EVIDEN

IDnomic PKI Intune Connector

Digitale Identitäten für Microsoft-zentrierte Infrastrukturen

Die heutigen Arbeits- und Geschäftsumgebungen sind auf Geräte wie Smartphones, Tablets und PCs angewiesen. Ihre Integration in die IT-Infrastruktur von Unternehmen ist ein Muss, was durch Trends wie BYOD (Bring Your Own Device) noch verstärkt wird, die die Bereitstellungsmodelle komplexer machen und den Sicherheitsbedarf erhöhen. Darüber hinaus erfordern mobile Anwendungen spezifische Prozesse für die Verwaltung kritischer Daten.

Microsoft Intune ist ein cloudbasierter Dienst, der Geräte und Anwendungen verwaltet und dabei für Sicherheit und Compliance sorgt. Er unterstützt BYOD, ermöglicht die Fernverwaltung, den Schutz von Anwendungen und die nahtlose Integration mit Microsoft 365 und Azure.

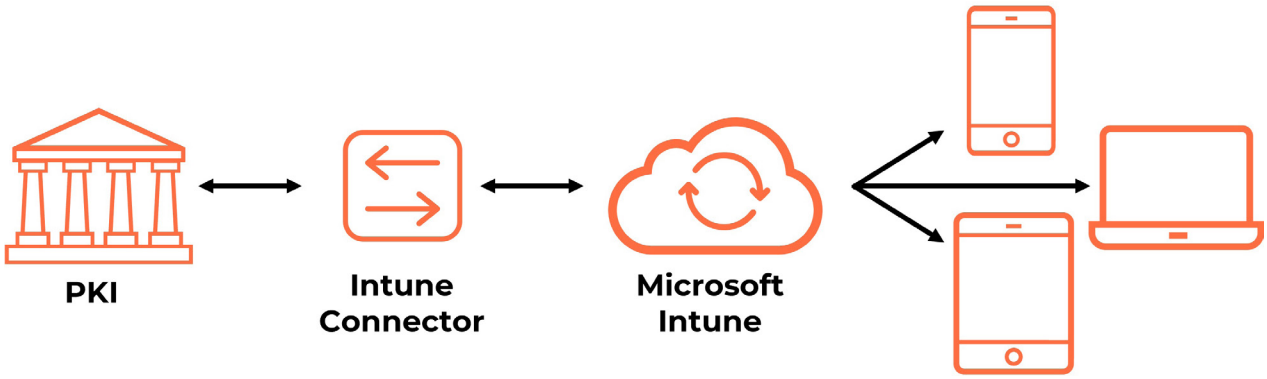
Der Intune-Konnektor in Kombination mit einer unserer IDnomic-PKI-Lösungen (ID PKI oder OT PKI) ermöglicht die Integration digitaler Zertifikate in mobile Geräte und Computer, die von Microsoft Intune verwaltet werden. Diese Zertifikate können für die Authentifizierung, E-Mail-Signatur und E-Mail-Verschlüsselung verwendet werden.

Die Integration eines Intune-Konnektors in eine IDnomic-PKI ermöglicht es Unternehmen, Zertifikate auf Mobil- und Desktopgeräten sicher zu verwalten und so die Sicherheit des Zugriffs auf Ressourcen und die Kommunikation zu erhöhen. Dies erleichtert die Verwaltung von Unternehmensgeräten unter Einhaltung hoher Sicherheitsstandards.

Der IDnomic Intune Connector ermöglicht die Umsetzung einer Vielzahl von Anwendungsfällen, insbesondere der gängigsten, wie zum Beispiel:

- **WLAN-Authentifizierung**: Bereitstellung von Zertifikaten für die sichere Authentifizierung über das 802.1X-Protokoll.
- **VPN**: Verteilung von Zertifikaten für die sichere Authentifizierung bei VPN-Servern.
- **S/MIME für E-Mails**: Bereitstellung von Zertifikaten zum Signieren und Verschlüsseln von E-Mails über S/MIME.
- **Zugriff auf Unternehmensanwendungen**: Integration von Zertifikaten für den Zugriff auf interne Ressourcen wie Intranets oder sichere Anwendungen.

