cryptocafé

so geht verschlüsselte kommunikation

Wer sind wir?

cryptocafé

Einführung

Motivation und Funktionsweise von Verschlüsselung

- PGP
- S/MIME

Praxisteil

- Demonstration zur Verschlüsselung
- Einrichtung der Methoden in Thunderbird

Warum Mails verschlüsseln?

Vertraulichkeit

Authentizität

Integrität

PGP / GPG

Software zum Verschlüsseln und Signieren von

- E-Mails
- Dateien
- Festplatten

Public Key Infrastruktur

Vertrauensmodell: Web Of Trust

PGP

Pretty **G**ood **P**rivacy

- Ursprüngliche Software
- 1991 Phil Zimmermann
- Mittlerweile Firma PGP Inc.

GPG / GnuPG

Gnu **P**rivacy **G**uard

Freie Software

Nachbau der Funktionalität

1999 Werner Koch

S/MIME

Ebenfalls asymmetrisches Verschlüsselungsverfahren

weitverbreiteter Standard

„out of the box" Unterstützung

Zertifikatbasiert

Abhängigkeit von Zertifizierungsstellen

Class 1 / Class 2

Praxisteil

PGP

Installation Thunderbird + Enigmail

Erstellen + Upload des eigenen Schlüssels

Versand einer Mail

Links

https://www.gpg4win.org/

https://www.mozilla.org/de/thunderbird/

https://addons.mozilla.org/de/thunderbird/addon/enigmail/

https://keyserver.pgp.com

S/MIME

Zertifikat erstellen

Import des Zertifkats

Versand einer Mail

Links

https://www.mozilla.org/de/firefox/

https://www.comodo.com/home/email-security/free-email-certificate.php

Signal Messenger