

Keep yourself, your family, friends, workplace
& community safe from
unwarranted spying.

#cryptoparty

Throw a party and learn how to
install and use Tor, VPN's, TrueCrypt, OTR, GPG

#cryptoparty

Teil 1:

Warum und was

verschlüsseln?

1.1 Warum verschlüsseln?



Creative Commons Attribution 3.0 Unported
by: McZusatz (Wikipedia)

Friedrich ruft zum Verschlüsseln auf

Die Innenpolitiker der CSU sagen, dass die Bürger beim Datenschutz nicht auf den Nationalstaat hoffen dürfen. Sie sollen ihre Daten selber schützen.



Kommt etwas ins Schwimmen: Bundesinnenminister Friedrich.

Bild: dpa

BERLIN *taz* | Als Konsequenz aus der Spähaffäre hat Bundesinnenminister Hans-Peter Friedrich (CSU) die Bürger zum Verschlüsseln ihrer Onlinekommunikation aufgerufen. „Wir werden dafür sorgen, dass noch mehr Menschen in Deutschland ihre eigene Kommunikation noch sicherer machen“, sagte Friedrich nach einer Sondersitzung des Parlamentarischen Kontrollgremiums zur Überwachung der Geheimdienste (PKGr). Als Mittel nannte er Verschlüsselungstechnik und Virenabwehrprogramme.

SCHWERPUNKT



Im Schwerpunkt legen wir ein Auge auf die Auswüchse der

Politik / Deutschland



ASTRID
Korrespondent
Parlament



THEMEN

Schwerpunkt Über
Hans-Peter Friedrich
Datenschutz, Har

<http://www.taz.de/!120071/>

EU-Parlament entwickelt Paket für „PGP-artige“ Software und verweist in der Zwischenzeit auf Office, 7zip und PDF

von Anna Biselli am 27. April 2015, 12:33 in EU / 15 Kommentare

Letzte Woche habe wir darüber berichtet,
dass im Europaparlament seit Beginn der



DG ITEC Generaldirektion Innovation und technologische Unterstützung

DG ITEC rät, sich mit der „internen Verschlüsselung“ von Office, 7zip und PDF in der
Zwischenzeit Abhilfe zu verschaffen. Dafür müsse man jedoch ein Passwort
austauschen – mündlich. Wir können uns leider bereits vorstellen, wie das über
ungesicherte Telefonleitungen passiert.

EU-Kommission hat weiterhin „Bedenken“ zu Verschlüsselung und plant Gespräche mit Internetdienstleistern

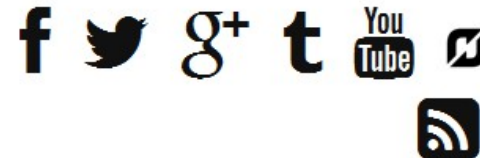
von [Matthias Monroy](#) am 29. April 2015, 14:00 in [Überwachung](#) / 14 Kommentare

Die EU-Kommission findet die Nutzung von Verschlüsselungswerkzeugen weiterhin

problematisch. Dies geht aus der gestern veröffentlichten „[Europäischen Sicherheitsagenda](#)“ hervor. Demnach hätten Strafverfolgungsbehörden „Bedenken in Bezug auf die neuen Verschlüsselungstechniken“. Damit knüpft die Kommission an Statements des EU-Anti-Terror-Koordinators Gilles de Kerchove an. Der hatte [im Januar in einer Wunschliste gefordert](#), Internet- und Telekommunikationsanbieter zum Einbau von



Sieht in
Verschlüsselungstechniken
das größte



Newsletter

Stellenanzeigen

Praktikum beim Digitale Gesellschaft e.V.

Praktikum bei netzpolitik.org

Anzeige

Hackerangriff auf den Bundestag: **Das entblößte Parlament**

Von *Annett Meiritz* und *Fabian Reinbold*



DPA

Reichstagsgebäude in Berlin: "Das ist kein normaler Zustand"

Wie dramatisch ist der Spähangriff auf den Bundestag? Die Abgeordneten fühlen sich alleingelassen, die Arbeit im Parlament leidet. Noch heute soll eine Entscheidung über das weitere Vorgehen fallen.

