EVIDEN

Souveräne und resiliente digitale Identitäten

Ein strategischer Leitfaden für Zertifikatsmanagement und Interoperabilität in komplexen IT-Infrastrukturen

Die Digitalisierung stellt Unternehmen und Institutionen vor neue Herausforderungen. Neben Effizienz und Skalierbarkeit rückt zunehmend die Frage nach digitaler Souveränität in den Mittelpunkt. Digitale Identitäten spielen dabei eine zentrale Rolle: Sie ermöglichen sichere Kommunikation, kontrollierten Zugriff, Nachvollziehbarkeit und Vertrauenswürdigkeit. Damit bilden sie das Fundament für geschützte digitale Prozesse in sensiblen Bereichen.

Dieser Leitfaden bietet einen strukturierten Überblick über Anforderungen, Umsetzungskriterien und bewährte Lösungsansätze für resiliente digitale Identitäten in komplexen Umgebungen mit hohem Schutzbedarf – mit Fokus auf Standards, Interoperabilität und Vermeidung von Anbieterabhängigkeiten.

Grundlagen und Anwendungs-bereiche digitaler Identitäten

Digitale Identitäten sind allgegenwärtig: Sie repräsentieren Menschen, Systeme oder Organisationseinheiten in digitalen Prozessen. Ihr Schutz ist essenziell für die Integrität, Nachvollziehbarkeit und Vertraulichkeit von Kommunikation und Transaktionen. Dazu dienen Authentifizierung, Verschlüsselung und digitale Signaturen auf Basis vertrauenswürdiger Zertifikate und sicherem Schlüsselmaterial.

Typische Einsatzszenarien

- **Authentifizierung** für Benutzer, Dienste und Geräte
- **Verschlüsselung** von E-Mails, Dateien, Datenströmen
- **Digitale Signatur** qualifiziert & automatisiert
- **Code Signing** Sicherstellung von Integrität und Authentizität
- **Zugriffskontrolle** auf sensible Ressourcen

Besonderheiten

- **Klassifizierte Informationen** erfordern erhöhten Schutz
- **Rechtevergabe in Echtzeit** statt statischem Schlüsselbesitz
- **Dynamische Teamzusammen-setzungen** mit wechselnden Rollen
- **Revisionssichere Sicherheit** effizient und auditierbar

Sicherheitskritische Umgebungen

Ein spezifisches Anwendungsfeld ist die Absicherung besonders schutzbedürftiger Informationen – etwa bei der Kommunikation mit eingestuften Inhalten. Für solche Szenarien sind spezielle, durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zugelassene Produkte erforderlich, die kryptografische Verfahren auf hohem Sicherheitsniveau ermöglichen. Die Interoperabilität dieser Lösungen mit bestehenden Infrastrukturen sowie die Einhaltung offener Standards sind entscheidend, um eine nachhaltige und skalierbare Integration sicherzustellen.

Anforderungen und Umsetzungskriterien sicherer digitaler Identitäten

Dynamisches Zugriffsmanagement

Ein flexibles Rechte- und Zugriffsmanagement ist unerlässlich. Eine gruppenübergreifende Nutzung von Ressourcen, wie der Zugriff auf Gruppen- oder Funktionsschlüssel, erfordert dynamische Lösungen. Statische Modelle, bei denen kryptografische Schlüssel dauerhaft auf physischen Smartcards gespeichert und an einzelne Mitarbeitende ausgegeben werden, sind in diesen Szenarien nur bedingt praktikabel. Bei personellen Veränderungen oder wechselnden Zuständigkeiten müssten diese Schlüssel manuell entzogen werden – ein Prozess, der nicht nur fehleranfällig, sondern auch mit hohem organisatorischem Aufwand verbunden ist.

Rechte lassen sich in Echtzeit vergeben oder entziehen.

Ein Client-Server-Modell mit zentral gespeicherten privaten Schlüsseln bietet hier entscheidende Vorteile: Die Nutzung der Schlüssel erfolgt temporär, kontrolliert und ohne dass diese den geschützten Speicher verlassen. Rechte lassen sich in Echtzeit vergeben oder entziehen.

