**Landesakademie für Fortbildung u. Personalentwicklung an Schulen - Standort Esslingen**

# Mail-Client & -Verschlüsselung

## Datenschutz in der mediatisierten Schule

Esslingen, 23. Okt. 2014

Andreas Grupp
grupp@lehrerfortbildung-bw.de

# Regionale Lehrerfortbildung

- Material ist ein Bestandteil der regionalen Lehrerfortbildung

  „***PC & Internet – Sicherheitsstrategien und -lösungen für mich!***“

- Multiplikatorenkonzept

- Intention: Lehrkräfte allg. Professionalisieren, mittelfristig wird Einfluss auf Unterricht erhofft

# Mail-Client? - Wozu denn das? Ich habe Webmail!

- Vorteile eines Webmailers
  - Internet → Browser → … geht! Ist doch fein …
- Nachteile eines Webmailers
  - Mails, Adressbuch, … nur online lesbar
  - Mailbearbeitung bzw. Verfassen nur online
  - Mehrere Mailprovider → mehrere Webmailer
  - Adressbuch an Mailprovider gebunden
  - Verschlüsselung nur über vorbereiteten Datei-Anhang (z.B. TrueCrypt-Container, 7z-AES-Container, …)
  - …

# Mail-Client: Exemplarisch → Thunderbird

- Frei & für mehrere Plattformen verfügbar
- Viele Fähigkeiten, über Add-On's erweiterbar
- Portable (z.B. auf USB-Stick) installierbar
- Generelle Fähigkeiten von Mail-Clients:
  - POP3- und IMAP-fähig
  - Mehrere Mailkonten / -provider in einer Software
  - Offline-Bearbeitung von Mails
  - Übergreifende Adressbücher
  - Verschlüsselung von Mails & Anhängen möglich
  - ...

