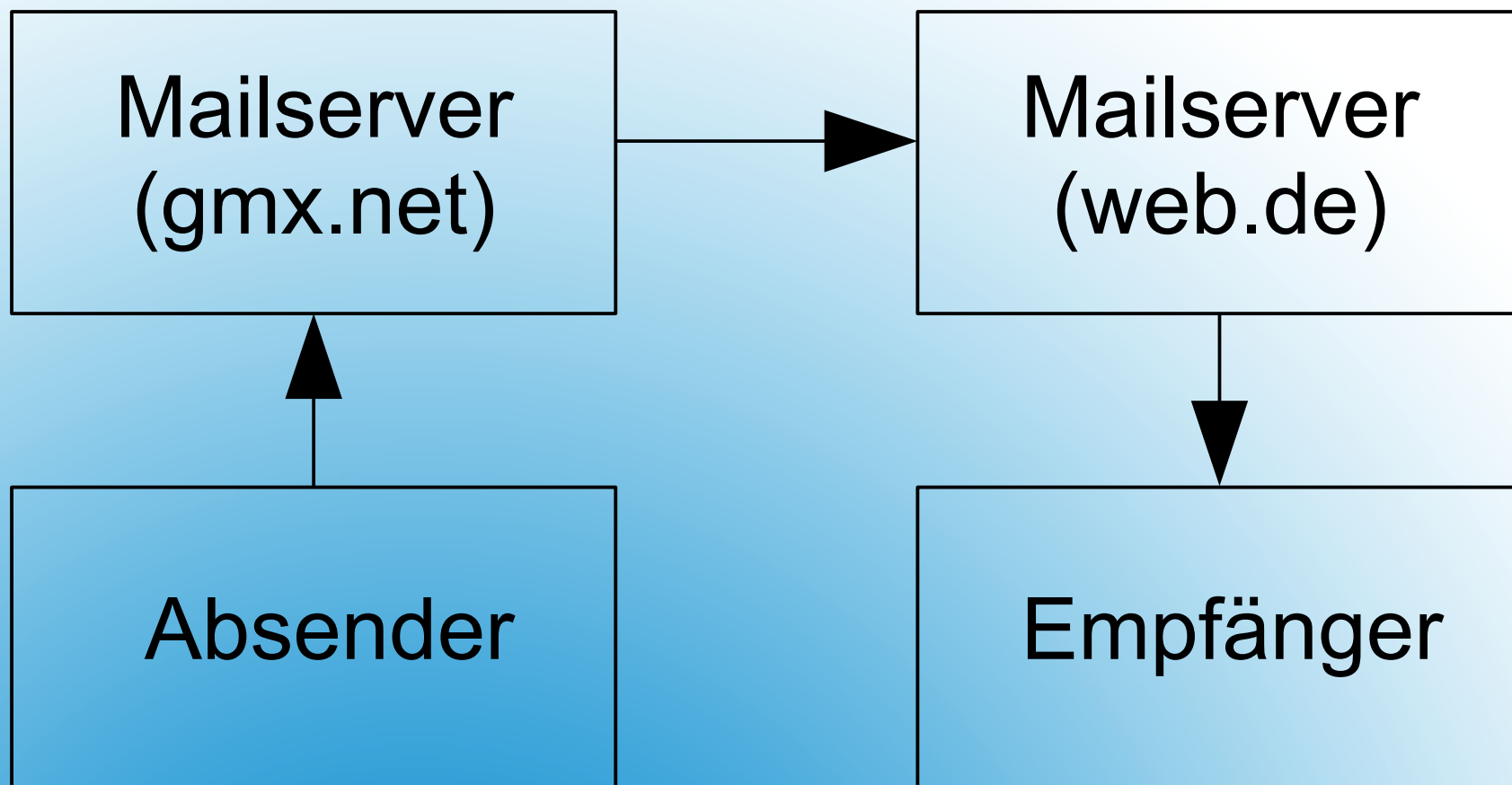


eMails verschlüsseln: Warum und Wie?

- Wie funktioniert eMail?
- Wo können Fremde mitlesen?
- Wie funktioniert Verschlüsselung (Prinzip)?
- Wie richte ich Thunderbird zur eMail-Verschlüsselung mit PGP ein?
- Was für Alternativen gibt es?
- Wogegen hilft Verschlüsselung nicht?

Übersicht



**Wie funktioniert eMail?
Wo können Fremde mitlesen?**

- Asymmetrische Verschlüsselung
- Jeder Nutzer erstellt ein Schlüsselpaar aus zwei Schlüsseln:
 - Privater Schlüssel, private/secret key
 - Öffentlicher Schlüssel, public key
- Absender verschlüsselt Nachricht mit public key des Empfängers
- Nachricht kann **nur** mit dazugehörigem secret key entschlüsselt werden

**Wie funktioniert eMail-
Verschlüsselung (Prinzip)**

- PGP-Software: gnupg, www.gnupg.org
 - Aktuell: 1.4.10 oder 2.x
- Frontend zur PGP-Software
 - Für Thunderbird, Seamonkey, Mozilla, Netscape: enigmail, enigmail.mozdev.org (aktuell: 0.96.0)
 - Evolution enthält bereits ein PGP-Frontend
 - Auch für Outlook und OE...
http://www.gnupg.org/related_software/frontends.en.html#mua

**Wie richte ich Thunderbird o.a.
für Verschlüsselung ein? (I)**

- Schlüsselpaar generieren
- (Revocation Key generieren)
- Public Key auf Keyserver (oder Webseite oder... hochladen)
- Public Key des Empfängers von Keyserver (oder Webseite oder...) organisieren
- Mail schreiben

Vorführung

**Wie richte ich Thunderbird o.a.
für Verschlüsselung ein? (II)**

- **S/MIME**
 - Meist kostenpflichtig.
 - Zertifikate (= Schlüssel) werden zentral gemanaged und überprüft
 - In mehr eMail-Clients direkt integriert
- IMHO für Verschlüsselung weniger wichtig, eher für Signaturen (was das ist? Nächste Seite)

Alternativen

- Empfänger will sicher sein, dass der Sender stimmt
 - Signatur: Mit private key signieren, mit public key verifizieren
- Sender will sicher sein, dass der Empfänger stimmt
 - Web of trust
 - Zentrale Authentifizierungsstelle (Modell S/MIME)
- Unverschlüsselte Passwortangabe → Zeigen

Wogegen hilft Verschlüsselung nicht?

- Gnupg: www.gnupg.org
- Enigmail: enigmail.mozdev.org
- Schlüsselpaar generieren
- Öffentlichen Schlüssel hochladen
- Öffentlichen Schlüssel des Empfängers runterladen
- BKA, NSA, FBI können uns mal :)

**Danke für die Aufmerksamkeit.
Fragen?**