Public Key Infrastructures (PKI)

Sichere Kommunikation zwischen Menschen, Applikationen und Devices

Eine Public Key Infrastructure (PKI) ist eine Hierarchie von digitalen Zertifikaten. Im Kontext digitaler Kommunikation ermöglicht sie die eindeutige Identifikation und Authentifizierung der Kommunikationspartner. Hierdurch wird die Vertraulichkeit als auch die Datenintegrität bei der Nutzung elektronischer Services sichergestellt.

PKI und das Prinzip der asymmetrischen Verschlüsselung

Digitale Zertifikate dienen der Absicherung rechnergestützter Kommunikation. Sie stellen quasi eine Art digitale Beglaubigung dar, mittels derer Vertrauen zwischen Sender und Empfänger etabliert werden soll. Eine PKI basiert auf dem Prinzip der asymmetrischen Verschlüsselung, bei der für jeden, der verschlüsselt kommunizieren möchte, ein Schlüsselpaar – bestehend aus einem privaten und einem öffentlichen Schlüssel - erstellt wird. Nun gilt das Schlüssel-Schloss-Prinzip. Eine Datei, die mit dem öffentlichen Schlüssel verschlüsselt wurde, kann nun nur mit dem dazugehörigen privaten Schlüssel entschlüsselt werden. Ein digitales Zertifikat beinhaltet nun eben genau diesen öffentlichen Schlüssel eines solchen Schlüsselpaares sowie Angaben dazu, wer das Zertifikat für wen ausgestellt hat und wie lange es gültig ist.

Bei einer PKI handelt es sich um die technische Infrastruktur, mit der die Zertifikate und Informationen zu ihrer Gültigkeit erzeugt und öffentlich bereitgestellt werden. Hier werden die Zertifikate verwaltet und hierarchisiert. Ausgangspunkt und Vertrauensbasis einer jeden Hierarchie und Infrastruktur bildet dabei stets das sogenannte Wurzelzertifikat (Root Certificate) inklusive des zugehörigen Schlüsselpaares. Alle weiteren Zertifikate innerhalb der Infrastruktur werden dann mit dem privaten Schlüssel des Wurzelzertifikats signiert. Derartige Zertifikatsketten können beliebig lang werden. Wichtig ist lediglich, dass sie stets mit dem Wurzelzertifikat beginnen. Ein Zertifikat innerhalb einer PKI gilt als echt und vertrauenswürdig, wenn sämtliche Zertifikate, die zwischen dem zu prüfenden Zertifikat und dem Wurzelzertifikat liegen, erfolgreich verifiziert werden konnten.

Die Vorteile einer Public Key Infrastructure (PKI) auf einen Blick

Erfüllung der Kriterien von Informationssicherheit und Nichtabstreitbarkeit

Eine PKI unterstützt essentielle Kriterien der Informationssicherheit wie Authentifizierung, Integrität und Vertraulichkeit. Darüber hinaus gewährleistet der Einsatz von digitalen Signaturen, dass die Urheberschaft signierter Nachrichten nicht abgestritten werden kann.

Geringerer Verwaltungsaufwand

Bei einer PKI werden die öffentlichen Schlüssel zentral verwaltet und müssen gegen Angriffe geschützt werden. Die Komplexität und der Verwaltungsaufwand bezogen auf die unterschiedlichen Zertifikate und deren Schlüssel reduziert sich hierdurch erheblich.

Erhöhte Sicherheit und vertrauenswürdige Automatisierung von Geschäftsprozessen

Neben der Verbesserung des Sicherheitsniveaus unterstützt eine PKI die zentrale Verwaltung von kryptografischen Sicherheitsmechanismen bzw. asymmetrischer Verschlüsselungstechniken. Dank des Einsatzes von digitalen Zertifikaten profitieren zwei kommunizierende Parteien von der jeweils hohen Glaub- und Vertrauenswürdigkeit des anderen. Digitale Signaturen erlauben darüber hinaus auch eine umfassende vertrauenswürdige Automatisierung der Geschäftsprozesse von Unternehmen.

Erleichterte Durchsetzung von Richtlinien und Vorgaben

Eine zentral administrierte PKI unterstützt die unternehmensweite Umsetzung von Richtlinien und Verhaltensregeln zum Beispiel bezogen auf die Erneuerungen und Sperrungen von Zertifikaten.

ASCONSIT: Eine sorgfältige Planung ist das A und O!

Bei der Implementierung einer PKI sehen sich Unternehmen nicht selten mit diversen Problemen konfrontiert. Sei es, dass die Einführung einer PKI unzureichend geplant oder dass vorschnell bestimmte Software installiert wurde. Kurzfristiger Aktionismus führt selten zu dem gewünschten Ergebnis. Das gilt auch im Zusammenhang mit der Implementierung einer PKI. Aufsetzend auf dem bestehenden Sicherheitskonzept ist vor allem eine sorgfältige Planung und Konzepterstellung. Das übergeordnete Ziel einer PKI ist es, die in Unternehmen meist vorhandene Vielfalt an Sicherheits- und Verschlüsselungsverfahren (z. B. bei der Netzwerkanmeldung, dem Zugriff auf E-Mails oder beim Remote-Access-Zugang aus dem Homeoffice) zu vereinheitlichen und hierdurch Fehler zu reduzieren sowie Kosten durch die vereinfachte Administration einzusparen.

Unsere Fachexperten stellen eine präzise Planung und nachhaltige Konzeption Ihrer PKI sicher!