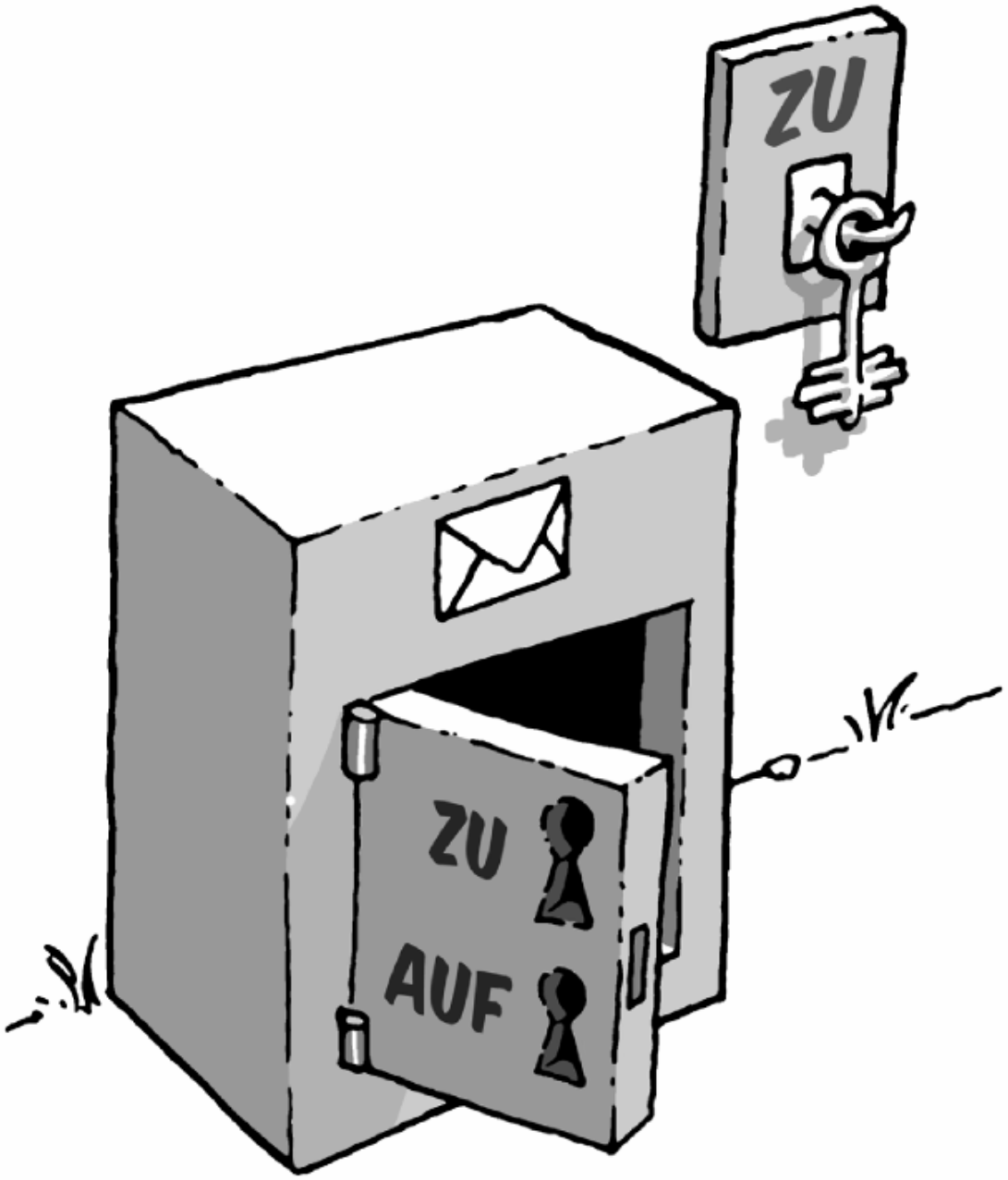
# Thunderbird-AddOns

- Erweiterte Fähigkeiten
  - Lightning – Kalender u. Aufgaben in Thunderbird. Auch synchronisierbar (z.B. mit CalDAV-Servern)
  - Mail Redirect
  - LookOut – zum Lesen von Microsoft TNEF-Anhängen
  - Enigmail – zur Ver- und Entschlüsselung von Mails mit dem OpenPGP-Standard (dazu später mehr)
  - …
- Siehe auch unter https://addons.mozilla.org/de/thunderbird/

# Übung 1: Mailprogramm verwenden

In dieser Übung installieren Sie Thunderbird, verbinden es mit einem Mailkonto und senden / empfangen Testmails an / von anderen TeilnehmerInnen

