



**ENTRUST**



# Entrust nShield HSMs sichern Fingervenens-Biometrik von Hitachi

**HITACHI**  
Inspire the Next

Wie Entrust hilft, eine BioPKI-Lösung zu sichern, die elektronische Signaturen von Dokumenten im Bankwesen erstellt.

## **DIE HERAUSFORDERUNG: EINE BAHNBRECHENDE AUTHENTIFIZIERUNGSTECHNOLOGIE IN EINER STARK REGULIERTEN BRANCHE ZU SICHERN**

Als einer der globalen Vorreiter bei der Entwicklung von Technologien für Verbraucher, Unternehmen und Behörden, erkannte Hitachi die Chance für sein biometrisches Fingervenens-Authentifizierungssystem, um digitale Signaturen im Bankwesen zu revolutionieren.

Die Fingervenentechnologie nutzt das Muster der Blutgefäße im Finger, um die Identität einer Person zu überprüfen – eine genaue, effiziente und fortschrittliche Form der biometrischen Authentifizierung. Im Hinblick auf das Bankwesen würde die Technologie von Hitachi bedeuten, dass Banken ihre Kunden in weniger als einer Sekunde identifizieren könnten, indem der Finger des Kunden in Echtzeit mit dem in der Datenbank gespeicherten Fingervenensprofil verglichen wird. Die Nutzung der Fingervenentechnologie würde den Verbrauch von Papierdokumenten sowie die Kosten für Drucken, Scannen, Indexierung, Archivierung und Vernichtung von Papierdokumenten erheblich reduzieren.

**WEITERE INFORMATIONEN AUF [ENTRUST.COM/HSM](https://www.entrust.com/hsm)**

Der Schlüssel zum Erfolg dieser Authentifizierungstechnologie im Bankensektor wäre die Sicherheit der biometrischen digitalen Signaturen, auch BioPKI genannt – eine Alternative zum traditionellen Modell der digitalen Signatur. Fingervenen-BioPKI ist eine Mischung aus Biometrik und PKI (publik key infrastructure, öffentliche Schlüsselinfrastruktur) und erfordert die Authentifizierung der Fingervenen, um den Zugriff auf private Schlüssel der Nutzer zu verwalten, die sicher im Back-Office-System der Bank gespeichert sind. Hitachi wusste, dass eine hochgradig sichere Lösung zum Schutz des Authentifizierungsprozesses und aller damit verbunden gespeicherten Daten vonnöten war, um im Bankensektor große Akzeptanz zu erreichen.

### **DIE LÖSUNG: DIE ROLLE VON ENTRUST HSMS**

Hitachi entschied sich für Hardware-Sicherheitsmodule (HSMs) von Entrust nShield® für seinen BioPKI-Einsatz in Mittel- und Osteuropa (MOE). Der Zugriff auf private Schlüssel der Fingervenen-Authentifizierung ist durch ein zertifiziertes Entrust nShield HSM geschützt, ein hochgradig sicheres und manipulationssicheres Gerät im Back-Office der Bank, wo es digitale Signaturen erstellt und geheime Schlüssel schützt. Die einzigartige CodeSafe-Funktion von Entrust wird verwendet, um benutzerdefinierten Code zur Erstellung von Signaturen innerhalb des zertifizierten Sicherheitsrahmens des HSM auszuführen.

Diese innovative biometrische Lösung wurde in Europa zum ersten Mal zur Kundenauthentifizierung in polnischen Bankfilialen verwendet. Aufbauend auf der Erfahrung, die Hitachi bei der praktischen Umsetzung von Projekten im Finanzsektor in Polen gewinnen konnte, empfahl das Unternehmen seinen BioPKI-Kunden den Einsatz von HSMs.

Die Entrust nShield HSM-Hardware wurde erfolgreich für biometrische digitale Signaturen in Banken wie der BZ WBK (Pilotprojekt in Filialen) und der Getin Noble Bank (Filialen und Geldautomaten) verwendet.

Die Lösung von Hitachi entspricht den Anforderungen der polnischen Gesetze zur Gänze. Dass die Erwartungen von Prüfern und Regulatoren erfüllt wurden, ist unter anderem der Verwendung von HSMs zur Speicherung und zum Schutz der privaten Schlüssel zu verdanken.

### **ÜBER DIE LÖSUNG**

#### **Entrust HSMs**

Entrust nShield HSMs bieten eine manipulationssichere Umgebung für sichere kryptographische Verarbeitung und Schlüsselverwaltung. nShield HSMs sind zertifiziert und erfüllen etablierte und neue Sicherheitsstandards für kryptographische Systeme und bleiben dabei höchst effizient. nShield HSMs isolieren und schützen kryptographische Vorgänge und Schlüssel für die kritischsten Anwendungen von Unternehmen.

nShield HSMs führen Verschlüsselung, digitale Signierung und Schlüsselverwaltung für eine Vielzahl von Anwendungen durch, darunter PKIs, SSL/TLS und Code Signing. nShield HSMs sind hochgradig sichere Alternativen zur softwarebasierten Kryptographie. Sie unterstützen alle führenden Algorithmen und bieten eine erstklassige ECC-Leistung.

