Elektronische Zertifikate

Elektronische Zertifikate sind – allgemein beschrieben – elektronische Bescheinigungen, die einem Zertifikatsinhaber bestimmte Informationen zuordnen.

Als Teil der DFN-PKI stellt die HHU Düsseldorf über den TCS Zertifikate aus. Dies wird mithilfe eines externen Anbieters, aktuell Sectigo, realisiert.

Damit erhalten Mitarbeiter:innen der HHU die Möglichkeit, Zertifikate nach dem X.509 Standard zu beantragen und dadurch Verschlüsselungsverfahren nach S/MIME zu nutzen. Ein solches Zertifikat bietet Ihnen für folgende Anwendungsszenarien ein Mehr an Sicherheit:

Nutzerzertifikate für signierte und verschlüsselte Mails

Wie hinlänglich bekannt, sind Mails – übertragen auf den Briefwechsel in der analogen Welt – eher mit Postkarten zu vergleichen als mit Briefen. Das bedeutet: alle am Transport Beteiligten können theoretisch mitlesen oder sogar Inhalte verändern.

Die Einbindung von elektronischen Zertifikaten in Ihren Mailclient hat diese Vorteile:

1. **Authentizität** durch Verifikation des Absenders (präziser formuliert: Bestätigung, dass ein bestimmter öffentlicher Schlüssel zu einer bestimmten Person gehört)
2. **Vertraulichkeit** durch Ende-zu-Ende-Verschlüsselung per S/MIME
3. **Integrität** der Inhalte

Wichtig

Private Schlüssel des persönlichen Nutzerzertifikates dürfen an niemanden weitergegeben werden und müssen mit einem guten Passwort geschützt werden, da sonst Gefahr zum Missbrauch des Zertifikats besteht.

Öffentliche Schlüssel werden mit jeder unterschriebenen Mail automatisch mitgeschickt und im Mail-System des Empfängers gespeichert. Über diesen Öffentlichen Schlüssel können Ihre Empfänger Ihre Unterschrift überprüfen und verschlüsselte Mails an Sie senden, demnach müssen sie Jemanden der eine verschlüsselte Mail an sie senden soll zuerst eine signierte Mail schicken oder den öffentlichen Schlüssel anders überreichen. Verschlüsselte Mails können nur mit dem zugehörigen privaten Schlüssel wieder entschlüsselt werden.

Nutzerzertifikate für den Schutz und die Integrität von PDF-Dokumenten

Mit einem Nutzerzertifikat können Sie auch PDF Dokumente per S/MIME signieren und verschlüsseln. Die Einbindung eines Nutzerzertifikates des DFN ermöglicht Ihnen, PDF-Dokumente mit einer fortgeschrittenen elektronische Signatur (nach eIDAS Verordnung § 26) zu versehen. Damit ist die Signatur eindeutig dem Zertifikatsinhaber zuzuordnen, da nur dieser Zugriff auf die Zertifikatsdatei inkl. Passwort hat und vorab eine Authentifizierung der Identität des Nutzers stattgefunden hat. Neben der Bestätigung der Identität kann durch elektronische Signaturen zudem sichergestellt werden, dass das übermittelte Dokument nach dem Versenden nicht geändert wurde.

S/MIME – Grundlegende Funktionsweise

Grundlage von S/MIME ist ein asymmetrisches Verschlüsselungsverfahren. Als Nutzende erhalten Sie somit ein komplementäres Schlüsselpaar, das aus einem **privaten Schlüssel** und einem **öffentlichen Schlüssel** besteht. Während der private Schlüssel nur dem Anwender selbst bekannt sein darf, kann und soll der öffentliche Schlüssel mit den Kontaktpersonen geteilt werden.

Die sendende Person verschlüsselt eine Nachricht mit dem öffentlichen Schlüssel der empfangenden Person (den diese zuvor per signierter E-Mail oder ähnlich erhalten hat). Daraufhin kann nur die Person mit ihrem privaten Schlüssel den Inhalt dechiffrieren und lesen.

Serverzertifikate

Die vom DFN ausgestellten Zertifikate ermöglichen es Ihnen als IT- Dienstbetreiber, Ihren IT-Dienst gegenüber Nutzenden auszuweisen. Durch die Zertifizierung wird bestätigt, dass ein bestimmter öffentlicher Schlüssel zu einem bestimmten IT-Dienst gehört. Digitale Zertifikate auch hier:

- **Integrität**
- **Vertraulichkeit**
- **Authentizität**

Direkt zu

Abkürzungen

Abk	steht für	Infos
DFN	Deutsches Forschungsnetz	Verein zur Förderung eines Deutschen Forschungsnetzes e. V. - eine selbstverwaltete Organisation
PKI	Public Key Infrastruktur	ein hierarchisches System zur Ausstellung, Verteilung und Prüfung von digitalen Zertifikaten
TCS	Trusted Certificate Service	TCS wird das bisherige DFN-PKI Sicherheitsniveau „Global“ ablösen.

Rechtliche Grundlagen elektronischer Signaturen

Bei elektronischen Signaturen wird zwischen drei Varianten unterschieden:

- Einfache elektronische Signatur
- Fortgeschrittene elektronische Signatur
- Qualifizierte elektronische Signatur

Die Erklärungen dazu können Sie auf den Seiten des DFN nachlesen: https://doku.tid.dfn.de/de:dfnpki:pkifaq:sigsie_faq

Bei fachlichen Fragen und Anmerkungen rund um das Thema Zertifikate wenden Sie sich bitte an ca@hhu.de

CSR	Certificate Signing Request	digitaler Antrag, um mittels einer digitalen Signatur aus einem öffentlichen Schlüssel ein digitales Zertifikat zu erstellen
CA	Certification Authority	Eine Zertifizierungsinstanz (engl. Certification Authority, CA) stellt Zertifikate aus, indem sie die Zertifikatsinhalte mit einer digitalen Signatur versieht
S/MIME	Secure Multipurpose Internet Mail Extension	Protokoll für die E-Mail-Kommunikation, das es ermöglicht, Nachrichten zu verschlüsseln oder zu signieren.