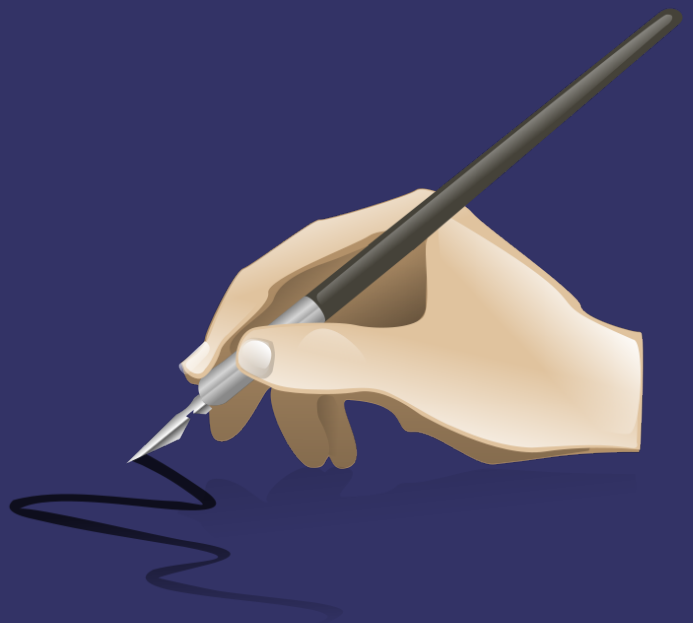
Verschlüsselung und Signatur mit SSL und S/MIME



Prinzip von „Public Key“ Verfahren

- Es gibt ein zueinander passendes **Schlüssel-PAAR**
- Der „**öffentliche** Schlüssel“ muss den Kommunikationspartnern bekannt sein
- Der „**geheime**“ Schlüssen befindet sich NUR im Besitze des Schlüsseleigentümers.
- Was man mit dem einen VERschlüsselt, kann man NUR mit dem ANDEREN Key wieder ENTschlüsseln.

Vorteil

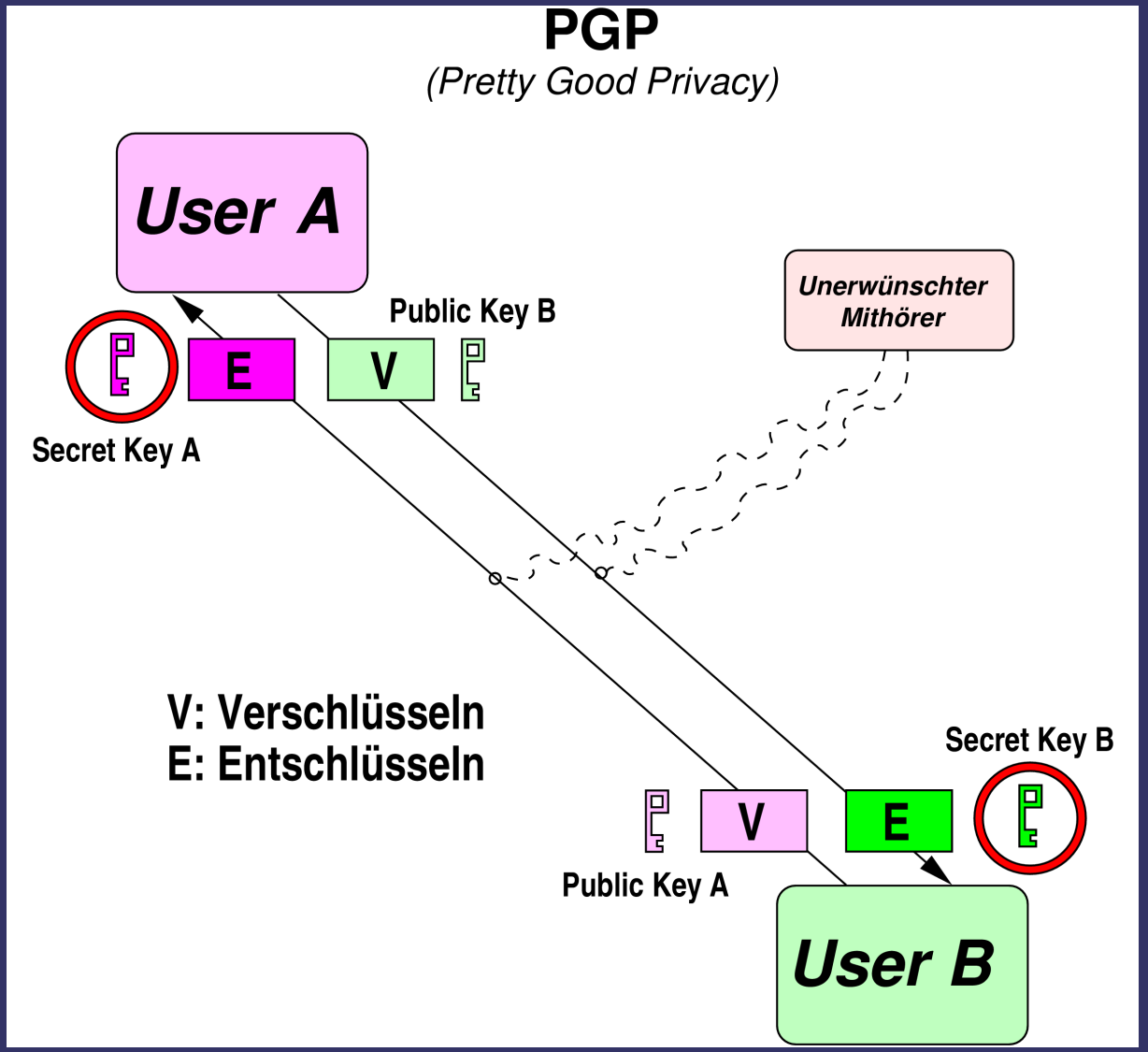
- Der öffentliche Schlüssel kann über ein „unsicheres“ Netzwerk übertragen werden, da die Verschlüsselung immer „one-way“ ist.
- Der geheime Schlüssel verlässt nie seinen Besitzer, und schützt dessen Identität.
- Das Verfahren ist mathematisch gut erfasst und gilt, bei ausreichender Schlüssellänge, als sehr sicher.

