

## Sichere E-Mails mit Thunderbird und GPG

In Thunderbird sind nur wenige Handgriffe nötig, um PGP-verschlüsselte E-Mails zu verschicken und zu empfangen. Nachfolgend zeigen wir Ihnen die Einrichtung.

Ein rar-Archiv mit allen nötigen Dateien können Sie von dem vom Lehrer angegebenen Web-Server oder von <http://intranet/files/sichere-e-mails-mit-thunderbird-und-gpg.rar> herunterladen.

Rechner-Zeit korrekt einstellen stellen Sie die Rechner-Zeit auf die aktuelle Zeit ein!

### Erreichbarkeit des Mail-Servers sicherstellen

- notieren Sie sich die angegebene IP-Adresse des Mail-Servers: \_\_\_\_\_
- testen Sie die Erreichbarkeit des Mail-Servers mit **ping**
- da wir keinen DNS-Server betreiben, muss die Namensauflösung lokal über die **hosts**-Datei erfolgen:  
Tragen Sie dazu die IP-Adresse des Mail-Servers in `C:\WINDOWS\system32\drivers\etc\hosts` ein:  
**Beispiel: 192.168.10.13 mail.localserver.com**
- testen Sie die lokale Namensauflösung und die Erreichbarkeit des Mail-Servers noch einmal mit:  
**ping mail.localserver.com**
- prüfen Sie, ob der Mailserver die Ports 25 (SMTP) und 110 (POP3) geöffnet hat:  
**nmap mail.localserver.com**

### Thunderbird-Portable installieren

- installieren Sie Thunderbird-Portable in ein Verzeichnis, in dem Sie über Schreibrechte verfügen
- erstellen Sie auf das Programm **ThunderbirdPortable.exe** einen Link auf den Desktop
- starten Sie Thunderbird und aktivieren Sie die Menüleiste
- konfigurieren Sie über *Einstellungen* --> *Einstellungen* folgendes:  
*Allgemein:* Startseite nicht anzeigen  
*Chat:* Chat-Konten nicht verbinden  
*Erweitert:* Updates und Hintergrunddienst deaktivieren

### E-Mail-Adresse und Mail-Server einstellen

- richten Sie in Thunderbird über *Einstellungen* --> *Konto-Einstellungen* für **Ihren** Platz ein neues E-Mail-Konto ein:

#### Achtung:

Benutzen Sie **Ihre** Platz-Kennung!

#### Beispiel-Konfiguration:

#### E-Mail Konto für Platz13 einrichten

Hinweis: Eingabe für Platz 0-9 ohne führende 0 → Platz1

Name: platz13  
 E-Mail-Adresse: platz13@mail.localserver.com  
 Passwort: platz13

Posteingangsserver:  
 POP3, Server-Adresse: mail.localserver.com

Postausgangsserver:  
 SMTP, Server-Adresse: mail.localserver.com

dann auf den Button **Testen** drücken

- wenn der Test erfolgreich war, klicken Sie auf **Fertig** und akzeptieren Sie die Warnung über den unverschlüsselten Mail-Versand
- testen Sie die Mail-Zustellung, indem Sie sich selbst eine Mail zusenden
- testen Sie den Mail-Abruf
- senden Sie jetzt eine Mail an ihren Nachbarn mit dem Betreff: *Testmail*

### gpg4Win installieren

- starten Sie die Installations-Datei **gpg4win-2.2.1.exe** und installieren Sie das Programm mit den vorgeschlagenen Optionen

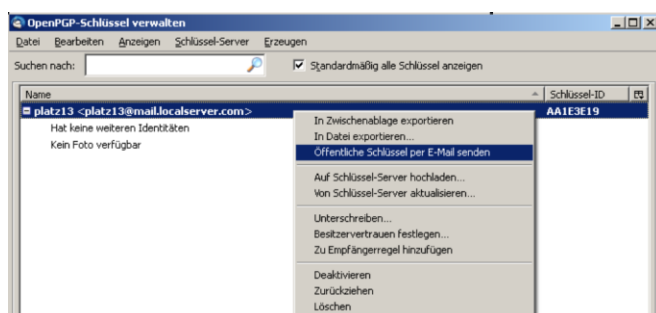
### Thunderbird Add-On Enigmail installieren

- klicken Sie in Thunderbird über *Add-ons* auf das kleine Zahnrad-Symbol in der oberen rechten Ecke und aktivieren Sie *Add-on aus Datei installieren*,
- wählen Sie **enigmail-1.6-sm+tb.xpi** aus und starten Sie Thunderbird anschließend neu

### OpenPGP in Thunderbird aktivieren

- in Thunderbird über *OpenPGP* den Assistenten starten und folgendes durchführen:
  - *Ja, ich möchte, dass mir der Assistent hilft*
  - *Nein, ich möchte in den Empfängerregeln festlegen, wann unterschrieben werden soll*
  - *Nein, ich möchte in Empfängerregeln festlegen, wann verschlüsselt werden soll*
  - *Ja, Einstellungen anpassen lassen*
  - *Neues Schlüsselpaar erzeugen*
  - Passphrase eingeben, min. 8 Zeichen, z.B.: *platz13-phrase*
  - kein Widerrufszeugat erzeugen

### Ihren öffentlichen Schlüssel verschicken



- im Menü über *OpenPGP* --> *Schlüssel verwalten*
- aktivieren Sie *Standardmäßig alle Schlüssel anzeigen*
- über das Kontextmenü des zu versendenden Schlüssels *Öffentlicher Schlüssel per E-Mail versenden* Ihren Öffentlichen Schlüssel an Ihren Nachbarn senden
- mit **Betreff:** PGP-Key (*IhrePlatzNr*)

### Öffentliche Schlüssel importieren

- Sie können die Öffentlichen Schlüssel direkt aus dem Anhang der Mails Ihrer Nachbarn importieren, indem Sie im Posteingangsfenster unten links über das Kontext-Menü der .asc Datei im Anhang den Menüpunkt *OpenPGP-Schlüssel importieren* auswählen.

### Verschlüsselte Nachricht senden

- wenn Sie eine verschlüsselte Mail senden wollen, müssen Sie dies vor dem Senden im OpenPGP-Menü über *Nachricht verschlüsseln* auswählen.
- bei der ersten Sendung an eine E-Mail-Adresse müssen Sie deren Identität noch konfigurieren, hier können Sie die angebotenen Standardeinstellungen akzeptieren.

**ACHTUNG:** Es wird immer nur der Mail-Text (Body) verschlüsselt, nie die Betreff-Zeile!

### Digital signierte Nachricht senden

- um eine unverschlüsselte, aber digital signierte Nachricht zu senden, müssen Sie vor dem Senden im OpenPGP-Menü *Nachricht unterschreiben* auswählen.

### Datenverkehr beobachten

- versenden Sie Mails unverschlüsselt, digital signiert und verschlüsselt und beobachten Sie den dabei entstehenden Datenverkehr mit dem Netzwerksniffer **wireshark**
- benutzen Sie bei **wireshark** die Funktion *Follow TCP Stream*, die Sie über das Kontextmenü der aufgezeichneten Datenpakete erreichen

**Links**     [www.tacticalcode.de/2013/06/emails-verschluseln-mit-thunderbird-gpg-und-enigmail.html](http://www.tacticalcode.de/2013/06/emails-verschluseln-mit-thunderbird-gpg-und-enigmail.html)  
               [www.heise.de/ct/artikel/Thunderbird-Mails-mit-PGP-verschluseln-1916630.html](http://www.heise.de/ct/artikel/Thunderbird-Mails-mit-PGP-verschluseln-1916630.html)