



primeID CERTIFY

Die Basis für zertifizierte Sicherheit

PKI FÜR JEDEN ANWENDUNGSFALL

- Migration von Legacy-CAs auf eine moderne, mandantenfähige, flexible High-Performance-PKI
- PKI-Bereitstellung und Zertifikatsausgabe für DevOps und Microservices automatisieren
- Vertrauenswürdige Identitäten für IoT-Geräte und vernetzte Fertigungsumgebungen
- Hervorragende Skalierbarkeit für umfangreiche Deployments durch Datenbank-Tier-Clustering und High Availability (HA) Konfigurationen
- Deployment als Software, Container, Cloud-Instanz oder Managed Service

primeID CERTIFY VERÄNDERT DIE SPIELREGELN

Betreiben Sie mehrere PKI-Hierarchien auf einer einzigen Plattform, zentralisieren Sie Konfiguration und Verwaltung von Zertifikatsrichtlinien und greifen Sie zentral auf detaillierte (bei Bedarf signierte) Audit- und Transaktionsprotokolle zu.

primeID CERTIFY: EINE ROBUSTE CERTIFICATE AUTHORITY (CA), DIE SICH SCHNELL EINFÜHREN LÄSST, BEDARFSGERECHT SKALIERT UND SICH AN JEDES ANWENDUNGSSZENARIO ANPASST.

In einer vernetzten Welt, in der Vertrauen essentiell ist, hat sich die Public-Key-Infrastruktur (PKI) als bewährte Lösung für digitale Identitäten etabliert. Sie ermöglicht sichere, verschlüsselte und verifizierte Verbindungen für jeden Benutzer, jedes Gerät und jeden Workload. Doch viele PKI-Systeme sind komplex und veraltet, erfordern viel Expertenwissen und skalieren kaum mit neuen Anwendungsfällen. Der PKI-Betrieb wird so zur Herausforderung.

primeID CERTIFY definiert neu, wie Unternehmen PKI betreiben. Mit einem schlanken Prozess für die Ausstellung, Verwaltung, Erneuerung und Pflege digitaler Zertifikate. Dank Open-Source-Prinzipien und -Plattformen ist **primeID CERTIFY** eine weltweit genutzte, vertrauenswürdige PKI-Plattform für zahlreiche Anwendungsfälle.

ÖFFENTLICH

VORTEILE

- Kritische Systeme und Daten schützen und Zero-Trust mit PKI-basierten Identitäten stärken
- Multi-Tenant-Betrieb auf einer Plattform
- Nahtlose Enterprise-Integration
- Strenge Sicherheits- und Compliance-Anforderungen mit einer bewährten und vertrauenswürdigen PKI erfüllen
- Horizontal und vertikal skalierbare Lösung für jede Infrastruktur

ZENTRALE FUNKTIONEN

- Einheitliche PKI-Plattform für den parallelen Betrieb mehrerer Certificate Authorities (CAs), sowie nahtlose Integration in primelD AUTOMATE und primelD VALIDATE
- Hervorragende Skalierbarkeit – auch für sehr große Umgebungen dank Datenbank-Clustering und Hochverfügbarkeits-Setups (HA)
- Flexible Bereitstellungsoptionen: PKI als Software, Container, Cloud-Instanz oder Managed Service
- Automatisiertes Lifecycle-Management der Zertifikate mit primelD AUTOMATE
- Nahtlose Integration mit Active Directory (AD), Azure AD, Kubernetes und vielen weiteren Systemen
- Vertrauenswürdige, Compliance-fähige Lösung, nach Common Criteria evaluiert und bereits in WebTrust- und ETSI/eIDAS-konformen Umgebungen im Einsatz

SCHNELL STARTEN — ÜBERALL BETREIBEN

Jedes Unternehmen steht vor eigenen betrieblichen Herausforderungen, von Sicherheitsanforderungen über Budgetgrenzen bis zu IT-Ressourcen. **primelD CERTIFY** ist plattformunabhängig und läuft nahtlos auf jedem Betriebssystem, Applikationsserver und jeder Datenbank. Dank modularer Architektur lässt sich die Lösung mühelos auch in komplexen Umgebungen einsetzen.

ÖFFENTLICH

JEDE MASCHINE, JEDEN WORKLOAD SCHÜTZEN

Containerisierung, DevOps, IoT und Remote Work haben die Zahl der Geräte und Benutzer, die eine interne PKI absichern muss, stark erhöht. Deshalb integriert sich primelD CERTIFY nahtlos in zahlreiche Anwendungen und Systeme von Drittanbietern und erweitert Ihre PKI flexibel für neue Anwendungsfälle. Möglich wird dies durch die Unterstützung gängiger Protokolle und zahlreicher vorkonfigurierter Plug-ins für unterschiedlichste Plattformen und Anwendungen.

UNTERSTÜTZTE TECHNOLOGIEN

Zertifikatsformate und Standards

- RFC 5280 konforme X.509-Zertifikate und CRLs
- PKCS#10-, CRMF- und SPKAC-Certificate-Requests
- PKCS#12-, JKS-, PEM- und PKCS#11-Keystores
- eIDAS-konforme Zertifikate nach EN 319 412
- OCSP gemäß RFC 6960 und RFC 5019
- ICAO 9303, EAC 1.11 und EAC 2.10 für ePass und eID
- Certificate Transparency gemäß RFC 6962

Protokolle

- ACME, CMP, EST und SCEP als Enrollment-/Management-Protokolle
- REST-API
- Web-Services

Hardware-Sicherheitsmodule (HSMs)

- Thales Luna, Entrust nShield, Utimaco, AWS CloudHSM, Azure Key Vault Managed HSM und PKCS#11-konforme Module

Kryptografie

- RSA-, ECDSA- und EdDSA-Schlüssel, CVC, EMV-konform
- **PQC:**
FIPS 203, ML-KEM, basiert auf CRYSTALS-Kyber
FIPS 204, ML-DSA, basiert auf CRYSTALS-Dilithium
FIPS 205, SLH-DSA, basiert auf SPHINCS+
In Kürze:
FIPS 206, FN-DSA, basiert auf FALCON