Allgemeine Hinweise

Um in der digitalen Welt sinnvoll etwas unterschreiben zu können, muss jemand bestätigen, dass eine Unterschrift einer bestimmten Person gehört. Diese Aufgabe übernimmt eine Zertifizierungsstelle, auch CA[1)] genannt: Sie stellt ein Zertifikat aus, welches zu einem geheimen Schlüssel (der Unterschrift) passt und Informationen darüber enthält, wem die Unterschrift gehört.

Damit die ausgestellten Zertifikate glaubwürdig sind, ist vertraglich geregelt, wer unter welchen Bedingungen ein Zertifikat bekommt. Diese Verträge kann man auf der Webseite der TU-Clausthal-CA unter dem Punkt „DFN-PKI-Policy“ bzw. „Anwender-Policy“ ansehen.

Da der Betrieb einer Zertifizierungsstelle mit einer großen Verantwortung und hohem Aufwand einhergeht, nutzen wir an der TU Clausthal das Angebot des DFN-Vereins, eine ausgelagerte Zertifizierungsstelle für uns zu betreiben. Um bei der Beantragung und Erstellung neuer Zertifikate unnötig lange Wege zu vermeiden, sind einige Mitarbeiter des Rechenzentrums dazu berechtigt worden, Zertifikatsanträge nach einer Identitätskontrolle zu genehmigen und die Generierung eines Zertifikates zu beauftragen.

Arten von Zertifikaten und deren Einsatzzweck

Es gibt verschiedene Arten von Zertifikaten. Von der TU Clausthal CA können derzeit folgende Zertifikate ausgestellt werden:

Nutzer-Zertifikate

Nutzer-Zertifikate bestätigen die Identität einer Person bzw. einer bestimmten Gruppe von Personen. Sie werden vor allem verwendet, um E-Mails zu unterzeichnen und damit sicher zu stellen, dass eine E-Mail auch tatsächlich vom vermeintlichen Absender verfasst wurden. Leider ist das bei E-Mails nicht automatisch sichergestellt: Genauso wie Sie auf einem Briefumschlag eine falsche Absenderadresse angeben können, können E-Mails unter falschem Absender verschickt werden. Während man zwar vielleicht am Inhalt der E-Mail feststellen kann, ob es sich um den richtigen Absender handelt, bekommt man durch eine digitale Unterschrift größere Sicherheit: Neben der Identität des Absenders kann man auch noch prüfen, ob der Nachrichtentext verändert wurde.

Eine weitere Möglichkeit beim Einsatz von Nutzer-Zertifikaten ist, dass man den Inhalt einer E-Mail verschlüsselt vom Absender zum Empfänger übermittelt. Dadurch wird die Vertraulichkeit der Nachricht gewahrt.

Neben E-Mails können auch z.B. PDF-Dokumente digital unterschrieben werden.

Des Weiteren können Nutzer-Zertifikate auch für die Anmeldung an Webseiten (z.B. SAP-System)

verwendet werden.

Server-Zertifikate

Ein Server-Zertifikat bestätigt die Echtheit eines Servers. Wenn Sie z.B. den Webmail-Dienst der TU-Clausthal aufrufen, prüft ihr Browser anhand eines Zertifikats, ob sich der richtige Server gemeldet hat. Das ist gut und wichtig, weil sie dort ja schließlich ihren Benutzernamen und Ihr Passwort eintragen.

Weitere Informationen zu Server-Zertifikaten finden Sie auf der Seite Allgemeine Informationen zu Server-Zertifikaten.

Technische Vorgehensweise

- Beim Erzeugen des Zertifikates per Web-Browser wird ein privater Schlüssel und ein öffentlicher Schlüssel generiert. Während der private Schlüssel im Zertifikatsspeicher der Anwendung oder des Systems liegt, wird der öffentliche Schlüssel über die Registrierungsstelle im Rechenzentrum an die TU Clausthal CA weitergereicht und signiert. Damit erhalten Sie ein X.509-basiertes Zertifikat, mit dem Sie eine Email mit S/MIME-Content erzeugen können, also einen verschlüsselten Mail-Text incl. Anhänge erzeugen können. Email-Clients wie Mozilla Thunderbird und MS Outlook beherrschen dieses Verschlüsselungsverfahren.
- Um ein User-Zertifikat registriert bzw. signiert zu bekommen, muss die Identität der beantragenden Person anhand eines gültigen Lichtbildausweises überprüft werden. Dazu lesen Sie bitte unter „Akkreditierte Personen“ weiter.
- Asymmetrischen Verschlüsselungsverfahren
- Nutzer-Zertifikate mit Mozilla-Applikationen unter Linux/Unix (Firefox, Thunderbird)
- Nutzer-Zertifikate unter Windows (IE8 und Outlook)

Links

- TU Clausthal CA Einstiegsseite
- FAQs zu Nutzer- und Server-Zertifikaten

[rzmitarbeitende], [dev0]

1)

Certification Authority