Verschlüsseln und Signieren mit Zertifikaten

Zertifikat: Digital signierter öffentlicher Schlüssel mit Zusatzinformationen

Zu jedem Zertifikat hat der Eigentümer (!) einen privaten Schlüssel.

Grundlegendes: Privater Schlüssel und Zertifikat (öffentlicher Schlüssel) werden zusammen erzeugt.

Was mit dem einen VERschlüsselt wird, kann NUR mit dem anderen ENTschlüsselt werden!

Daten/Dokumente verschlüsseln

Mit dem ÖFFENTLICHEN Schlüssel wird verschlüsselt. Der Empfänger kann mit mit seinem PRIVATEN Schlüssel wieder entschlüsseln.

Daten/Dokumente digital signieren

1. Es wird (vom Programm, Word, Outlook, Thunderbird, Libreoffice, … eine Prüfsumme gebildet über das Dokument, diese ist für das Dokument eindeutig, d.h. es gibt kein zweites Dokument (und lässt sich auch nicht herstellen), das die gleiche Prüfsumme hat.
2. Der Urheber des Dokument (bzw. sein Programm, s.o.) VERSCHLÜSSELT die Prüfsumme des Dokuments mit seinem PRIVATEN Schlüssel (den sonst niemand hat), und verschickt das Dokument und die verschlüsselte Prüfsumme an alle Empfänger.
3. Die Empfänger können nur mit Hilfe des ÖFFENTLICHEN Schlüssels des Urhebers die Prüfsumme entschlüsseln, und schauen, ob sie noch auf das Dokument passt.