Zertifikate - Regeln und Begriffserklärung

Zusammenfassung

Rund um die Thematik "Zertifikate" sind hier die wesentliche Begriffe näher erklärt.

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**

Begriffe und Abkürzungen

Authentizität bedeutet Echtheit im Sinne von "als Original befunden". Das Adjektiv zu Authentizität heißt authentisch.

Ein **digitales Zertifikat** ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten.

Integrität (Informationssicherheit) Integrität ist neben Verfügbarkeit und Vertraulichkeit eines der drei klassischen Ziele der Informationssicherheit. Eine einheitliche Definition des Begriffs Integrität gibt es nicht. In den Evaluationskriterien für Informationssicherheit der frühen 1990er Jahre (ITSEC) wird Integrität definiert als "Verhinderung unautorisierter Modifikation von Information". Laut Glossar des Bundesamtes für Sicherheit in der Informationstechnik bezeichnet Integrität die "Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen".

Die Abkürzung **PKI** steht für ein System in der Kryptologie (Public-Key-Infrastruktur). Mit Public-Key-Infrastruktur (PKI, public key infrastructure) bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

D**as Recht auf informationelle Selbstbestimmung** ist im bundesdeutschen Recht das Recht des/der Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate. Aktuell ist Version 3 (X.509v3).

GRID (engl.: Verteilernetz) GRID-Server ermöglichen das GRID-Computing. Es ist ein virtueller Computer, der aus mehreren Computern erzeugt wird, um komplexe rechenintensive Aufgaben zu lösen. Es wird auch als verteiltes Rechnen bezeichnet.

Zusammenfassung

Verlust und Ungültigkeit; abgelaufene Schlüssel

In folgenden Fällen ist es notwendig, das Zertifikat offiziell sperren zu lassen, um Missbrauch zu verhindern:

- Änderung der zum Zertifikat gehörenden E-Mail-Adresse. Das Zertifikat muss zur E-Mail-Adresse passen, beides gehört unbedingt zusammen.
- Der Verlust des persönlichen Schlüssels (durch Datendiebstahl, Einsicht des Speicherortes durch Dritte oder Löschen) macht das Schlüsselpaar für die künftige Nutzung zum Verschlüsseln oder Signieren unbrauchbar.

Das aktuelle Zertifikat sollte zum Standard erklärt, das abgelaufene Zertifikat aber nicht gelöscht werden. Nur mit den "alten" Zertifikaten können die "alten" E-Mails gelesen werden. Das gilt für alle E-Mail-Partner/Innen, mit denen verschlüsselte und/oder signierte E-Mails ausgetauscht werden.

Das aktuelle Zertifikat zum Standarderklären, aber das abgelaufene Zertifikat nicht löschen. Nur mit den "alten" Zertifikaten kann man die "alten" E-Mails lesen. Das gilt für alle E-Mail-Partner, mit denen verschlüsselte und/oder signierte E-Mails ausgetauscht werden.

Außerdem:

1. Der private Schlüssel muss unbedingt aufgehoben werden!
2. Alle Schlüssel bleiben bis zum Widerruf gültig.

3. Ein Zertifikat immer mit demselben Browser beantragen und abholen, zwischen Beantragung und Abholung darf nie der PC gewechselt oder eine neue Installation vorgenommen werden.
4. Der Link von der CA (Zertifizierungsstelle) sollte aus der E-Mail kopiert und im Browser, mit dem die Beantragung erfolgt ist, in die Adresszeile /URL eingefügt werden.
5. Keine Umlaute und/oder Leerzeichen verwenden.
    a. Das Zertifikat muss auf die E-Mail-Adresse passen, beides gehört unbedingt zusammen.
    b. Eine E-Mail-Verschlüsselung betrifft immer die komplette E-Mail einschließlich der Anhänge;

Mit dem öffentlichen Schlüssel (des Partners/der Partnerin) können Mails (für den Partner/für die Partnerin) verschlüsselt sowie dessen Unterschrift geprüft werden;

Mit dem privaten Schlüssel (des Besitzers/der Besitzerin) können E-Mails entschlüsselt werden, die mit (des Besitzers/der Besitzerin) öffentlichem Schlüssel verschlüsselt wurden, und der Besitzer/die Besitzerin kann seine/ihre Nachrichten damit unterschreiben.

Verwandte Artikel

- Zertifikate in E-Mail-Programmen am Beispiel von Outlook
- Überprüfung offener Port 443 und gültige Serverzertifikate
- Zertifikate auf dem iPhone einrichten
- Zertifikate - Regeln und Begriffserklärung

Titel: "Zertifikate - Regeln und Begriffserklärung"

Stand: 01.01.2021

FRIEDRICH-SCHILLER-UNIVERSITÄT JENA