



**ENTRUST**

# Rahmenuntersuchung für öffentliche Schlüsselinfrastruktur (PKI)

PKI-Implementierung oder -Upgrade richtig planen

## ECKPUNKTE

- Expertenanalyse Ihrer Anforderungen, Wünsche, Einschränkungen und Prioritäten liefert kosteneffizienten und praktischen Ansatz für die Implementierung oder das Upgrade Ihrer PKI
- Dank jahrzehntelanger Erfahrung mit PKIs (öffentliche Schlüsselinfrastruktur, Public Key Infrastructure) kann Entrust durchdachte Optionen und Empfehlungen für PKI-Design, -Richtlinien und -Governance sowie Implementierungspläne anbieten, die zu Ihren Sicherheits- und Geschäftsbedürfnissen passen
- Erweiterte Sicherheit dank Planung in Entrust Hardware-Sicherheitsmodulen (HSMs), die sich bereits in Tausenden von weltweit bereitgestellten Einheiten bewährt haben

Viele Unternehmen nutzen eine öffentliche Schlüsselinfrastruktur (Public Key Infrastructure, PKI) für die Bereitstellung digitaler Zertifikate und sichern so wichtige Assets. PKIs werden für verschiedene Zwecke genutzt. Dazu zählen Authentifizierung, digitale Signaturen und Verschlüsselung.

Die Bedeutung der Unternehmens-PKI nimmt üblicherweise mit der Zeit zu geht oft bald über die Zwecke, wofür sie ursprünglich geschaffen wurde, hinaus, da stets neue Anforderungen für die PKI entstehen. Es ist unerlässlich, dass die PKI das Maß an Sicherheit bieten kann, die seiner zentralen Rolle entspricht. Darüber hinaus muss sie die aktuellen und potenzielle zukünftige Anforderungen des Unternehmens unterstützen.

Ein Upgrade der Unternehmens-PKI oder die Implementierung einer neuen erfordert eine Analyse der Anwendungsfälle, Sicherheitsanforderungen, Systemkompatibilität, Unternehmenspläne und -wünsche sowie der Compliance-Anforderungen.

Ein PKI-Projekt in Angriff zu nehmen, kann aufgrund der großen Bandbreite an Optionen und Möglichkeiten zunächst etwas einschüchternd wirken. Das Team von Entrust Professional Services (PS) hilft Ihnen aber dabei, die sicherheitsbezogenen, technischen und betrieblichen Aspekte für Ihr Implementierungs- oder Upgrade-Projekt zu planen.



# PKI-Rahmenuntersuchung

## Hauptbestandteile

Ein Entrust PS-Berater wird sich im Zuge der PKI-Rahmenuntersuchung den folgenden Faktoren widmen:

- Analyse Ihrer Anwendungsfälle für die PKI
- Kennenlernen Ihrer PKI-Anforderungen, Einschränkungen und vorhandenen Unternehmens-PKI (falls vorhanden)
- Bewertung der Sicherheitsrisiken für von der PKI abhängige Systeme und somit die Ermittlung der erforderlichen PKI-Sicherheitsebene
- Analyse der PKI-Übergangsanforderungen und -optionen
- Auswahlempfehlung
- Entwicklung eines empfohlenen, vorläufigen PKI-Designs
- Erstellung eines Plans für das PKI-Implementierungsprojekt (oder die Projekte)

## Das Verfahren der PKI-Rahmenuntersuchung

Vor Beginn der Untersuchung erstellt Entrust eine gegenseitige Vertraulichkeitsvereinbarung zum Schutz Ihrer und unserer Daten, und um eine offene Diskussion zu ermöglichen.

Die PKI-Rahmenuntersuchung ist in drei Phasen unterteilt.

### Phase 1: Datenerhebung

Ein Berater wird bei Ihnen vor Ort mittels Meetings und Workshops mit den wichtigsten Stakeholdern Ihres Unternehmens alle notwendigen Daten erheben. Dies erfolgt über einen detaillierten Entrust-Fragebogen. Die Erfahrung zeigt, dass dies effektiver ist, als den Unternehmen Fragebögen zukommen zu lassen, die ohne damit verbundene Gespräche und

Erklärungen ausgefüllt werden. Die Fragebögen können auch im Vorhinein zur Verfügung gestellt und dann von Ihrem Team und dem Entrust-Berater in gemeinsamen Meetings im Detail besprochen werden.

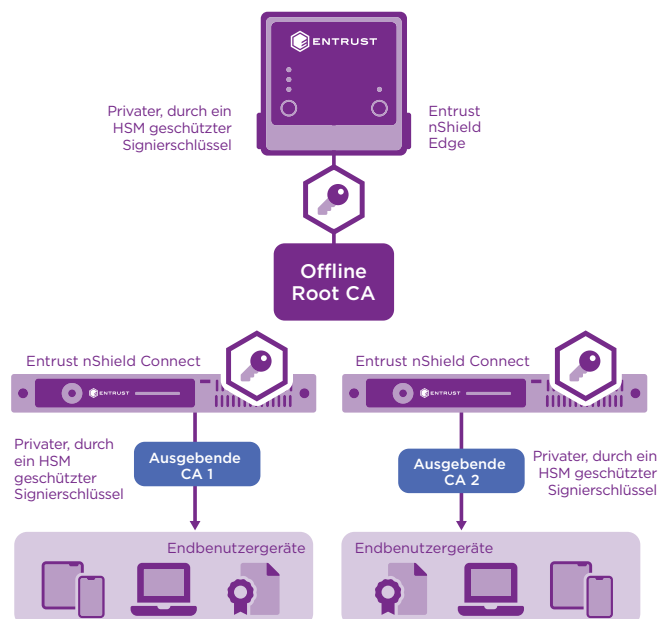
Alle im Rahmen dieser ersten Phase gesammelten Informationen werden in den Bericht aufgenommen, den Sie von Ihrem Berater erhalten.

### Phase 2: Analyse und Bericht

Anschließend analysiert der Berater die in Phase 1 erhobenen Daten, hält durch E-Mails und Telefonate Rücksprache, falls Klärungsbedarf besteht, und erstellt einen Bericht mit folgenden Inhalten:

- PKI-Anwendungsfälle
- Aktuelle Umgebungen
- PKI-Anforderungen
- Vorläufiges PKI-Design und -Empfehlungen
- Implementierungsplan

Die Lösung wird auf jener PKI-Software basieren, die für Ihr Unternehmen am besten geeignet ist und Entrust HSMs zum Schutz privater Schlüssel nutzen.





# PKI-Rahmenuntersuchung

## Phase 3: Managementpräsentation

Der Berater präsentiert die Ergebnisse der Rahmenuntersuchung dann der Managementebene vor Ort und finalisiert den Bericht anhand des erhobenen Feedbacks.

## Entrust HSMs

Entrust nShield® HSMs gehören zu den leistungsstärksten, sichersten und am einfachsten integrierbaren HSM-Lösungen am Markt. So erleichtern sie die Einhaltung regulatorischer Vorschriften und bieten höchste Daten- und Anwendungssicherheit für Unternehmen sowie Finanz- und Regierungsbehörden.

Unsere einzigartige Security World-Architektur für die Schlüsselverwaltung bietet starke, granulare Schlüsselkontrollen hinsichtlich Zugriff und Nutzung.

## Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf [entrust.com/HSM](https://entrust.com/HSM). Auf [entrust.com](https://entrust.com) erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

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**