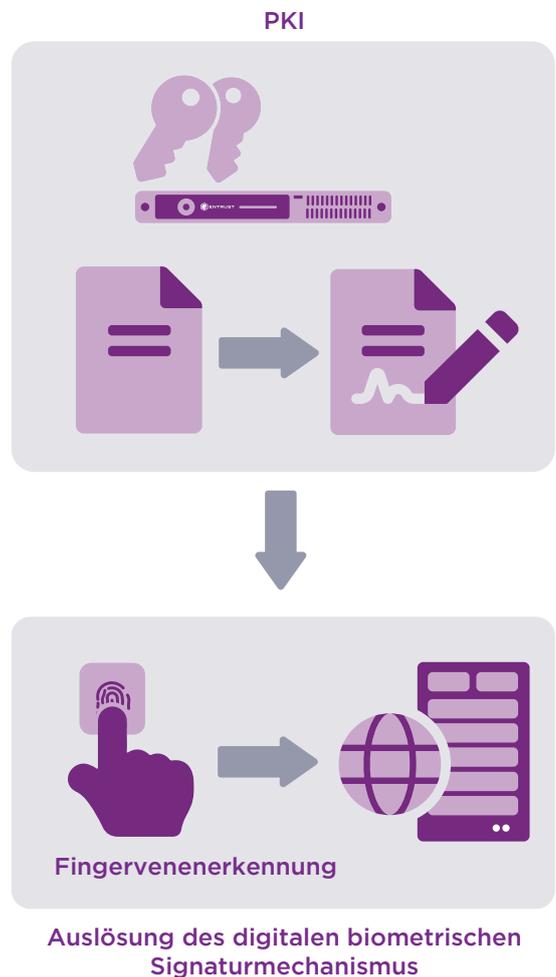
## Entrust CodeSafe

CodeSafe ist eine einzigartige Funktion der Entrust nShield HSMs, mit der Entwickler Anwendungen innerhalb der zertifizierten Sicherheitsgrenzen des HSM ausführen können. So sind sie vor Bedrohungen wie Insider-Angriffen, Malware und Trojanern geschützt, denen sie auf herkömmlichen Serverplattformen ausgesetzt wären.

### WARUM ENTRUST?

Hitachi entschied sich aus mehreren Gründen für Entrust nShield HSMs als bevorzugte Verschlüsselungstechnologie ihrer BioPKI-Lösungen am MOE-Markt:

- **Sicherheit.** HSMs bieten eine gefestigte, manipulationssichere Umgebung für sichere kryptographische Verarbeitung, Schlüsselschutz und Schlüsselverwaltung. Mit diesen Geräten konnte Hitachi Lösungen bereitstellen, die höchste Sicherheitsanforderungen sowie etablierte und neue Best Practices für kryptographische Systeme und bewährte Verfahren erfüllen – während gleichzeitig ein hohes Maß an betrieblicher Effizienz beibehalten wird.
- **Leistung.** „Von einem HSM wird ein hohes Maß an Sicherheit erwartet. HSMs bieten außerdem die herausragende Leistung, Skalierbarkeit und Verlässlichkeit, die erforderlich ist, um den Authentifizierungsprozess zu schützen und ausgewählten Code (in unserem Fall den Code zur Signaturerstellung) innerhalb der Grenzen des HSM zu installieren und auszuführen“, erklärte Przemysław Cychowski, Technical Director, Europa und CIS für Information Systems Group, Hitachi.



- **Bewährtheit.** Laut Tadeusz Woszczyński, Regional Director, Mittel- und Osteuropa und CIS für Information Systems Group, Hitachi, ist die „Verwendung einer bewährten Lösung wie Entrust nShield HSMs ein wesentliches Element unserer Strategie, die sicherste biometrische Signaturlösung im Bankwesen anzubieten.“

## HAUPTVORTEILE DER VERWENDUNG VON ENTRUST NSHIELD HSMs

- Automatisierung von risikoanfälligen administrativen Tätigkeiten, garantierte Schlüsselwiederherstellung und Eliminierung teurer und arbeitsintensiver Backup-Prozesse
- Ermöglichung einer sicheren Ausführung von benutzerdefiniertem, sicherheitskritischem Anwendungscode innerhalb der manipulationssicheren Grenzen der Hardware
- Unterstützung von hochvolumigen Transaktionen auf Unternehmensebene mit beschleunigten Transaktionsraten
- Vereinfachte Skalierung mit flexibler Architektur wenn die Sicherheitsanforderungen steigen
- Reduzierung der Kosten für Reisen zu Rechenzentren dank nShield Remote Administration
- Strenge Aufgabentrennung durch robuste Verwaltungsrichtlinien wie rollenbasierter Multifaktor-Authentifizierung und Quorum-Authentifizierung

## 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.