<http://www.spiegel.de/politik/deutschland/deutscher-bundestag-nach-hacker-angriff-das-entbloesste-parlament-a-1038290.html>

Facebook kommuniziert PGP-verschlüsselt mit seinen Mitgliedern

vorlesen / MP3-Download



(Bild: dpa, Peter Dasilva)

Facebook ermöglicht seinen Nutzern, ihren öffentlichen PGP-Key zu hinterlegen und Status-Mails damit verschlüsseln zu lassen.

<http://www.heise.de/security/meldung/De-Mail-Ende-zu-Ende-Verschlueselung-mit-PGP-gestartet-2616388.html>

22.04.2015 12:13

« Vorige | Nächste »

De-Mail : Ende-zu-Ende-Verschlüsselung mit PGP gestartet

vorlesen / MP3-Download



(Bild: dpa, Jochen Lübke)

De-Mail-Kunden können nun ihre Nachrichten und Anhänge im Web-Frontend des Diensts lokal mit PGP verschlüsseln und danach versenden.

Die Anbieter von De-Mail haben heute die angekündigte [Option für Ende-zu-Ende-Verschlüsselung mit PGP](#) freigeschaltet. Damit können nun De-Mail-Kunden der

<http://www.heise.de/security/meldung/De-Mail-Ende-zu-Ende-Verschlueselung-mit-PGP-gestartet-2616388.html>

1.2 Was verschlüsseln?

- Festplatte **TrueCrypt** Version 7.1a (2012)
- E-Mails **Enigmail** Thunderbird-Addon
Gpg4Win Schlüsselmanagement
Mailvelope Browserplugin
- Anonym Surfen **Tor Project**
Tails Linux-Distribution

aber: keine absolute Sicherheit möglich

1.3 Ein Modell für die Zukunft?

- sicher?
- bedienerfreundlich?

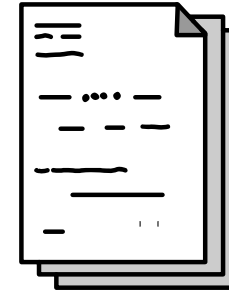
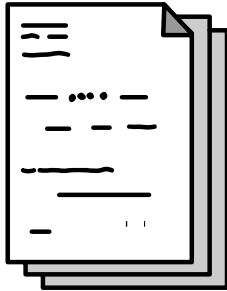
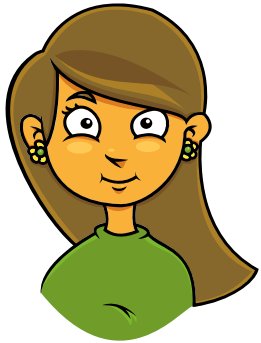
Teil 2:

Das Prinzip

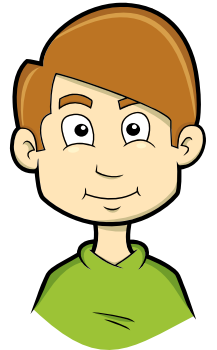
2.1 Symmetrische Verschlüsselung

Symmetrische Verschlüsselung

Alice

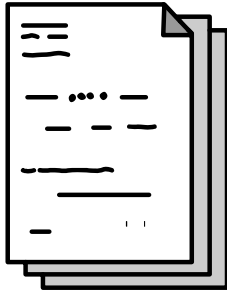
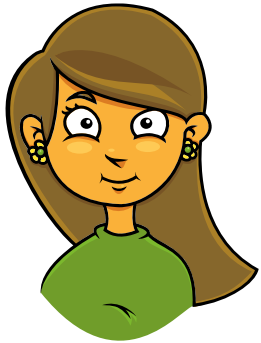


Bob

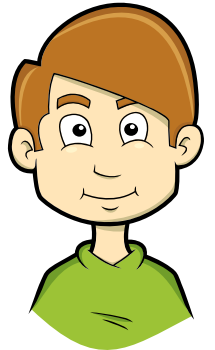


Symmetrische Verschlüsselung

Alice

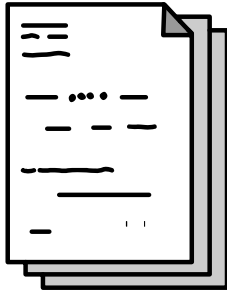
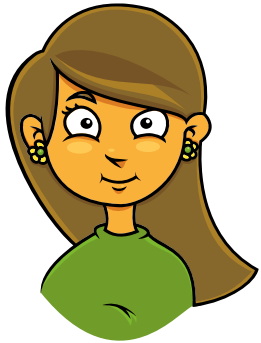


