Digitale Zertifikate

Zusammenfassung

Nutzen und Einsatz von digitalen Zertifikaten

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

Das Prinzip des digitalen Zertifikates basiert auf der asymmetrischen Verschlüsselung. Bei der asymmetrischen Verschlüsselung wird für jede/n, der/die verschlüsselt kommunizieren möchte, ein Schlüsselpaar erstellt. Dieses besteht jeweils aus einem privaten (geheimen) und einem öffentlichen Schlüssel. Diese werden so generiert, dass eine Datei, die mit dem öffentlichen Schlüssel verschlüsselt wurde, nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden kann.

Das bedeutet, dass der/die E-Mail-Partner/in mit dem **öffentlichen Schlüssel**, den er/sie von einem/er Absender/in bekommen hat, E-Mails an diese/n Absender/in **verschlüsseln** kann. Diese sind nur für diese/n lesbar, d.h. **entschlüsselbar**, weil der **private Schlüssel** in Verbindung mit der E-Mail-Adresse steht. Einer anderen Person steht dieser private Schlüssel nicht zur Verfügung.

Außerdem ist es mit demselben privaten Schlüssel möglich, eine Datei digital zu signieren. Mit dem zugehörigen öffentlichen Schlüssel kann dann geprüft werden, ob die Datei seit der Signatur unverändert ist.

Ein digitales Zertifikat beinhaltet den öffentlichen Schlüssel eines solchen Schlüsselpaares und zudem weitere Angaben, wie z.B. wer das Zertifikat ausgestellt hat, für wen es ausgestellt wurde (= der/die Besitzer/in des passenden privaten Schlüssels) und der Gültigkeitszeitraum. Wenn zwei Kommunikationspartner/innen einander sicher Nachrichten übermitteln möchten, tauschen sie ihre Zertifikate aus und erhalten damit die Möglichkeit, Nachrichten so zu verschlüsseln, dass sie nur der/die jeweils andere entschlüsseln kann. Zusätzlich können sie auch die digitale Signatur des/der anderen überprüfen.

Damit die Zertifikate ausgetauscht werden können, müssten sich die Kommunikationspartner/innen allerdings kennen und einen sicheren Weg für den Austausch finden, damit sie auch tatsächlich das Zertifikat der Person oder Institution erhalten, mit der sie kommunizieren möchten. Eine Möglichkeit wäre, die Zertifikate per E-Mail zu versenden und anschließend per Telefon den jeweiligen elektronischen Fingerabdruck der beiden Zertifikate (dieser ist eine für jedes Zertifikat eindeutige Buchstaben-Zahlen-Kombination) zu überprüfen.

Um den Austausch von Zertifikaten zu vereinfachen und auch dann zu ermöglichen, wenn die Kommunikationspartner/innen sich vorher nicht persönlich kennen, werden so genannte Public Key Infrastructures oder Public Key Infrastrukturen gebildet.

Mehr Informationen findet man hier:

Cookies und Fingerprints verhindern

Der Browser – Gefahren und Risiken

Quelle: BSI

- Gruppenzertifikate beantragen und herunterladen
- PDF digital signieren mit Adobe Acrobat
- Persönliches Zertifikat anfordern und herunterladen
- Verschlüsselung von Cloudspeichern
- Zertifikate auf dem iPhone einrichten
- Zertifikate in E-Mail-Programmen am Beispiel von Outlook
- Zertifikate - Regeln und Begriffserklärung

--> Serverzertifikat für *.uni-jena.de-Domain beziehen

Titel: "IT-Sicherheit Digitale Zertifikate"

Stand: 27.05.2022

FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA