



Nexus Certificate Manager

Certificate Manager ist vermutlich die weltweit flexibelste mandantenfähige PKI-Plattform für Unternehmen, staatliche Einrichtungen, Militär, Serviceanbieter etc. vom PKI-Spezialisten Nexus. Elektronische IDs (digitale Zertifikate) lassen sich in nahezu jedem Format und für jede Anwendung in Netzwerken und Systemen ausstellen, nutzbar im Unternehmensumfeld ebenso wie für Internet- und mobile Dienste oder Komponenten der IT-Infrastruktur.

PUBLIC KEY KRYPTOGRAPHIE ist eine der praxistauglichsten Neuerungen der Mathematik des 20. Jahrhunderts mit einem gewaltigen Einfluss auf die Computer-Sicherheitstechnologie.

Public Key Infrastrukturen (PKI) bieten eine hoch skalierbare Sicherheitsinfrastruktur für sichere Identifizierung, Authentifizierung, Vertraulichkeit und Datenintegrität bei der elektronischen Kommunikation und der Nutzung elektronischer Dienste. In einer Ära globaler Kommunikation und massiver Verbreitung von Internetdiensten und vermehrt mobilen Diensten, bietet PKI einen generischen Sicherheitsmechanismus für verschiedenste Anwendungen. Der Einsatz von PKI ist in einigen Anwendungsgebieten gar unumgänglich.

PKI stellt Nutzern elektronische Identitäten (eID) aus und liefert die Strukturen zur Verwaltung und Validierung derselben während ihres gesamten Lebenszyklus. Die eIDs können quasi als Ausweis angesehen werden, mit dem der Fernzugriff auf Ressourcen, der Zugang zur Kommunikation und Zusammenarbeit über Firmennetzwerke und öffentliche Netzwerke ermöglicht wird und höherwertige Transaktionen elektronisch abgewickelt werden können.

Nexus Certificate Manager ist vermutlich die weltweit umfassendste und flexibelste PKI Plattform überhaupt. Er bietet eine hoch skalierbare, hochsichere Plattform zur Ausstellung, Verwaltung und Validierung von jeglicher Art PKI-basierter elektronischer IDs, sogenannter digitaler Zertifikate: Nutzerzertifikate, Chipkarten, Hardware-Token, Software-Token, Zertifikate für Desktoprechner, Server, Router,

Was ist ein digitales Zertifikat?

Ein digitales Zertifikat beinhaltet:

- die Identitätsdaten des Zertifikatsinhabers
- den einzigartigen öffentlichen Schlüssel des Zertifikatsinhabers
- die Zertifikatsgültigkeitsdauer
und
- die digitale Signatur der CA, die die genannten Angaben verbindlich beglaubigt

VPN Gateways, Netzwerkgeräte und eingebettete Systeme. Die Compliance mit gültigen Standards sichert die Nutzung von eIDs über Anwendungen verschiedener Anbieter auch in größeren verteilten Umgebungen.

Nexus Certificate Manager kann an beliebige Sicherheitspolicies, eID-Formate, Datenquellen und Verzeichnisdienste angepasst werden. Die eingebauten Funktionalitäten wie Schlüsselverwaltung, Kartenverwaltung und PIN-Druckfähigkeit ermöglichen den kostengünstigen Einsatz als Einzelplattformlösung für elektronische IDs.

Trustservice-Anbieter profitieren von der Mandantenfähigkeit:

Zertifizierungsdienste für verschiedene Kundenunternehmen können auf ein und demselben System verwaltet werden, bei sicherer Trennung der Nutzerdaten und Richtlinien.

Nexus Certificate Manager erstellt eIDs für Millionen von Nutzern. Ihm vertrauen viele große Regierungseinrichtungen, Verteidigungsorganisationen, Banken und Unternehmen überall auf der Welt.

