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.

Da der Betrieb einer Zertifizierungsstelle mit einer großen Verantwortung und hohem Aufwand einhergeht, nutzen wir an der TU Clausthal sowohl ein Angebot des DFN-Vereins als auch den allgemein Verfügbaren Dienst "Let's Encrypt". Um bei der Beantragung und Erstellung neuer Zertifikate unnötigen Aufwand zu vermeiden, erfolgt die Zertifikatserstellung automatisiert.

Arten von Zertifikaten und deren Einsatzzweck

Es gibt verschiedene Arten von Zertifikaten. Über das Angebot des DFN-Vereins werden im Allgemeinen Nutzer-Zertifikate erstellt, während für Server-Zertifikate "Let's Encrypt" empfohlen wird.

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.

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.

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. Hier ist allerdings wichtig, dass die E-Mail nur mit dem entsprechenden Zertifikat wieder gelesen werden kann - es muss also aufbewahrt werden, selbst wenn es abgelaufen ist.

Außerdem ist das Übergeben von E-Mails an einen Nachfolger im Amt nicht ohne weiteres möglich, weil sie an den Empfänger persönlich verschlüsselt wurden.

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.

Zertifikate, die von Zertifizierungsstellen wie Let's Encrypt erstellt werden, werden automatisch von den Nutzerprogrammen akzeptiert. Aufforderungen zur manuellen Überprüfung von Zertifikaten werden nicht mehr angezeigt.

Technische Vorgehensweise

- Beim Erzeugen des Zertifikates auf der Webseite der CA wird ein privater Schlüssel und ein signierter öffentlicher Schlüssel generiert und ihnen zum Herunterladen bereitgestellt. Damit erhalten Sie ein X.509-basiertes Zertifikat, mit dem Sie eine E-Mail mit S/MIME-Content erzeugen können, also einen verschlüsselten Mail-Text incl. Anhänge erzeugen können. E-Mail-Clients wie Mozilla Thunderbird und MS Outlook beherrschen dieses Verschlüsselungsverfahren.
- Um ein Nutzer-Zertifikat zu bekommen, muss die Identität der beantragenden Person anhand ihres Benutzernamens und Passworts überprüft werden. Dazu folgen Sie bitte der Anleitung Zertifikatserstellung / Beantragung eines Nutzerzertifikats.
- Für Server-Zertifikiate sollen in der Regel selbst-aktualisierende Mechanismen ("Let's Encrypt", ACME) eingesetzt werden. Im Umkehrschluss bietet das RZ Server-Zertifikate nur noch in Ausnahmefällen an. Bitte kontaktieren Sie uns, bevorzugt per E-Mail falls Sie eine Sonderlösung benötigen, um gemeinsam eine gute individuelle Lösung zu finden.
- Asymmetrischen Verschlüsselungsverfahren
- Nutzer-Zertifikate mit Mozilla-Applikationen unter Linux/Unix (Firefox, Thunderbird)
- Nutzer-Zertifikate unter Windows (IE8 und Outlook)

[rzmitarbeitende], [dev0]

1) Certification Authority