Nachteil

- Die Herkunft des **öffentlichen** Schlüssels muss überprüft werden, um sicherzustellen, dass man mit dem richtigen Besitzer des geheimen Schlüssels „spricht“. → Keyserver, Web-of-Trust (Signieren von öffentlichen Schlüsseln durch „vertrauenswürdige Organisationen“).

- Veröffentlicht der Besitzer seinen **geheimen** Schlüssel versehentlich, oder wird dieser „gestohlen“, ist es nicht einfach, alle Gesprächspartner zu informieren.

PGP und SSL
Verfahren (graphisch)



SSL-Variante im WWW: *https*

- Web-Server schickt den für seine **Adresse** ausgestellten **Public Key**,
- Browser fragt ggf. zurück, ob Aussteller „vertrauenswürdig“ ist, falls er diesen nicht „kennt“,
- Bei Bestätigung unterhalten sich Browser und Webserver verschlüsselt.

SSL-Fehler


Dies ist wahrscheinlich nicht die Website, nach der Sie suchen!
Beim Versuch, auf www.knopper.net zuzugreifen, haben Sie einen Server erreicht, der sich knopper.net nennt. Dies kann an einer fehlerhaften Konfiguration liegen, jedoch auch schwerwiegendere Ursachen haben. Möglicherweise versucht ein Hacker, Sie auf eine gefälschte und potenziell gefährliche Version von www.knopper.net zu locken.
Fahren Sie nicht fort, insbesondere wenn diese Warnung für diese Website vorher noch nie erschienen ist.
Trotzdem fortfahren
Zurück zu sicherer Website
Mehr Infos dazu

SSL Zertifikat

Erzeugen eines Schlüsselpaars mit „selbstsigniertem“ Zertifikat

```
openssl req -new -x509 -nodes
        -days 3650
        -keyout geheim.pem
        -out public.pem
```

Erzeugt geheimen Schlüssel in `geheim.pem`, und signierten öffentlichen Schlüssel in `public.pem`.

Während des Erzeugens werden die „persönlichen“ Informationen abgefragt.

Der „Common Name“ bezeichnet die Webseite bzw. den Namen mit Mailadresse.

Verpacken für Firefox oder Thunderbird

```
openssl pkcs12 -export
        -out datei.p12
        -inkey geheim.pem
        -in public.pem
        -name "Mein Name"
```

Die datei.p12 enthält nun geheimen und öffentlichen Schlüssel zum Import in Thunderbird oder anderen SSL-fähigen Mailprogrammen.