Bob



Symmetrische Verschlüsselung

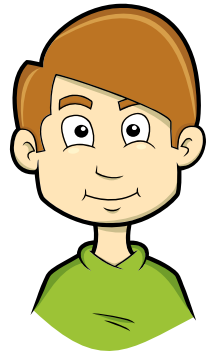
Alice



Verschlüsselung mit
Schlüssel XYZ

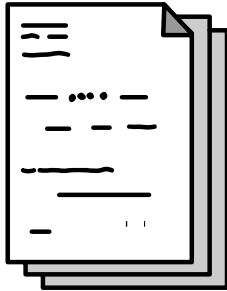
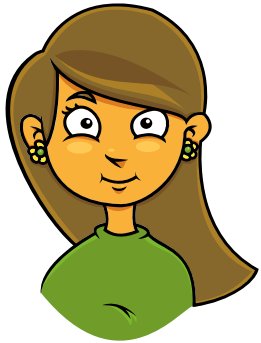


Bob

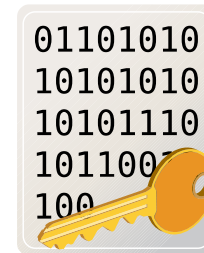


Symmetrische Verschlüsselung

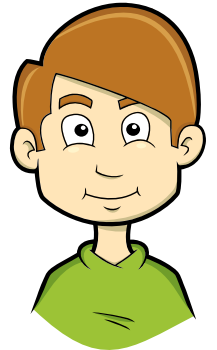
Alice



Verschlüsselung mit
Schlüssel XYZ

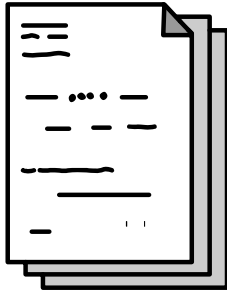
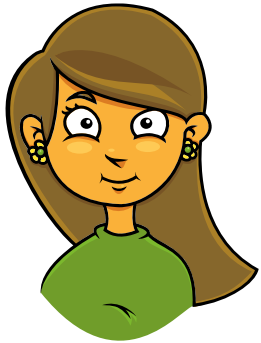


Bob

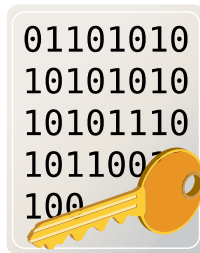


Symmetrische Verschlüsselung

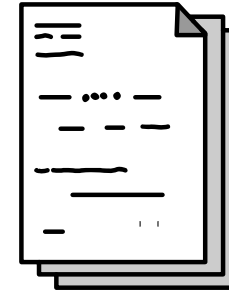
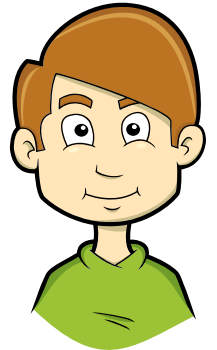
Alice



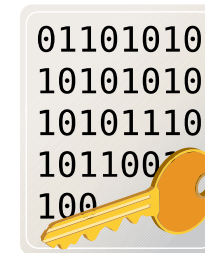
Verschlüsselung mit
Schlüssel XYZ



Bob



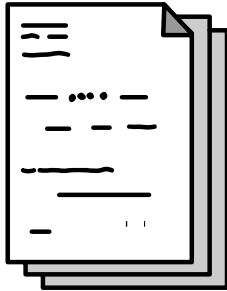
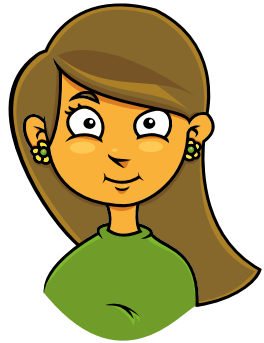
Entschlüsselung mit
Schlüssel XYZ



