

EINE MANAGED PKI – DIGITALE ZERTIFIKATE FÜR JEDE ORGANISATIONSGRÖSSE

indevis bietet IT-Sicherheits- und Netzwerk-Lösungen auf höchstem Niveau für Unternehmen und Behörden jeder Größenordnung. Unser Produktportfolio wird durch unsere managed Security Services (**SaaS**) ergänzt. Unsere Public Key Infrastructure (**PKI**) indevis PKI (**iPKI**) auf der Basis von *Nexus Certificate Manager* ist eine hoch-flexible mandantenfähige PKI-Plattform für Unternehmen, staatliche Einrichtungen, Serviceanbieter, etc. Elektronische IDs (digitale Zertifikate) lassen sich in nahezu jedem Format und für jede Anwendung in Netzwerken und Systemen ausstellen. Diese IDs sind nutzbar im Unternehmensumfeld sowie für Internet- und mobile Dienste oder Komponenten der IT-Infrastruktur. Unsere managed PKI als Security Service ist sofort verfügbar und erfordert keine zusätzliche Software, keine Hardware und keinen Wartungsaufwand durch Ihre eigenen IT-Experten. Unsere PKI ist kompatibel mit zahlreichen Netzwerkprodukten verschiedenster Hersteller.



Die indevis GmbH bietet auf der technologischen Basis von Nexus Certificate Manager (www.nexussafe.com) eine zentrale PKI-Lösung für Organisationen jeder Größe. Die Technologie eignet sich hervorragend für die Ausgabe von elektronischen Identitäten in den Bereichen Internet, mobile Dienste und Komponenten der IT-Infrastruktur.

Mit den Produkten von Nexus setzen wir eine Lösung ein, die sowohl von der technologischen Reife, als auch von der Umsetzungsfähigkeit als Markt- und Technologieführer eingestuft wird. Die Lösung ist branchenübergreifend im Einsatz.

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

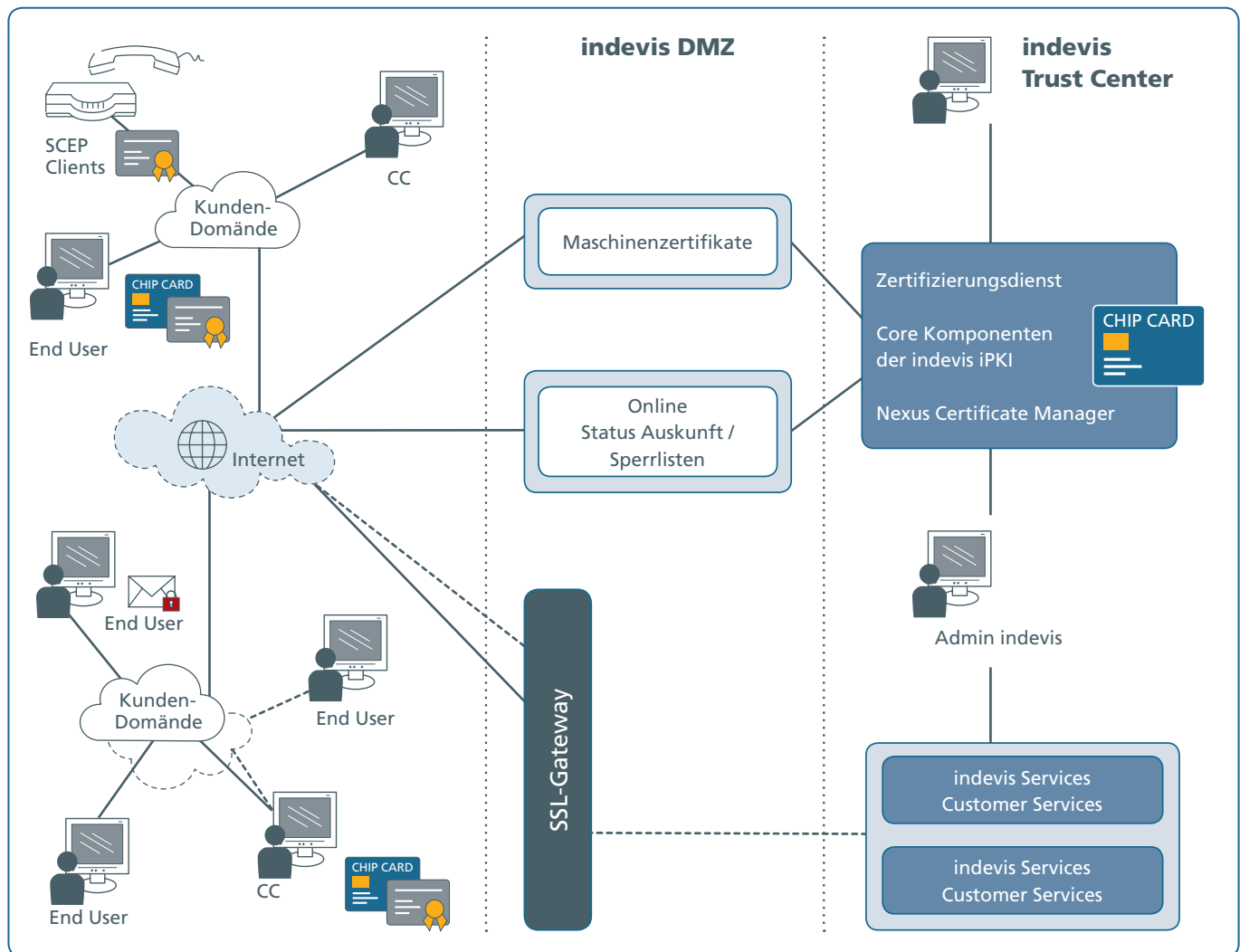
PUBLIC KEY KRYPTOGRAPHIE ist eine der praxistauglichsten Neuerungen der Mathematik des 20. Jahrhunderts mit einem gewaltigen Einfluss auf die Computer- Sicherheitstechnologie.