# Bei Mails verwendete Verschlüsselung - asymmetrisch

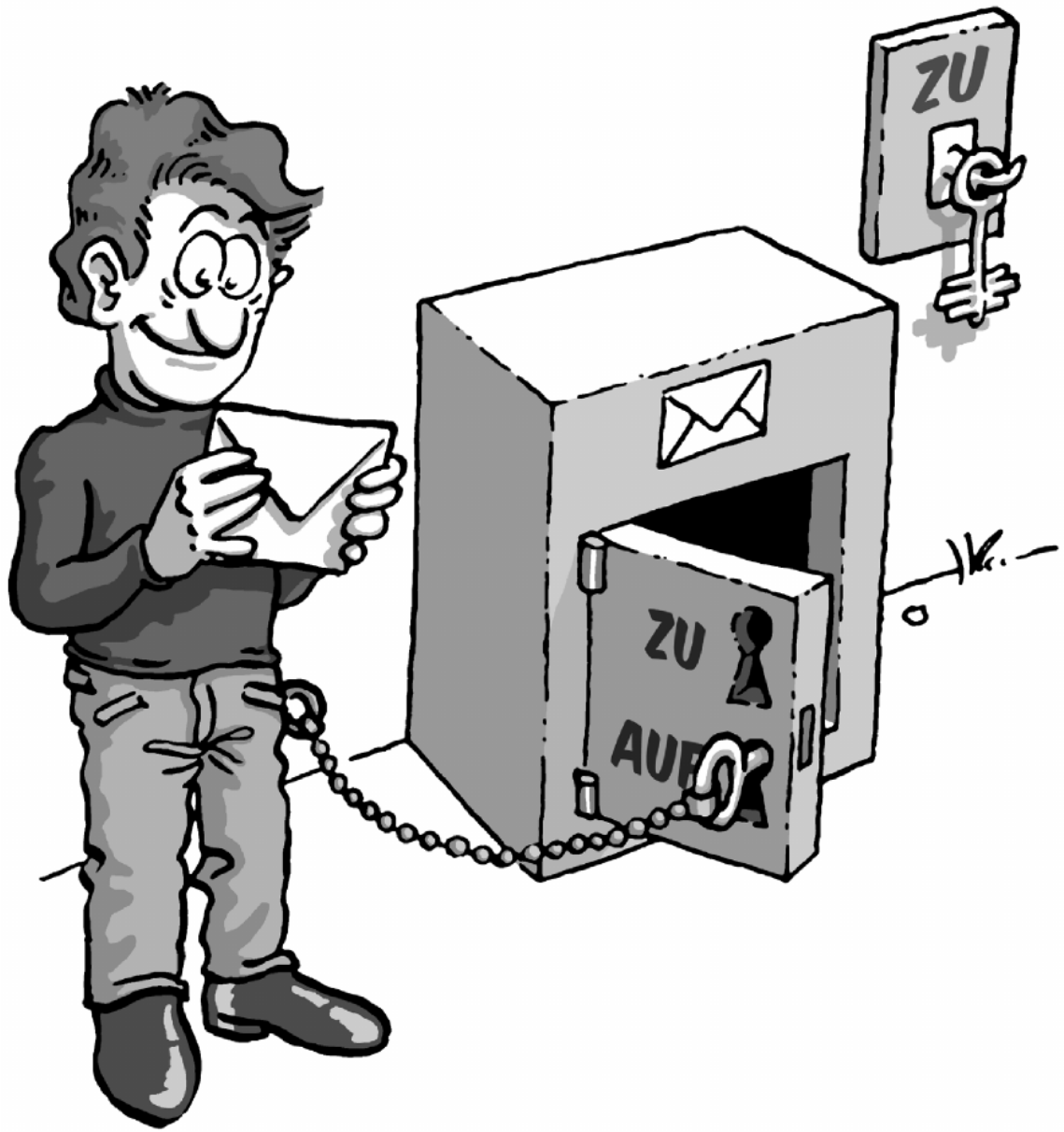



Durch den öffentlich verfügbaren „ZU“-Schlüssel kann jede Person etwas „einschließen“
→ **Verschlüsseln**

Einmal verschlüsselt kann es mit dem „ZU“-Schlüssel nicht mehr entschlüsselt werden!

Grafik-Quelle: Gpg4win-Kompendium
http://www.gpg4win.org/doc/de/gpg4win-compendium.html

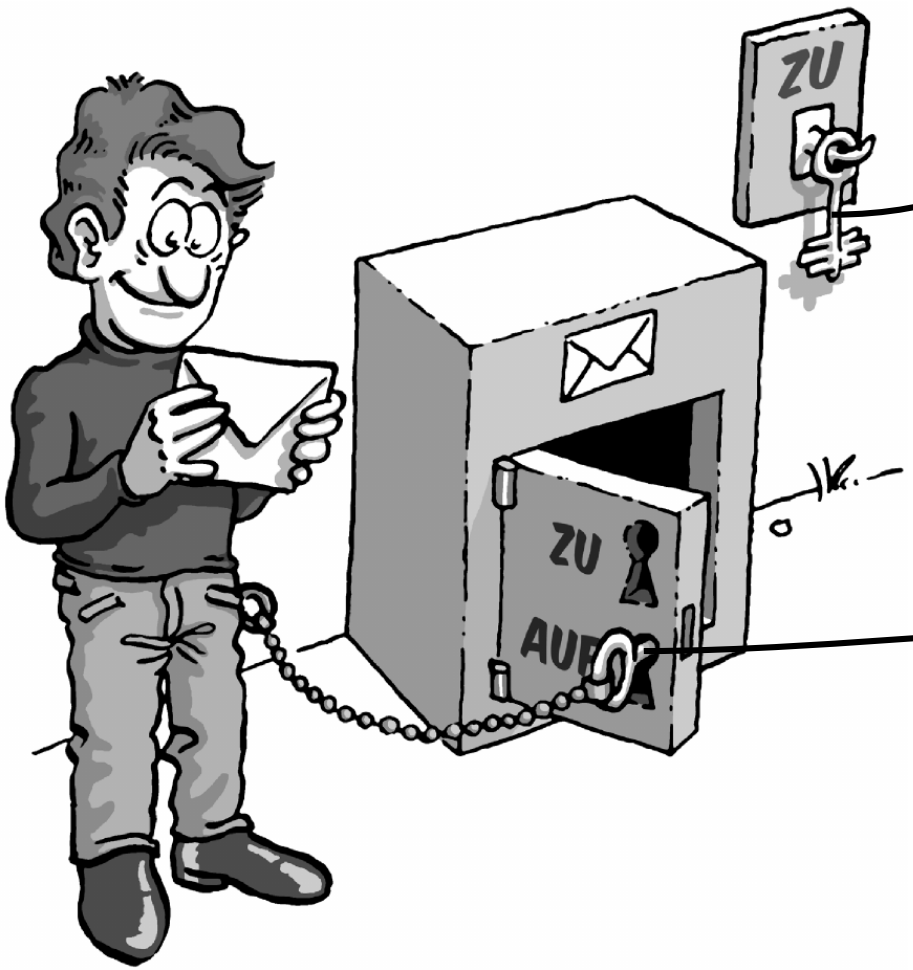
# Bei Mails verwendete Verschlüsselung - asymmetrisch




