Lernzusammenfassung

Public-Key-Infrastrukturen (PKI - Öffentlicher-Schlüssel-Infrastruktur)

Eine Public Key Infrastructure (deutsch: Öffentliche-Schlüssel-Infrastruktur; kurz: PKI) dient zur Verwaltung und Verteilung von Schlüsseln und digitalen Zertifikaten in öffentlich zugänglichen Netzwerken, um eine sichere digitale Kommunikation zu gewährleisten. Der Austausch von Daten, Informationen und Nachrichten via Internet erfolgt in einer PKI durch ein Schlüsselpaar, das aus einem öffentlichen (public key) und einem privaten Schlüssel (private key) besteht.

Die Schlüssel sind über eine mathematische Funktion miteinander verbunden, sodass Daten, die mit dem öffentlichen Schlüssel verschlüsselt wurden, nur mit dem privaten Schlüssel entschlüsselt werden können (Einwegfunktion).
Public-Key-Infrastruktur stellt Zertifikate aus, gibt sie an die Kommunikationsteilnehmer weiter und prüft die Zertifikate auf Echtheit. Mit dieser mehrstufigen Prüfung werden Sender und Empfänger authentifiziert und die zu übermittelnden Daten einem Integritätstest unterzogen. Public Key Infrastrukturen sind eine Kombination aus symmetrischen und asymmetrischen Verschlüsselungsverfahren, die mit zwei verschiedenen Schlüsseln arbeiten und das Schlüsselaustauschproblem anhand einer IT-Infrastruktur und einer Zertifizierungsstelle lösen wollen.

Eine Öffentlicher-Schlüssel-Infrastruktur besteht aus:

- einer Sicherheitsrichtlinie - definiert den Sicherheitsgrad, die Prozesse und Verwendungen der Kryptographie; beinhaltet Angaben über das Handling von Schlüsseln und wertvollen Informationen,
- einer Zertifizierungsstelle (Certification Authority – CA) – diese Instanz ist die Vertrauensbasis der PKI und erstellt die Zertifikate,
- einer Registrierungsstelle (Registration Authority – RA) - die Schnittstelle zwischen Benutzer und CA; erfasst und authentifiziert die Identität der Benutzer und reicht die Anfrage nach einem Zertifikat an die CA weiter,
- einem Verteilungssystem für die Zertifikate - beispielsweise die Verteilung durch die Nutzer selbst oder einen Verzeichnisserver wie LDAP. Die Verteilung hängt von der PKI-Umgebung ab.
- PKI-Applikationen: z.B. E-Mails, Kommunikation zwischen Webserver und Webbrowser.

Public Key Infrastructure (PKI) werden eingesetzt für

- Starke Authentisierung für Intra-/Extra-/Internet-Ressourcen
- Sichere Kommunikation mit SSL/TLS/Signieren Verschlüsseln von E-Mail (S/MIME)
- Elektronischer Zeitstempel (Qualifiziert - Akkreditiert)
- Single Sign On
- Signatur von elektronischen Dokumenten
- Einsatz durch TrustCenter "getrusteter" elektronischer Zertifikate
- Internet der Dinge (z.B. Smart Meter Datenaustausch)
- Mobile PKI und Mobile Device Management u.v.m.

Lernzusammenfassung

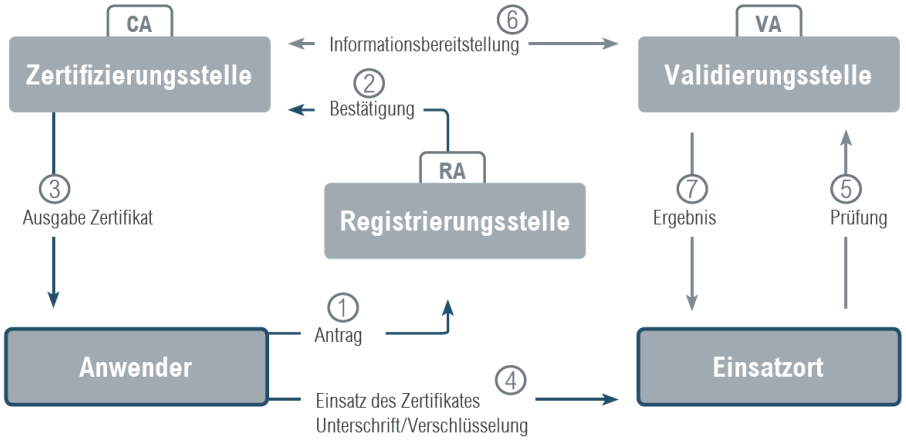
Public-Key-Infrastrukturen (PKI - Öffentlicher-Schlüssel-Infrastruktur)

Was ist ein digitales Zertifikat?

Ein digitales Zertifikat ist ein elektronischer Echtheitsnachweis, der die Identität einer Person, eines Rechners oder einer Organisation bescheinigt. Im realen Leben kann ein Zertifikat mit einem Personalausweis verglichen werden. Anhand der Angaben in dem Personalausweis kann die Identität einer Person festgestellt werden.
Eine CA (Certificate Authority oder Certification Authority) ist eine vertrauenswürdige Instanz, eine Zertifizierungsstelle, die digitale Zertifikate herausgibt. Mit Hilfe der Zertifikate wird die elektronische Identität von Kommunikationspartnern bescheinigt. CAs bilden den Kern der Public-Key-Infrastruktur und übernehmen die Rolle von Trust Centern.

RA: registration authority. → zuständig für das Registrieren und sichere Identifizieren des Zertifikatnehmers.

VA: validation authority → Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht



Wie komme ich zu einem Zertifikatsserver?

Installieren Sie die Zertifikatstelle entweder auf einem Domänencontroller oder einem anderen Server im Netzwerk. Wenn Sie allerdings den Server, der die Zertifikatstelle verwaltet, aus der Domäne entfernen, verlieren die Zertifikate ihre Gültigkeit. Die Installation nehmen Sie über das Hinzufügen der Rolle **Active Directory-Zertifikatsdienste** im Servermanager vor.