Nexus

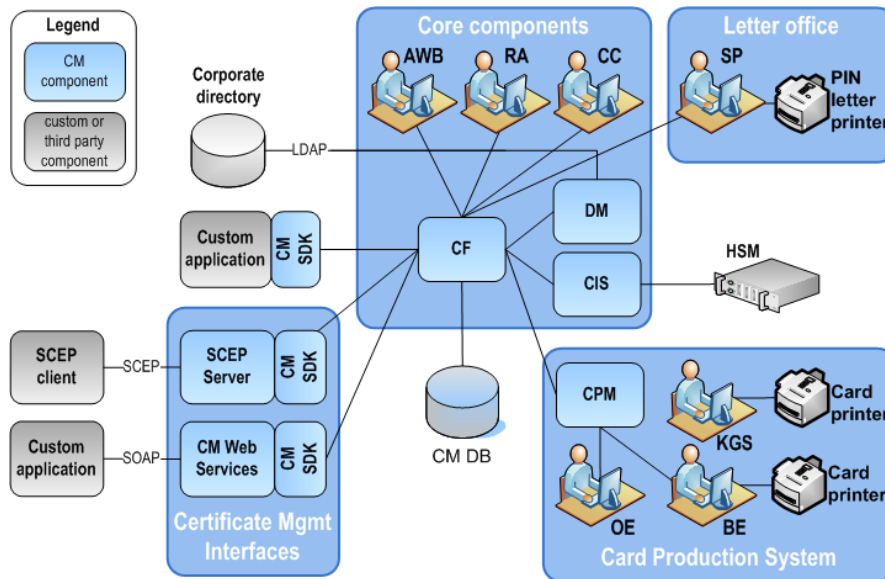
www.nexusafe.com
contact@nexusafe.com



Identifying and Authenticating
the Connected World



PRODUCT SHEET



Nexus Certificate Manager ist die universale CA-Plattform, die die Erstellung und die Lebenszyklusverwaltung PKI-basierter Berechtigungsnachweise unterstützt. Dazu zählen bspw.:

- Elektronische Identitäten (eIDs) für Staatsbürger zur sicheren grenzüberschreitenden Identifikation und für eine starke Authentifizierung bei der Online-Nutzung von E-Government-Diensten
- Berechtigungsnachweise für Bank- und Versicherungskunden zum sicheren Zugriff auf private Konten, zum elektronischen Vertragsabschluss und Abwickeln elektronischer Transaktionen
- Berechtigungsnachweise für Endkunden des Handels beim Interneteinkauf
- Zugangsberechtigungsdaten für Mitglieder von Arbeitsnetzwerken, die gemeinsame Ressourcen per Fernzugriff teilen und streng vertrauliche Daten austauschen
- Zugangsdaten für Firmenmitarbeiter, die sich damit in das Firmennetzwerk über PC, VPN oder Smartphone einloggen
- Zugangsdaten für Kunden von Cloud-Services zum Zugriff auf dedizierte Daten und Anwendungen bei externen Cloud-Service Providern
- Zugangsberechtigungsdaten für Computer einer Netzwerkdomäne für die Authentisierung beim Domaincontroller

- Router und Firewalls zur Einrichtung verschlüsselter, integritätsgesicherter Kommunikationskanäle

Umfassende, universale CA-Plattform

Nexus Certificate Manager ist für die großflächige Verwendungen elektronischer IDs in Regierungseinrichtungen, bei Trustcenter-Anbietern (TSPs), Telekommunikationsbetreibern und Finanzinstitutionen entwickelt worden, ebenso wie für den Einsatz in mittelgroßen Unternehmen und Organisationen.

Nexus Certificate Manager beinhaltet alle notwendigen Funktionen einer Zertifizierungsstelle (CA): hochflexible Registrierungs-, Ausstellungs- und Sperrprozesse, CA-Policy-Management, Cross-Zertifizierungen, Ausgabeschnittstellen, Erstellung und Veröffentlichung der Zertifikate und Sperrlisten an Verzeichnisse und OCSP Responder, Schlüsselarchivierung und Wiederherstellung, Erstellung von Chipkarten und PIN-Briefen in Stapelverarbeitung, Nutzer- und Zugangsverwaltung über GUI.

Die Plattform für alle PKI Anwendungen

Nexus Certificate Manager bewältigt jede beliebige Anzahl an CAs mit individuellen Policies, individuellen Ausgabe- und Wartungsprozessen und separaten Gruppen von Policy-Administratoren.