Typische Anwendungsszenarien mit variablen Zugriffsberechtigungen

- **Projektgruppen**
  (z. B. Referate oder Abteilungen) mit wechselnder Zusammensetzung und dynamischem Bedarf an Zugriff auf Daten, E-Mail-Konten oder Netzwerksegmente
- **Funktionspostfächer**
  (z. B. „Referatsleitung“, „Abteilungsleitung“), die nicht personenbezogen, sondern rollenbasiert genutzt werden
- **Mobile Techniker,**
  deren Zugriffsrechte sich je nach Einsatzort und Aufgabe situativ ändern

Governance und Nachvollziehbarkeit

In sicherheitsbewussten Organisationen reicht technische Absicherung allein nicht aus. Entscheidende sicherheitsrelevante Vorgänge – insbesondere die Vergabe von Schlüsseln oder die Ausstellung neuer Zertifikate – unterliegen daher strengen organisatorischen Auflagen. In besonders sensiblen Fällen ist ein Vier-Augen-Prinzip etabliert, bei dem sicherheitskritische Entscheidungen stets von mindestens zwei autorisierten Personen gemeinsam getroffen und dokumentiert werden müssen. Das betrifft etwa die Freigabe von Entschlüsselungsschlüsseln oder die Zuteilung neuer qualifizierter Signaturzertifikate für sensible Informationen.

Sicherheitsrelevante Vorgänge unterliegen strengen organisatorischen Auflagen.

Zusätzlich ist ein umfassendes Logging erforderlich. Alle sicherheitsrelevanten Aktivitäten müssen nachvollziehbar dokumentiert werden, sodass im Bedarfsfall ein Audit gewährleistet werden kann – ein wesentliches Element sowohl für interne Compliance-Anforderungen als auch für externe Prüf- und Aufsichtsprozesse.

Automatisierung als Grundlage zur Skalierung und Akzeptanz

Benutzerfreundlichkeit ist ein zentraler Erfolgsfaktor für sicherheitsrelevante Prozesse. Denn Abläufe, die als zu aufwendig, komplex oder unverständlich wahrgenommen werden, werden in der Praxis häufig umgangen – mit entsprechendem Risiko für die Gesamtarchitektur. Um dem entgegenzuwirken, müssen sicherheitskritische Prozesse möglichst automatisiert, nachvollziehbar und nutzertransparent ablaufen.

Ein Beispiel ist das automatisierte Onboarding: Nach Abschluss eines Genehmigungsworkflows wird der Zugriff auf ein Gruppenpostfach automatisch eingerichtet. Die benötigten Zertifikate werden im Hintergrund beantragt, ausgestellt und eingebunden – ganz ohne aktives Zutun der Nutzerinnen und Nutzer. Lediglich eine einmalige PIN-Vergabe ist erforderlich. Selbst sicherheitsrelevante Vorgänge wie das Zurücksetzen vergessener PINs lassen sich auf diesem Weg zuverlässig und komfortabel umsetzen.

Moderne Zertifikatsmanagement-Systeme erkennen ablaufende Zertifikate eigenständig und stoßen deren Erneuerung automatisiert an – je nach Anwendungsfall differenziert und unter Berücksichtigung der jeweils zuständigen Zertifizierungsstelle. So werden Fehlerquellen reduziert und der administrative Aufwand nachhaltig gesenkt.

Nur was einfach ist, wird sicher genutzt.

Lösungsansätze für resiliente digitale Identitäten

Komplexität in der Praxis

Organisationen stehen häufig vor der Herausforderung historisch gewachsener, heterogener IT-Infrastrukturen. Diese bringen eine Vielzahl technischer und organisatorischer Besonderheiten mit sich:

- **Der Einsatz spezifischer Smartcards inklusive Middleware führt oft in einen Vendor-Lock-in**
- **Veraltete oder nicht mehr unterstützte Smartcards und Softwarekomponenten**
- **Mangelnde Interoperabilität zwischen unterschiedlichen Plattformen, Diensten oder Sicherheitslösungen**
- **Vielfältige Gerätetypen, Betriebssysteme, Sicherheitsdomänen und Nutzergruppen mit stark divergierenden Anforderungen**

Diese strukturelle und technologische Fragmentierung stellt ein erhebliches Hindernis für ein durchgängig einheitliches, skalierbares und sicheres Zertifikatsmanagement dar.

