Verschlüsseln und Signieren

Zusammenfassung

Das Prinzip Ihres digitalen Zertifikates basiert auf der asymmetrischen Verschlüsselung. Bei der asymmetrischen Verschlüsselung wird für jeden, der 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.

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**
- **alle sonstigen Zwecke**

Das bedeutet, dass Ihr E-Mail-Partner mit dem **öffentlichen Schlüssel**, den er von Ihnen bekommen hat, E-Mails an Sie **verschlüsseln** kann. Diese sind nur für Sie lesbar, d.h. **entschlüsselbar** , weil Sie Ihren **privaten Schlüssel** in Verbindung mit Ihrer E-Mail-Adresse benutzen. 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 Besitzer des passenden privaten Schlüssels) und der Gültigkeitszeitraum. Wenn zwei Kommunikationspartner einander sicher Nachrichten übermitteln möchten, tauschen sie ihre Zertifikate aus und erhalten damit die Möglichkeit, Nachrichten so zu verschlüsseln, dass sie nur der jeweils andere entschlüsseln kann. Zusätzlich können sie auch die digitale Signatur des anderen überprüfen.

ⓘ Damit die Zertifikate ausgetauscht werden können, müssten sich die Kommunikationspartner allerdings kennen und einen sicheren Weg für den Austausch finden, um sicher zu gehen, dass sie auch tatsächlich das Zertifikat der Person oder Institution erhalten, mit der sie kommunizieren möchten. Eine Möglichkeit wäre, die Zertifikate per eMail 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.

Wenn Sie mehr dazu wissen möchten, informieren Sie sich bitte hier. (Quelle: BSI)

Folgende Seiten geben detaillierte Informationen:

Titel: "Verschlüsseln und Signieren"

Stand: 11.02.2021

FRIEDRICH-SCHILLER-UNIVERSITÄT JENA