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 eine PKI einen generischen Sicherheitsmechanismus für verschiedenste Anwendungen. Der Einsatz einer PKI ist in einigen Anwendungsgebieten gar unumgänglich.

Eine 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. Die innerhalb einer PKI ausgestellten Zertifikate werden unter anderem zur Absicherung rechnergestützter Kommunikation verwendet.

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, 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.

Regierungseinrichtungen, Verteidigungsorganisationen, Banken und Unternehmen überall auf der Welt vertrauen Nexus.



indevis liefert die Nexus Certificate Manager Technologie als Cloud Service und ermöglicht Kunden damit einen sicheren Geschäftsbetrieb. Bisher war der Betrieb einer PKI sehr komplex und kostenintensiv. Der PKI Cloud Service von indevis ermöglicht die Nutzung einer PKI ohne Investitionen in IT-Systeme, Lizenzen und Wartung. Unser PKI Cloud Service ist flexibel und erhöht Ihre Sicherheit signifikant ohne größere Implementierungsprojekte.

managed indevis PKI (iPKI) bietet Ihnen folgende Vorteile:

- Einzigartige Unterstützung sowohl von Soft Token als auch von physischen Token und bietet eine auf anerkannten Standards basierende PKI Sicherheit zur Nutzerbeglaubigung und elektronischen Unterschrift. Es ermöglicht Kunden, e-Business Dienstleistungen ohne Kompromisse bei der Sicherheit anzubieten.
- Die managed indevis PKI (iPKI) ist von der Authentifizierung von internen elektronischen Identitäten in kleinen Unternehmen bis hin zu den Anforderungen großer Organisationen skalierbar und ist in der Lage, Millionen von Zertifikaten zu erstellen und zu verwalten.
- Wir realisieren den kompletten elektronischen ID-Produktionsprozess, vom Generieren des Schlüssels über die Profilierung der Smart Card bis zur Zuteilung des PIN-Codes an den Endnutzer.
- Wir erstellen Schlüssel und Zertifikate für Software wie Browser, Webserver, Smart Cards, VPN-Geräte usw. Skalierbar, mit der Möglichkeit, bis zu 40.000 Zertifikate pro Stunde auszustellen.
- Skalierbar von wenigen Zertifikaten bis größten Mengen.
- Zentralisierte oder dezentralisierte Verwaltung der Regeln und Prozesse.
- Durchgängige Unterstützung der Archivierung und Wiederherstellung von Schlüsseln.

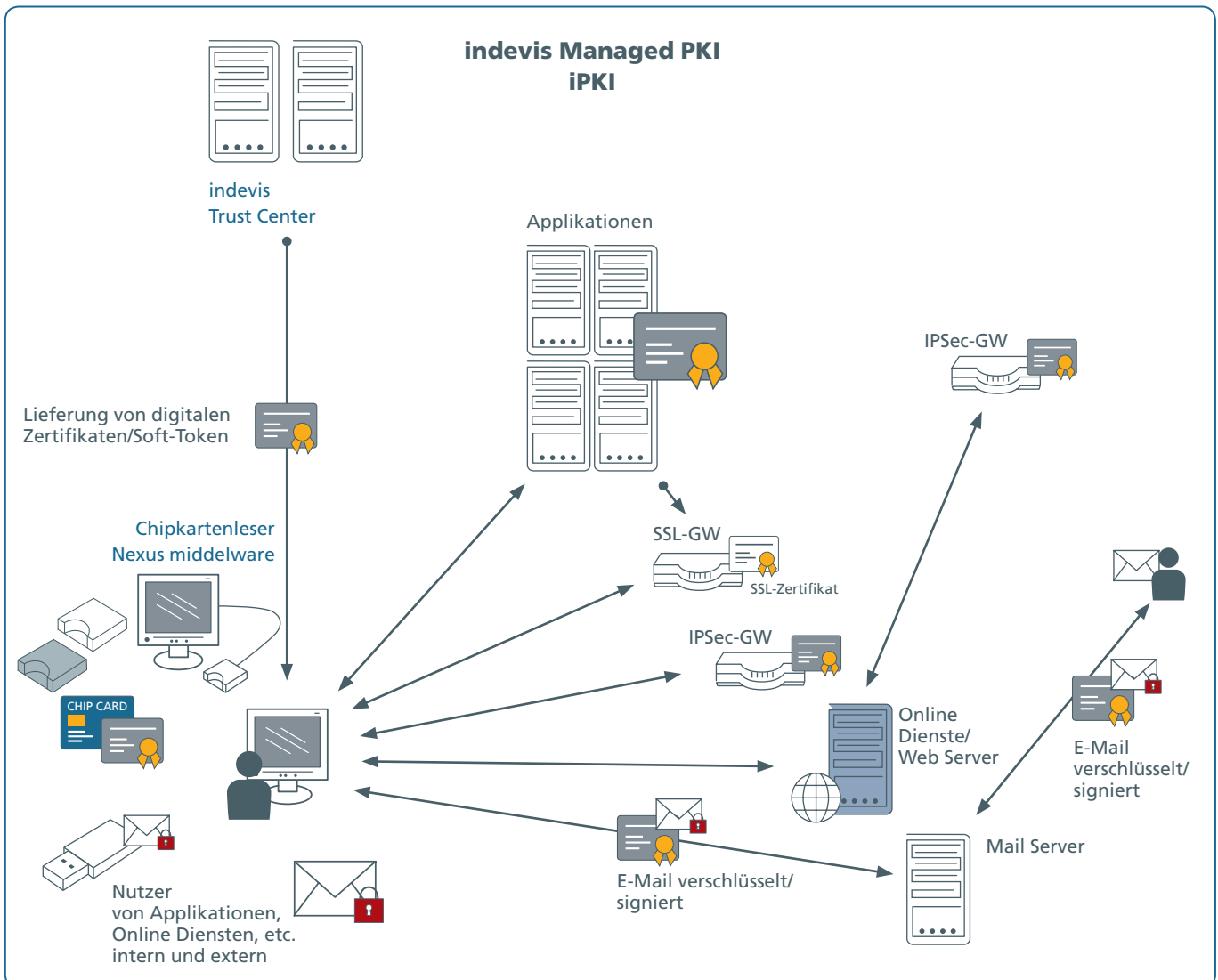
DIE ANZAHL VON STANDARDAPPLIKATIONEN, WELCHE DIGITALE IDENTITÄTEN (EID) NUTZEN KÖNNEN, HAT SEHR STARK ZUGENOMMEN.

Anwendungsszenarien für Maschinenzertifikate:

- Signierung und Verschlüsselung von E-Mails
- Signierung von Dokumenten in MS Office
- Signierung von PDF-Dokumenten
- Verschlüsselung von Ordnern und Daten
- Sicherer Remote Access (VPN)
- Digitale Unterschrift von Verträgen
- Sicherer Zugriff auf kritische Applikationen
- Sicherer Windows Login
- Berechtigungsnachweise für Endkunden beim Interneteinkauf
- Zugangsberechtigungsdaten für Mitglieder von Arbeitsnetzwerken
- Fernzugriff auf streng vertrauliche Daten
- Zugangsdaten für Kunden von Cloud-Services zum Zugriff auf dedizierte Daten und Anwendungen bei externen Cloud-Services
- Zugangsberechtigungsdaten für Computer einer Netzwerkdomäne für die Authentisierung beim Domaincontroller
- Router und Firewalls zur Einrichtung verschlüsselter, integritäts gesicherter Kommunikationskanäle
- Identifikation mobiler Geräte wie Notebooks, Smartphones, iPhone, iPad, Blackberry, etc.

Zentrale Dienste für den Endbenutzer bzw. Personenzertifikate:

- Ausgabe von Token mit digitalen Identitäten an Benutzer
- Freie Auswahl beim Token-Typ:
 - USB Token mit dem Sicherheitsniveau einer Smart Card, aber ohne Notwendigkeit eines Kartenlesegeräts – per Postversand
 - Soft Token – ausgeliefert über das Web oder per E-Mail
 - Smart Card und Card Reader – per Postversand
 - Alle Token oder Zertifikate sind durch eine PIN geschützt – Auslieferung der PIN direkt an den Benutzer per SMS
 - Alle Identitäten können online verifiziert werden (OCSP) oder von einer Sperrliste
 - Token können über ein Web-Portal blockiert werden (Revocation)
 - Vergessene Token können wieder hergestellt werden
 - SSL-Zertifikate können neu ausgestellt werden
 - Public Keys können an Directories gekoppelt werden
 - Veröffentlichung von Zertifikaten an Active Directory oder LDAP



FULL PKI-SERVICE DURCH INDEVIS

indevis liefert die PKI-Services direkt an den Endbenutzer. Das ermöglicht einen schnellen Service mit minimaler Administration auf Kundenseite. Vereinbarte SLAs, keine versteckten Kosten und 2nd und 3rd Level Support garantieren Kundenzufriedenheit.

UMFASSENDE, UNIVERSALE CA-PLATTFORM

Die managed indevis PKI (iPKI) 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 (Online Certificate Status Protokoll) Responder, Schlüsselarchivierung und Wiederherstellung, Erstellung von Chipkarten und PIN-Briefen in Stapelverarbeitung, Nutzer - und Zugangsverwaltung über GUI.

DIE PLATTFORM FÜR ALLE PKI ANWENDUNGEN

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, Domänenauthentifizierung und vielem mehr.

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. Signaturgesetzes. Die im Markt bewährte Technologie eignet sich für hochsichere Verwendung und kann für nahezu jedes Rollenkonzept und jede Zertifikatspolicy herangezogen werden.

AUSFALLSICHERHEIT, SKALIERBARKEIT UND VERFÜGBARKEIT - PKI FÜR JEDE ORGANISATIONSGRÖSSE

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. Mit Nexus Certificate Manager bietet die indevis GmbH eine hochsichere standardbasierte, skalierbare, mandantenfähige, hochperformante und plattform-unabhängige Lösung für Unternehmen, die sich eine kosteneffiziente, flexible CA-Lösung wünschen.

Weitere Informationen zu unseren Produkten und Dienstleistungen finden Sie im Internet unter:

www.indevis.de

Kontaktperson: Herr Andreas Mayer

Telefon: +49 (89) 45 24 24-103

eMail: andreas.mayer@indevis.de

WIR VERKAUFEN ZEIT – DURCH LÖSUNGEN DIE SICHER LAUFEN!

indevis IT Consulting and Solutions GmbH

Grimmstrasse 1
80336 München

Telefon +49 (89) 45 24 24-100
Telefax +49 (89) 45 24 24-199

info@indevis.de
www.indevis.de