PKI der TI

Was ist eine PKI?

Definitionen

> Mit Public-Key-Infrastruktur (PKI, englisch public key infrastructure) bezeichnet man in der Kryptologie eine Infrastruktur zur Verwaltung von Identitäten, Schlüsseln, Zertifikaten, Attributen usw.[1)]
>
> Die Infrastruktur für die Erzeugung, Authentisierung, Verteilung und Überprüfung von öffentlichen Schlüsseln sowie für die sichere Speicherung der geheimen Schlüssel wird Public-Key-Infrastruktur (PKI) genannt.„[2)]
>
> Eine PKI ist eine technische und organisatorische Infrastruktur, die es ermöglicht, kryptographische Schlüsselpaare (private Schlüssel in Form von PSEs und öffentliche Schlüssel in Form von Zertifikaten) auszurollen und zu verwalten. Zu den wesentlichen Kernkomponenten einer PKI zählt die Registrierungsinstanz, die Zertifizierungsinstanz und der Verzeichnisdienst. Unter Umständen umfasst eine PKI auch einen Zeitstempeldienst und Attributbestätigungsinstanzen.[3)]

Zertifikate sind eine von einer Ausgabestelle signierte Sammlung persönlicher Informationen (Attribute) über Nutzer und deren *öffentliche Schlüssel*. Darüber hinaus enthalten sie Angaben zu den für die Signatur verwendeten kryptographischen Algorithmen und One-Way-Hashfunktionen sowie zu ihrer eigenen Gültigkeit und zum Herausgeber. Mithilfe des öffentlichen Schlüssels einer Zertifizierungsstelle kann die Echtheit eines Zertifikats und seiner Inhalte verifiziert werden. Durchgesetzt haben sich Zertifikate nach dem *Standard X.509* der International Telecommunication Union (ITU).

Mithilfe von PKIs lässt sich in modernen IT-Landschaften ein einfaches und organisationsübergreifendes Key Management realisieren.

Digitale Zertifikate stellen die Authentizität öffentlicher Schlüssel in asymmetrischen Kryptosystemen sicher und bestätigen seinen zulässigen Anwendungs- und Geltungsbereich. Das digitale Zertifikat ist selbst durch eine digitale Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Ausstellers des Zertifikates geprüft werden kann.

Um die Authentizität des Ausstellerschlüssels zu prüfen, wird wiederum ein digitales Zertifikat benötigt. Auf diese Weise lässt sich eine Kette von digitalen Zertifikaten aufbauen, die jeweils die Authentizität des öffentlichen Schlüssels bestätigen, mit dem das vorhergehende Zertifikat geprüft werden kann. Eine solche Kette von Zertifikaten wird **Validierungspfad** oder Zertifizierungspfad genannt. Auf die Echtheit des letzten Zertifikates (und des durch dieses zertifizierten Schlüssels) müssen sich die Kommunikationspartner ohne ein weiteres Zertifikat verlassen können.

Eine **Persönliche Sicherheitsumgebung** (**PSU**, englisch Personal Security Environment (PSE)) ist ein Aufbewahrungsmedium für private Schlüssel und vertrauenswürdige Zertifikate. Ein PSE kann entweder als Software-Lösung, z. B. als mittels Passwort geschützte Datei im PKCS #12-Format, oder als Hardware-Lösung, beispielsweise in Form einer Smart Card, realisiert sein. In diesem Fall kann das

PSE gleichzeitig als Signaturerstellungseinheit dienen.

PKI der TI

- **TSL** = **Trust-service Status List** als zentraler Vertrauensraum der X.509-PKI
- Einsatz einer **hierarchischen Root-Struktur** bei den **CV-Zertifikate**n

Elementarfunktionen der TI-PKI

- **Authentisierung** von Akteuren (mit elektronischen Identitäten) gegenüber Systemen, Komponenten und Diensten über eine verbindlich registrierte Zuordnung von kryptographischen Schlüsseln zu dem Akteur (**Authentizität**)
- **Erstellung und Prüfung von digitalen Signaturen**,
  - die den bewußten **Willensakt** eines Akteurs dokumentieren (**Nichtabstreitbarkeit** signierter Transaktionen)
  - die den **Zustand eines Datums zum Zeitpunkt** des Signaturvorgangs dokumentieren. (**Integrität** des signierten Datums)
- **Ver- und Entschlüsselung** von Daten bei Speicherung und Transport (**Vertraulichkeit**)

Die Funktionen werden mittels asymmetrischer kryptographischer Verfahren bereitgestellt, sind in ein technisches und organisatorisches Regelwerk eingebunden und bilden in Summe die Public Key Infrastructure (PKI) der TI.

Basisfunktionen der TI-PKI aus Anwendersicht

- Bereitstellung und Lifecycle-Management des TI-Vertrauensraums
- Identifikation von Personen, Institutionen und technischen Komponenten
- Registrierung von Zertifikatsantragstellern
- Erzeugung und Bereitstellung von
  - nonQES-Endnutzerertifikaten
  - QES-Endnutzerzertifikate nach eIDAS
- Zertifikatssperrung durch Zertifikatsnehmer und attributbestätigende Stellen
- Zertifikatssperrung durch Herausgeber und gematik als Policy Authority“
- Suchen und Abrufen von Zertifikaten aus Verzeichnissen
- Abruf von Zertifikatsstatusinformationen (Sperrinformationen)
- Beantragung, Produktion und Auslieferung von Zertifikaten.

Vertrauensmodelle

Bei Vertrauensmodellen geht es darum, Zertifikate auf einen vertrauenswürdigen Anker oder gemeinsamen Vertrauensraum zurückzuführen.

Die TI implementiert gem. der regulatorischen Hoheit der unterschiedlichen Anwendungsfelder folgende Vertrauensmodelle.

- Vertrauensmodell für QES
- Vertrauensraum mittels **T**rust-service **S**tatus **L**ist (TSL)
- Vertrauensmodell der nonQES-TI-Zertifikate im Internet
- Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten

Gültigkeitsmodelle

Beim Gültigkeitsmodell geht es um die Feststellung, ob ein Zertifikat zu einem gewissen Prüfzeitpunkt als gültig angesehen werden kann. Der Prüfzeitpunkt hängt vom verwendeten Gültigkeitsmodell ab. Üblicherweise wird die Gültigkeit von Signaturen zum Zweck der Authentisierung zur aktuellen Zeit geprüft, während Signaturen für Dokumente auf den Zeitpunkt der Signaturerstellung geprüft werden.

Die TI nutzt folgende Gültigkeitsmodelle.

- PKIX-Schalenmodell
- Kompromissmodell
- QES-Kettenmodell

Zertifikatstypen

- X.509-Zertifikate für Identitäten der TI
- CV-Zertifikate für Karten in der TI

Für die Zertifikate zeichnen unterschiedliche Organisationen verantwortlich.

[TODO: Bild]

1)
POHLMANN, Norbert, 2022. *Cyber-Sicherheit*. 2. Auflage. Heidelberg: medhochzwei. ISBN 978-3-658-36242-3.
2)
ERTEL, Wolfgang. 2007. *Angewandte Kryptographie*. 3., aktualisierte Auflage. München: Hanser, S. 118.
3)
Definition altes BSI-Glossar: s. https://web.archive.org/web/20090409144328/http://www.bsi.de/esig/glossar.htm#Glossar_P.