LU07.L02 - Kontrollfragen zu digitale Zertifikat

Rahmenbedingungen

- **Zeitbudget:** 15 Minuten
- **Sozialform:** Einzel bzw. Partnerarbeit
- **Hilfsmittel:**
  - Dossier *LU07a - Digitale Zertifikate Grundlagen*
  - Dossier *LU07b - Die Schlüsselverteilung*
  - Dossier *LU07c - Der Aufbau eines digitalen Zertifikates*
- **Erwartetes Ergebnis:** PDF mit verschiedenen Begriffe rund um das Thema *digitale Zertifikate*

Ausgangslage

Sie haben einiges über digitale Zertifikate erfahren. Die nachfolgenden Fragen sollen das Neuerlernte festigen helfen.

Arbeitsauftrag

Beantworten bzw. bearbeiten Sie die nachfolgenden Kontrollfragen:

1. *Digitalen Zertifikate ermöglichen ein hohes Mass an Vertraulichkeit, die auch dann noch gegeben ist, wenn das Verschlüsselungsverfahren bekannt ist.* Bestätigen oder widerlegen Sie diese Aussage argumentativ.
   - Ja
   - Weil die Sicherheit über den geheimen Schlüssel bzw. über die Schlüssellänge gewährleistet wird.
2. Wie wird der Sicherheitsmechanismus genannt, der die Authentizität der Schlüssel bestätigt? Wie funktioniert dieser bzw. wie ist dieser realisert?
   - PGP = Pretty good privacy
   - Sicherheitsmechanismus, das einen öffentlichen und einen geheimen Schlüssel (starken) verwendet.
   - HTTPS: Sicherheitsprotokoll im Internet, das die Kommunikation zwischen den Teilnehmenden verschlüsselt.
3. Erläutern Sie drei konkrete Beispiele aus Ihrem Leben, in denen digitale Zertifikate eine wesentliche Rolle spielen.
   - Digitale Signaturen (https)
   - Autorisierungs- und Zugriffskontrollen (Dongle oder Authentificator-App)
   - Email-Verifizierung
4. Digitale Zertifikate konnten sich nur bedingt durchsetzen. Welche zwei relevanten Ursachen könnten dafür verantwortlich sein?
   - Aktualisierung
   - Grosser Aufwand

- Teuer
- Nicht wirklich bekannt
- Fehlendes KnowHow
- Kein Wirklicher Bedarf, Weil Daten nicht so heikel sind.

1. Beschreiben Sie die nachfolgenden Begriffe stichwortartig:
    1. X.509: Standard für Zertifikate, der den Inhalt und die Reihenfolge der relevanten Elemente darin beschreibt.
    2. PGP
    3. Certificate Policy
    4. PKI
    5. CRL
    6. WoT
2. Vergleichen Sie PKI und WoT miteinander. Nennen zu jedem Begriff je zwei Vor- und Nachteile.
    - +PKI: Sicher, unterschiedliche Sicherheitslevel
    - -PKI: Nicht 100% sicher, Kosten
    - +WoT: Günstig¸ individuelle Kontrolle, einfach Zertifikat zu erhalten
    - -WoT: Selten aktuell, Undurchsichtiges Validierungsverfahren, unsichere Infrastruktur
3. Vergleichen Sie PKI und Wot miteinander. Wie wird die Qualität der Zertifikate gewährleistet.
    1. PKI: Autoritäten bzw. unabhängigen Instanzen
    2. WOT: Vertrauen und Kreditpunkte
