Große britische Bank bietet mit Entrust nShield HSMs Vertrauen und Sicherheit für jeden Zahlungsvorgang

Da Finanzkriminalität immer häufiger auftritt und mit immer raffinierteren Methoden agiert wird, arbeiten Banken und Finanzdienstleistungsunternehmen ständig an besseren Methoden zur Betrugsbekämpfung. Dazu gehört die Installation neuester Technologien genau wie die Benachrichtigung der Kunden, wenn etwas nicht stimmt. Dies und die Gewährleistung der Sicherheit des Geldes ihrer Kunden steht im Zentrum des Geschäfts einer führenden britischen Bank.

Die überarbeitete Zahlungsdiensterichtlinie (PSD2/Payment Services Directive) soll den Verbraucherschutz verbessern, Zahlungen sicherer machen und die Kosten für Zahlungsdienste senken. Die PDS2 reguliert alle Zahlungsdienstleister, die Zahlungen in den EU-Mitgliedsstaaten durchführen, und gilt für Unternehmen auf der ganzen Welt.

Zur Verbesserung der Sicherheit und Reduzierung von Betrug schreibt die PSD2 eine starke Kundenauthentifizierung (Strong Customer Authentication/SCA) vor. Einfach ausgedrückt bedeutet dies, dass mehr Checks für Kunden eingeführt werden, die Online-Banking nutzen, etwas online kaufen oder kontaktlose Zahlungen vornehmen.

> **« Wir sind seit vielen Jahren Kunde von Entrust und die Entrust nShield HSMs sind unsere bevorzugten HSMs für den Schutz der kryptographischen Schlüssel und Prozesse der Bank. Mit dem Web-Services-Optionspaket können wir unsere vorhandenen HSMs nutzen und sind in der Lage, Transaktionsdaten gemäß den PSD2-Anforderungen zu verschlüsseln und zu signieren. »**

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

Große britische Bank

GESCHÄFTLICHE PROBLEMSTELLUNG

Die Bank musste einen starken Kunden-Authentifizierungsmechanismus einführen, der die PSD2-Anforderungen erfüllt, um das Potenzial für Online-Betrug zu reduzieren. Dazu gehörte die Implementierung einer starken Zwei-Faktor-Authentifizierung (2FA), die es von mehr als 300.000 Kunden digitaler Bankdienstleistungen erfordern würde, ihre Identität und Transaktionsdetails schnell, einfach und kostengünstig zu bestätigen.