Öffnen kann nur die Person die den „AUF“-Schlüssel hat
→ **Entschlüsseln**

Grafik-Quelle: Gpg4win-Kompendium
http://www.gpg4win.org/doc/de/gpg4win-compendium.html

# Ein „Zertifikat“ besteht aus ...




→ öffentlichem Schlüssel
→ Inhaber-Informationen (z.B. Mailadresse)
→ Gemeinsame Beglaubigung dieser beiden Komponenten

→ privatem Schlüssel der nicht „aus der Hand“ gegeben wird

Grafik-Quelle: Gpg4win-Kompendium
http://www.gpg4win.org/doc/de/gpg4win-compendium.html

# Verschlüsselung bei Mails – generell 2 Varianten! (1)

Eher für absolut gehobene Sicherheitsansprüche bei IT-Profis

- Über OpenPGP-Standard
  - Kein Standard in Mailprogrammen – muss meist über Add-Ons / Plugins nachgerüstet werden
  - Benötigt zusätzlich GnuPG-Software für eigentliche Verschlüsselung
  - Nur für überschaubare Anzahl an Plattformen verfügbar → z.B. für Smartphones nicht oder nur schwer verwendbar
  - Vertrauensbasis der verwendeten Schlüssel:

    → Gegenseitige Absprachen / Beglaubigungen, das sogenannte „Web of Trust“

    → Überprüfung von Beglaubigungen aufwändig

# Verschlüsselung bei Mails – generell 2 Varianten! (2)

Im Vergleich zu OpenPGP
besser standardisiert
→ einfacher anwendbar

- Über S/MIME-Standard
  - Standard in Mailprogrammen – fast immer schon „out-of-the-box“ vorhanden – auch bei Smartphones
  - Keine weitere Verschlüsselungs-Software nötig
  - Vertrauensbasis der verwendeten Schlüssel:

    → Beglaubigung durch „digitales Notariat“ (Fachsprache: Certification Authority - CA)

    → Überprüfung der Beglaubigung mit im Mailprogramm hinterlegten Notariats-Schlüssel.
  - Schlüsselaustausch zwischen Kommunikationspartnern ist erheblich einfacher