Bzw. Webmail

- Heute sind „echte“ Mailprogramme vielleicht schon „aus der Mode“ gekommen, daher sei hier darauf verwiesen, dass Web-basierte E-Mail ebenfalls mit SSL (https) funktioniert. Nur das Signieren wird oft nicht unterstützt.

- Wichtig: Bei SSL-Meldungen überprüfen, ob das richtige Zertifikat (=signierter öffentlicher Schlüssel) angezeigt wird.

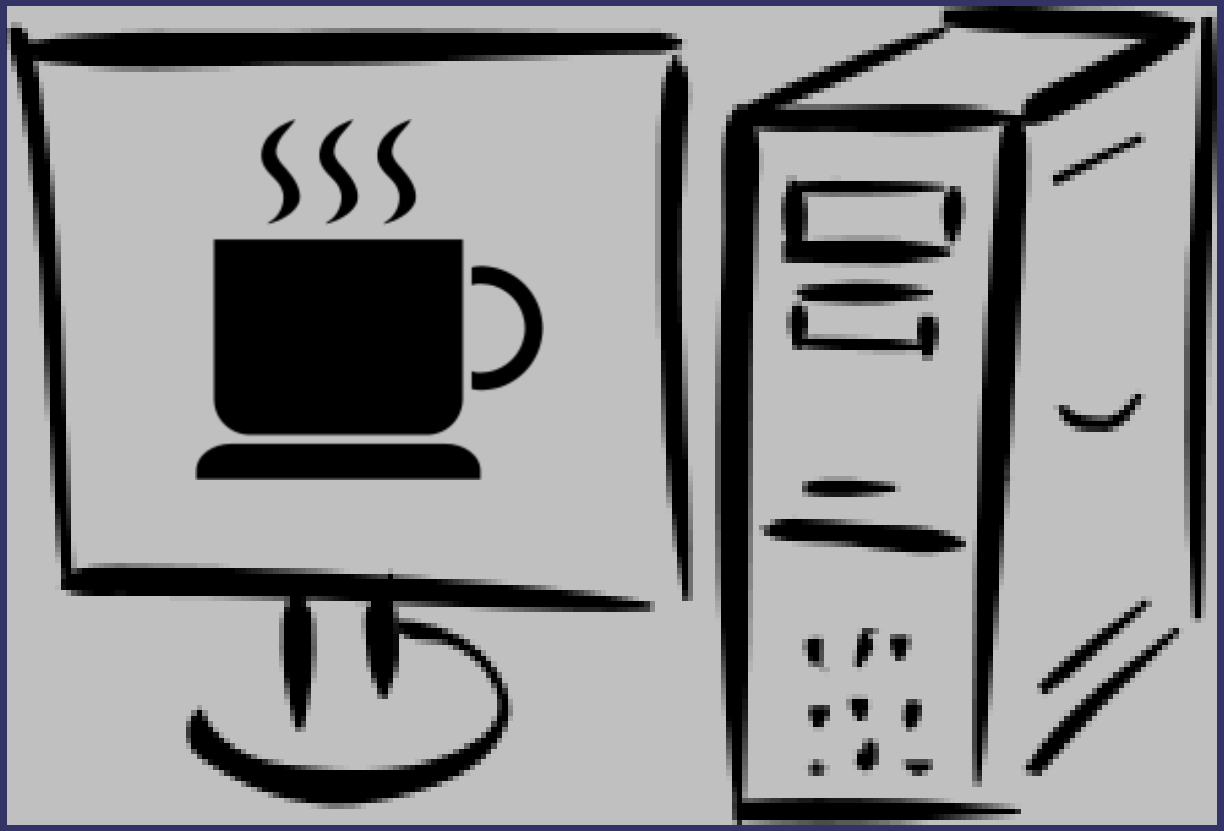
Problem: Unverschlüsselte Dienste

- Bei Kommunikations-Programmen wie ICQ und Skype wird keine Standard-Verschlüsselung verwendet.
- Wenn keine Verschlüsselung möglich ist: Wenigstens anderes Login/Passwortpaar verwenden!

SSH-Authentifizierung mit Public Keys

- ssh-keygen -t rsa
  → Erzeugt neues Schlüsselpaar
- .ssh/id_rsa.pub auf Zielrechner in .ssh/authorized_keys anhängen
- Ab sofort ist ssh Zielrechner ohne Passworteingabe möglich (sofern nicht lokal für den SSH-Schlüssel ein Passwort gesetzt wurde).

Fragen?



security@knopper.net