PRODUCT SHEET

Die Flexibilität der Konfiguration ermöglicht die Implementierung beinahe jeder Policy und verschiedenster Ausstellungsabläufe sowie die Einbindung in jede IT-Umgebung.

Standardschnittstellen unterstützen die Zertifikatsausstellung und die Lebenszyklusverwaltung sowie die automatische Auslieferung beim Abruf über externe Systeme. Die Zertifikate lassen sich zum Login am Rechner oder im VPN ebenso nutzen wie zur starken Nutzerauthentifizierung für die Daten- und E-Mailverschlüsselung, die Signatur von Dokumenten, für rechtsverbindliche digitale Signaturen, verschlüsselte ITSec und WIFI - Kommunikation, Domänen-authentifizierung und vielem mehr.

Konform mit Standards und Drittanbietern

Nexus Certificate Manager erfüllt alle Konformitätsansprüche für PKI Standards, Sperrlisten, Chipkarten und Schnittstellen für die Zertifikatsverwaltung. Dies stellt sicher, dass CA-Anfragen entsprechender Clients bedient und Zertifikate produziert werden, die von standardkonformen Anwendungen auch in großen herstellerneutralen Anwendungsumgebungen verstanden werden. HSMs und Chipkarten der großen Anbieter werden unterstützt.

Sicher mit Mandantenfähigkeit

Auf einer einzelnen Instanz des Nexus Certificate Manager können CAs vieler verschiedener Unternehmen betrieben werden, bei sauberer Trennung von Nutzungsdaten und Zugangsrechten auf dieser Plattform.

Vertrauen Sie Common Criteria EAL3+ evaluierter Sicherheitsarchitektur

Nexus Certificate Manager verwendet eine starke Nutzerauthentifizierung und granulare, rollenbasierte Zugangskontrollen für Nutzer und CAs. Jede Transaktion erfordert eine Signatur durch den Nutzer und wird im fälschungssicheren Protokoll geloggt. Subsysteme kommunizieren über verschlüsselte, integritätsgesicherte Kanäle. Sensible Daten wie Schlüssel und PINs werden bei Übertragung oder Speicherung immer verschlüsselt. Nexus Certificate Manager ist Common Criteria EAL3+ evaluiert und erfüllt die Bestimmungen der Europäischen Signatur-Richtlinie und des dt. Signatur-



Nexus Certificate Manager überschreitet Compliance-Anforderungen

turgesetzes. Die im Markt bewährte Technologie eignet sich für hochsichere Verwendung und kann für nahezu jedes Rollenkonzept und jede Zertifikatspolicy heran-gezogen werden.

Plattformunabhängige Unterstützung

Nexus Certificate Manager kann auf Windows und RedHat Linux betrieben werden und unterstützt verschiedene Datenbanken, einschließlich SQL Server, Oracle und MySQL.

Ausfallsicherheit, Skalierbarkeit und Verfügbarkeit

Nexus Certificate Manager hat seine Leistungsfähigkeit in kritischen großmaßstäblichen Multi-CA-Umgebungen bewiesen. Es ist möglich, alle Services mit hoher Leistung auf einem Host zu betreiben. Das System kann weiter ausgebaut werden, indem Prozesse auf mehrere Hostservern verteilt werden. Hochverfügbarkeit kann über eine aktiv/passiv Clusterkonfiguration sichergestellt werden, die mehrere HSM Instanzen enthält.

Die Quintessenz

PKI ist die beste verfügbare Technologie zur Authentifizierung, Verschlüsselung, Integritätssicherung und für digitale Signaturen in großen, verteilten Umgebungen und stellt eine grundlegende Sicherheitsinfrastruktur zur Verfügung. Digitale Zertifikate sind die elektronischen IDs der Nutzer für Datenzugriff und Dienste oder für den Abschluss hochwertiger kommerzieller Transaktionen. Nexus Certificate Manager bietet eine hochsichere standardbasierte, skalierbare, mandantenfähige, hochperformante und plattformunabhängige Lösung für externe Anbieter von Zertifizierungsdiensten und für Unternehmen, die sich eine kosteneffiziente, flexible haus eigene CA-Lösung wünschen.