# Zertifikate → Beantragung, Installation, Nutzung, ...

1.) Browser erzeugt Schlüsselpaar

Zertifikatsspeicher von Firefox

2b.) Privater Schlüssel

2a.) Öffentlicher Schlüssel

Certification Authority


3.) Zertifizierter öffentlicher Schlüssel

4.) Export als P12-Datei

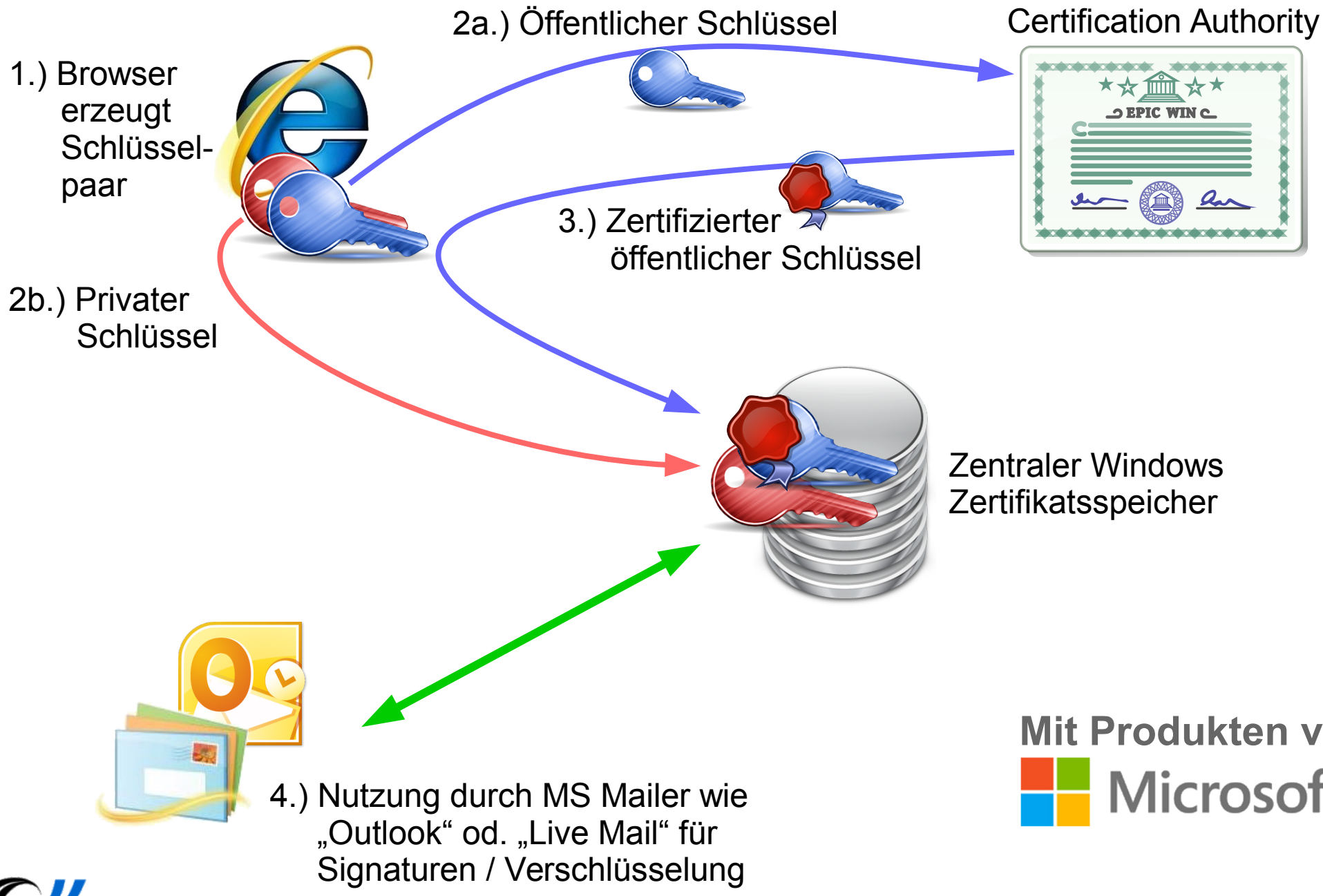
5.) Import aus P12-Datei

6.) Nutzung durch „Thunderbird“ für Signaturen / Verschlüsselung

Zertifikats-speicher Thunderbird

**Etwas komplizierter mit Produkten von mozilla**

# Zertifikate → Beantragung, Installation, Nutzung, ...




Mit Produkten von Microsoft

# Übung 2: CAcert-Registrierung und S/MIME-Tests

In dieser Übung:

→ wird Comodo als CA verwendet. Zertifikat mit Minimum an Daten erhältlich und es wird überall problemlos anerkannt

→ erstellen Sie ein eigenes Schlüsselpaar für S/MIME

→ integrieren Sie das in den Mail-Client

→ und Testen Sie unterschriebene bzw. verschlüsselte Mails

**Registrierung bei CAcert kann optional durchgeführt werden. Fragen Sie ggf. Ihre FortbildnerInnen ob er oder sie Ihre Identität bei CAcert bestätigen kann (Assurer).**

# Ausblick – im Rahmen der Tagung „med. Schule“

- Comodo od. StartSSL skaliert nicht auf Schulen
  - Lehrkräfte
  - Lernende
- CAcert als digitaler Notar skaliert
  - Stammzertifikat noch nicht in OS/Software
  - Datenschutzfragen, Verträge, Unterstützung, …
  - Traum
- Alternative: Landeseigene CA
  - Aufwand → Lehrkräfte ok … aber Schüler?
  - Kostenfrei im Internet?