ausstellungsprozess auf der anderen Seite des Globus“, erläutert Dutkiewicz. „Wir halten diesen Prozess für eine sehr effektive und sichere Möglichkeit, um die Ausstellung digitaler Zertifikat in unseren Fertigungsprozess zu integrieren.“

## VORTEILE EINER PARTNERSCHAFT MIT DEM PROFESSIONAL SERVICES TEAM VON ENTRUST:

- Schnellere Projektfertigstellung
- Sicherer Prozess, der Betrug und Fälschung verhindert
- Individuell an den Fertigungsprozess anpassbare Lösung
- Unübertroffenes Fachwissen im Bereich High-Tech-Fertigung

## UNTERNEHMENSPROFIL

Polycom, Inc. ist Weltmarktführer im Bereich Telepräsenz, Video und Sprachlösungen und ein Visionär auf dem Gebiet Unified Communications (UC), dessen Lösungen Menschen ermöglicht, sich von überall zu verbinden und zusammenzuarbeiten. Die Lösungen von Polycom bieten einen schnellen ROI und unterstützen Kunden dabei, Kosten zu senken, ihre Produktivität zu steigern und den CO2-Fußabdruck zu verkleinern – wichtig in der Wirtschaft von heute.

Weitere Informationen zu den UC-Lösungen von Polycom finden Sie auf [www.polycom.com](http://www.polycom.com).

## DER GRUNDSTEIN FÜR ANHALTENDEN ERFOLG

Laut Polycom hat der Geräteauthentifizierungsprozess mithilfe der nShield HSM unter dem Strich zwei große Vorteile für das Unternehmen: die Senkung des Fälschungsrisikos und erhöhte Absatzchancen.

„Egal wie authentisch ein gefälschtes Gerät erscheinen mag, ohne ein gültiges Zertifikat sollte es nicht in der Lage sein, ein autorisiertes VoIP-Netzwerk zu täuschen“, bemerkt Dutkiewicz. „Die nShield HSM von Entrust sind das Fundament des gesamten Prozesses – von der Herstellung zum alltäglichen Gebrauch des Telefons. Ich sehe sie als eine Art Banktresor, aber eigentlich sind sie noch sicherer. Am wichtigsten ist jedoch selbstredend, dass unsere Kunden davon profitieren. Kunden wünschen sich zweifelsohne Sicherheit ohne Probleme für ihre VoIP-Geräte. Wir sehen, dass digitale Zertifikate zur Steigerung unseres Umsatzes und Marktanteils beitragen.“

## ÜBER ENTRUST

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 Grenzüberritten, 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.