IDnomic PKI Intune Connector – Aufbau



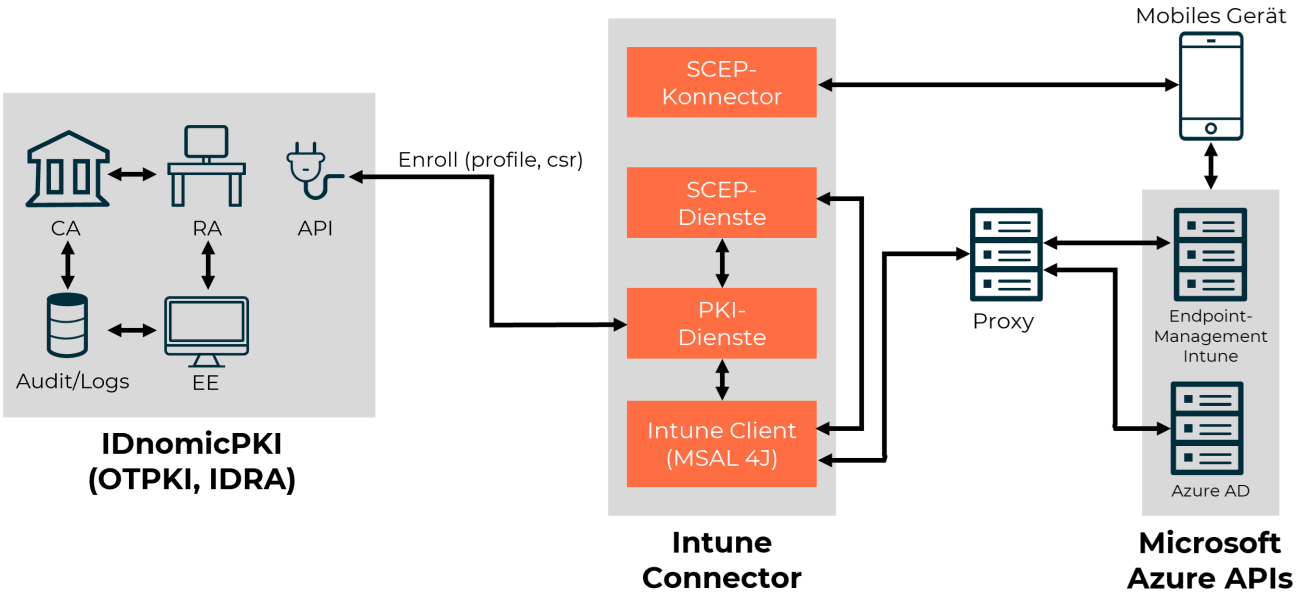
Der Intune Connector ermöglicht die Ausstellung digitaler Zertifikate, indem er die IDnomic-PKI mit dem Microsoft-Geräte-Ökosystem verbindet.

EVIDEN

PKI Intune Connector – Die Lösung

Der IDnomic Intune Connector ruft von einer PKI generierte digitale Zertifikate ab und überträgt sie an die entsprechenden Geräte. Die wichtigsten Bausteine sind folgende:

- **PKI-Server**: Die PKI stellt Zertifikate für Benutzer und Geräte aus.
- **Intune Connector**: Hierbei handelt es sich um eine Softwarekomponente, die Intune mit der PKI verbindet, um Zertifikate auf registrierten Geräten zu erhalten, zu erneuern, zu widerrufen oder zu verteilen. Diese Komponente muss auf einem Server im Unternehmensnetzwerk installiert sein.
- **Microsoft Intune**: Intune verwaltet unter anderem die Geräteregistrierung, die Anwendung von Sicherheitsrichtlinien und die Verteilung von Zertifikaten über Konfigurationsprofile.
- **SCEP**: Der Intune-Connector verwendet das SCEP-Protokoll, um Zertifikate auszustellen.



Unterstützte Optionen

Geräte-Enrollment

Wenn ein Gerät in Intune registriert ist, kann es so konfiguriert werden, dass es digitale Zertifikate von einem PKI-Server empfängt, um sichere Kommunikations- und Authentifizierungsprozesse zu gewährleisten.

Zertifikate-Verteilung

Das Gerät interagiert mit dem Intune-Connector, um Zertifikate über Konfigurationsprofile bereitzustellen. Innerhalb des Zertifikatsverteilungsprozesses fungiert der Connector als Vermittler zwischen den Geräten und Intune. Er überträgt und leitet Informationen weiter.

Authentifizierung und Autorisierung

Digitale Zertifikate können zur Authentifizierung verwendet werden, um Netzwerke (WLAN, VPN), Anwendungen oder interne Dienste zu sichern.

EVIDEN

Kundenvorteile

- **Native Kompatibilität** mit IDnomic PKI, wodurch Infrastrukturkosten gesenkt werden können. Mit dem Intune Connector kann ein Unternehmen von der Flexibilität und Leistung der IDnomic PKI profitieren, ohne Einschränkungen hinsichtlich seiner Geräteinfrastruktur hinnehmen zu müssen.
- **Transparente Zertifikatserneuerung** ohne Auswirkungen auf Endbenutzer. Verwalten Sie den Lebenszyklus von Anmeldedaten nahtlos und verbergen Sie die Komplexität der Zertifikatsausstellung und -erneuerung durch automatisierte, flexible Workflows.
- **Steigern Sie die Produktivität**, indem Sie kostspielige Supportprozesse für die manuelle Zertifikatsausstellung für bestimmte Geräte reduzieren.
- **Gewährleisten Sie Sicherheit und Zugriffskontrolle** für alle Geräte, die mit der IT-Infrastruktur eines Unternehmens verbunden sind, indem Sie Zertifikate für die Authentifizierung und Verschlüsselung verwenden, die über den IDnomic Intune Connector bereitgestellt werden.

Standards und technische Spezifikationen

Protokolle

» SCEP

Server

» Redhat Enterprise Linux 6/7/8 (x86_64)

» Rocky Linux 8 (x86_64)

» SLES 11/12/15 (x86_64)

Mobile Geräte

» Microsoft Windows 10

» Android 11

» iOS 15

PKI

» IDnomic PKI

» OpenTrust PKI

Weitere Informationen: www.cryptovision.com

Soziale Medien

eviden.com

 20251021