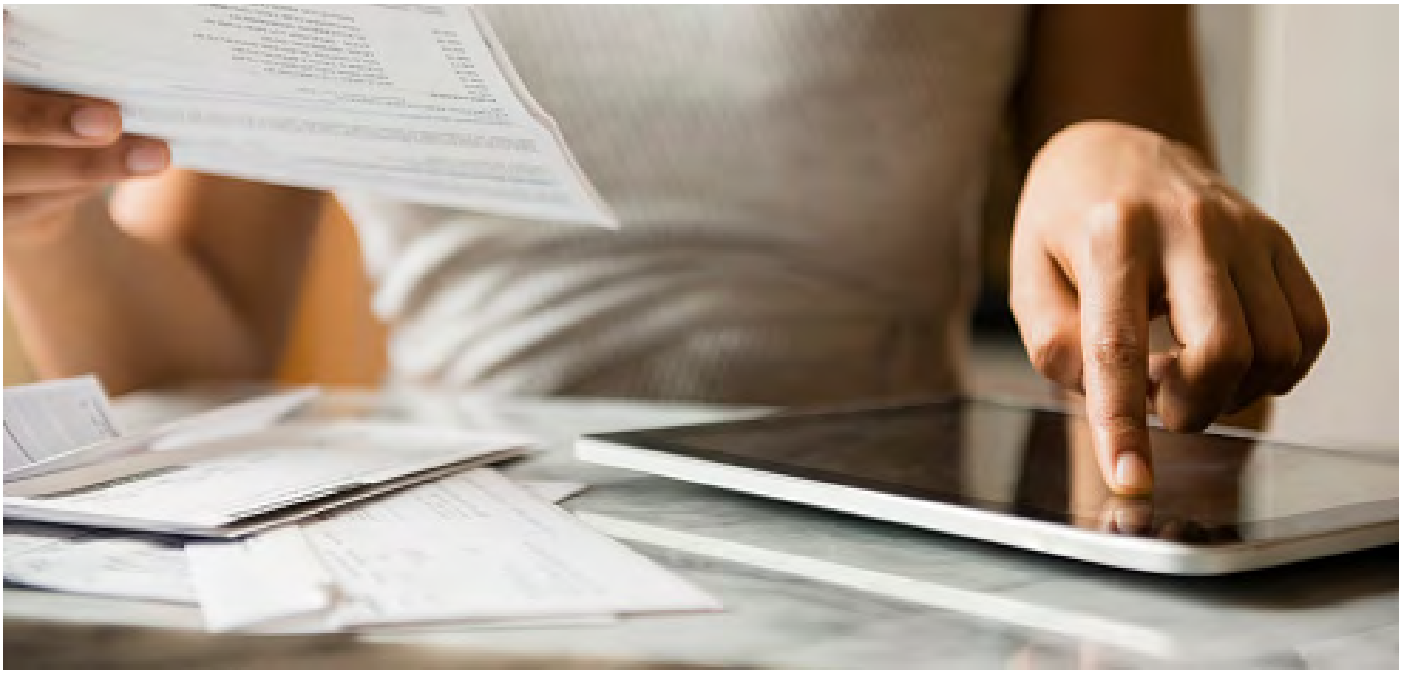
TECHNISCHE PROBLEMSTELLUNG

Zu den Änderungen der PSD2 gehört auch, dass die SCA die Einbeziehung sowohl des Transaktionsbetrags als auch des Zahlungsempfängers in den Authentifizierungsprozess erfordert. Die Einbeziehung von Transaktionsdaten in den 2FA-Prozess bedeutet, dass die Daten verschlüsselt werden müssen, um sicherzustellen, dass sie gesichert und vor Hackern oder böswilligen Eingriffen geschützt sind. Die Lösung musste auch in Echtzeit funktionieren können, ohne dass für den Endbenutzer eine Verlangsamung des Service sichtbar wird.

LÖSUNG

Die Bank stellte ihren Online-Banking-Kunden ein verbessertes Smartcard-Lesegerät mit einer Quick-Response-Code-Funktionalität (QR-Code) zur Verfügung, mit dem sie sich anmelden, Zahlungen autorisieren oder Änderungen in ihrer Nutzerverwaltung vornehmen können. Die Kartenlesegeräte verfügen über eine vollständige Anzeige und eine Scanfunktionalität anstelle des Challenge/Response-Verfahrens herkömmlicher Kartenlesegeräte.

Die Online-Banking-Anwendung zeigt einen QR-Code an, der die verschlüsselten Transaktionsdaten enthält. Der Kunde scannt den QR-Code mit dem Smartcard-Lesegerät, das dann die Details der Transaktion anzeigt. Wenn der Kunde mit dem, was er sieht, zufrieden ist, gibt er die Smartcard-PIN ein. Der Kartenleser zeigt dann einen Antwortcode an, der wieder in die Online-Banking-Anwendung eingegeben wird. Der Antwortcode wird dann überprüft und die Transaktion autorisiert.



Große britische Bank

> **Entrust und sein Professional Services Team unterstützten uns hervorragend. So konnten wir eine maßgeschneiderte Lösung entwickeln, die sowohl den Bedürfnissen der Bank als auch den Anforderungen der in der PSD2 festgesetzten SCA entspricht. Das Team von Entrust war sowohl gründlich als auch reaktionsschnell, was eine robuste, schnell einsetzbare und starke 2FA-Lösung ermöglichte.**

Um die Transaktionsdaten während des gesamten Prozesses zu schützen, müssen der Kartenleser verifiziert und die Transaktionsdaten verschlüsselt werden. So wird sichergestellt, dass sie zu keinem Zeitpunkt während des Prozesses manipuliert werden können.