Offenheit, Standardisierung und Interoperabilität als Erfolgsfaktoren

Ein entscheidendes Ziel moderner Identitätsinfrastrukturen sollte die Vermeidung von Lock-in-Effekten sein.

Proprietäre Lösungen, die Organisationen an einzelne Anbieter oder Technologien binden, stehen langfristiger Flexibilität entgegen.

Eviden setzt daher gezielt auf allgemeingültige Standards, modulare Architekturen und Interoperabilität. Die Nutzung interner, externer und öffentlicher Zertifizierungsstellen sowie deren Kombination ist dabei ein zentrales Prinzip.

Diese Offenheit ermöglicht es, bestehende Komponenten weiter zu nutzen, neue Lösungen nahtlos zu integrieren und zukünftigen Anforderungen – etwa durch regulatorische Änderungen oder technologische Fortschritte wie Post-Quanten-Kryptografie – flexibel und angemessen zu begegnen. Gleichzeitig wird so eine hohe Resilienz gegenüber technologischen Abhängigkeiten sichergestellt.

Handlungsempfehlungen für CISOs und IT-Entscheider

Analyse
Bestehende Abhängigkeiten und Insellösungen identifizieren

Architekturprüfung
PKI-Applikationen auf Standards und Skalierbarkeit bewerten

Zukunftsplanung
Post-Quantum-Readiness strategisch berücksichtigen

Nutzerzentrierung
Benutzer-freundlichkeit als Sicherheitsfaktor betrachten

Souveränität
Europäische, standardisierte Lösungen bevorzugen

Integration
Zertifikats-management in ITSM-Prozesse einbinden

Fazit

Die sichere und souveräne Verwaltung digitaler Identitäten zählt zu den zentralen Herausforderungen moderner IT-Architekturen. Dabei geht es nicht nur um die technische Implementierung kryptografischer Verfahren, sondern um das Zusammenspiel aus Architektur, Prozessen, Automatisierung, Interoperabilität und Benutzerfreundlichkeit.

Ein durchdachtes und zukunftssicheres Zertifikatsmanagement kann für Organisationen zum entscheidenden Hebel werden: Es reduziert operative Komplexität, erhöht die Sicherheit und erleichtert die Integration neuer Anwendungsfelder – etwa digitale Signaturen, sichere E-Mail-Kommunikation oder Bring Your Own Device (BYOD)-Szenarien. Darüber hinaus schafft es die Voraussetzung für die Vorbereitung auf kommende Herausforderungen wie Post-Quanten-Technologie.

Organisationen, die ihre bestehenden PKI-Strukturen modernisieren, ihre Verwaltungsprozesse verschlanken oder regulatorische Anforderungen zuverlässig erfüllen möchten, profitieren von einer ganzheitlichen Strategie – insbesondere, wenn sie auf Standards, modularem Design und hoher Interoperabilität basiert.

Eviden bietet hierfür ein umfassendes Portfolio praxiserprobter Lösungen: von Zero-Touch-Onboarding über skalierbare PKI-Dienste bis hin zu rollenbasiertem Schlüsselmanagement. Eviden bietet zudem vom BSI zugelassene Lösungen an, die eine sichere Übertragung und Verarbeitung von Verschlusssachen bis zum Geheimhaltungsgrad VS-NfD gewährleisten. Besonderer Wert wird dabei auf technologische Souveränität und standardbasierten, modulare Architekturen gelegt – für maximale Flexibilität, Sicherheit und Zukunftsfähigkeit.

Technologische Souveränität braucht standardbasierte, modulare Architekturen.

Weitere Informationen:
www.cryptovision.com

cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Germany
Tel: +49 (0) 2 09 / 1 67 – 24 50
Fax: +49 (0) 2 09 / 1 67 – 24 61

About Eviden

Eviden is the Atos Group brand for hardware and software products with c. € 1 billion in revenue, operating in 36 countries and comprising four business units: advanced computing, cybersecurity products, mission-critical systems and vision AI. As a next-generation technology leader, Eviden offers a unique combination of hardware and software technologies for businesses, public sector and defense organizations and research institutions, helping them to create value out of their data. Bringing together more than 4,500 world-class talents and holding more than 2,100 patents, Eviden provides a strong portfolio of innovative and eco-efficient solutions in AI, computing, security, data and applications.

Connect with us

eviden.com