In jedes der Smartcard-Lesegeräte ist ein öffentlicher Schlüssel eingebettet und die im QR-Code angezeigten Daten werden mit dem zugehörigen privaten Schlüssel verschlüsselt. Das bedeutet, dass der QR-Code nicht mit einem Standard-QR-Code-Scanner gelesen werden kann, sondern nur mit einem von der Bank ausgegebenen Smartcard-Lesegerät mit dem korrekten öffentlichen Schlüssel.

Die Bank nutzte für den Schutz ihrer kryptographischen Schlüssel und Prozesse bereits Entrust nShield® Hardware-Sicherheitsmodule (HSMs). Für die Speicherung und den Schutz der privaten Schlüssel, die zum Signieren der im QR-Code angezeigten Transaktionsdaten verwendet werden, wurden dieselben nach FIPS 140-2 zertifizierten HSMs zusammen mit dem Entrust nShield Web-Services-Optionspaket eingesetzt.

Das Entrust nShield Web-Services-Optionspaket bietet unabhängig von deren Standort Zugriff auf Entrust nShield HSMs und stellt eine REST API zwischen Anwendungen, die kryptographische Schlüssel und Datensicherungsdienste benötigen, zur Verfügung. Es bietet eine einfache, nahtlose Schnittstelle zwischen den Smartcard-Lesegeräten und den Entrust nShield HSMs, ohne dass ein Client installiert werden muss. Damit werden die Schwierigkeiten beseitigt, die eine Software-Installation auf eingebetteten Systemen wie Kartenlesern mit sich bringen kann.

Zudem war es eine kostengünstige Lösung, da nicht Hunderttausende von Clients lizenziert werden mussten. Einrichtung und Inbetriebnahme erfolgten schnell und einfach mit Hilfe des Professional Services Teams von Entrust. Die Bank benötigte eine maßgeschneiderte Anpassung des standardmäßigen nShield Web-Services-Optionspakets, die vom Professional Services Team entwickelt und eingerichtet wurde. Während des gesamten Projekts wurde dabei Hand in Hand mit dem entsprechenden Team der Bank gearbeitet.

Große britische Bank

Geschäftliche Problemstellung

Bereitstellung einer starker Kundenauthentifizierung (SCA) mit Zwei-Faktor-Authentifizierung (2FA) zur Erfüllung der PSD2-Anforderungen

Lösung

- Entrust nShield Connect HSMs
- Entrust nShield Web-Services-Optionspaket
  - Hochgradig zugängliche Verbindung zwischen Cloud-Anwendungen und HSM-Diensten
  - Einfache Schnittstelle, einfache Integration
  - Reduzierung von Kosten und Einrichtungszeit
- Entrust Professional Services Team

Resultat

Eine leistungsstarke Authentifizierungslösung in Echtzeit, die einfach zu implementieren war und für den Endbenutzer reibungslos funktioniert

RESULTAT

Die Bank kann ihren mehr als 300.000 Online-Banking-Kunden eine SCA-Option anzubieten, die der PSD2 entspricht und dazu beiträgt, ihre Unternehmen vor Betrug und Cyberangriffen zu schützen. Aufgrund des hohen Durchsatzes der Entrust nShield HSMs findet der Prozess der Transaktionsauthentifizierung in Echtzeit statt, was ihn für den Endbenutzer reibungslos und nahtlos macht. Die den speziellen Bedürfnissen angepasste Standardlösung war viel billiger und schneller zu implementieren als die anderen Optionen, die von der Bank in Betracht gezogen wurden.

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 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