Problem

Symmetrische Verschlüsselung

Alice



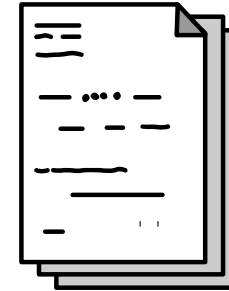
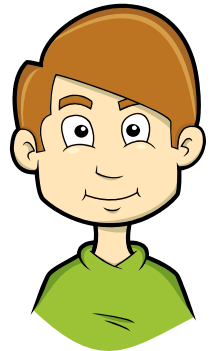
Verschlüsselung mit
Schlüssel XYZ



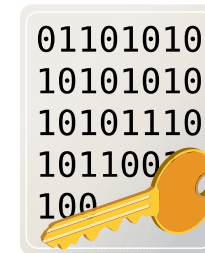
Übermittlung des gemeinsamen
Schlüssels XYZ



Bob



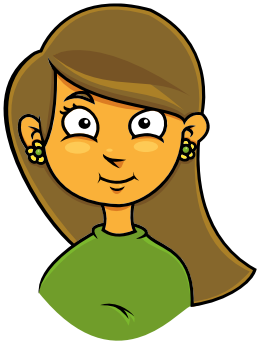
Entschlüsselung mit
Schlüssel XYZ



2.2 Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselung

Alice



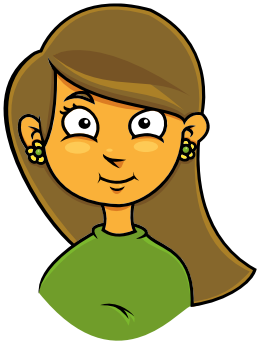
private key (Alice)

Öffentlich

public key (Alice)

Asymmetrische Verschlüsselung

Alice



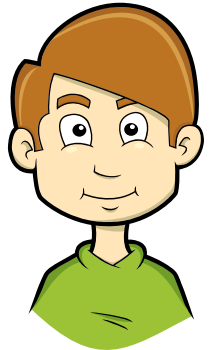
private key (Alice)

Öffentlich

public key (Alice)

public key (Bob)

Bob



private key (Bob)

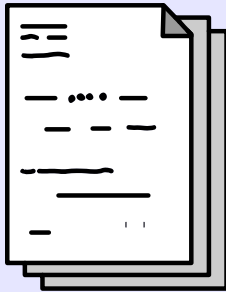
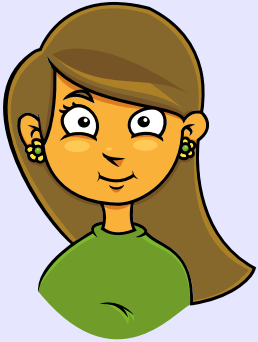
Alice an Bob: Verschlüsseln

Privat

Öffentlich

Privat

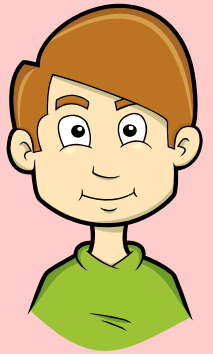
Alice



public key (Alice)

public key (Bob)

Bob



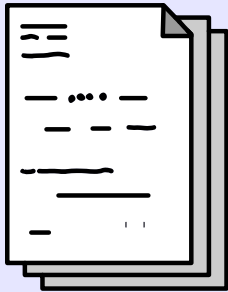
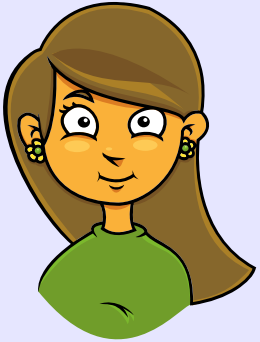
Alice an Bob: Versenden

Privat

Öffentlich

Privat

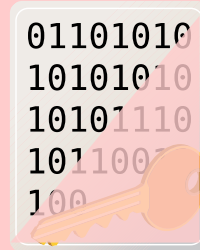
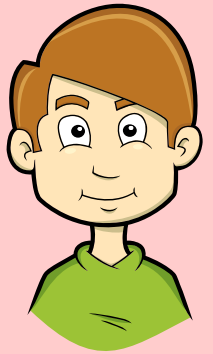
Alice



public key (Alice)

public key (Bob)

Bob



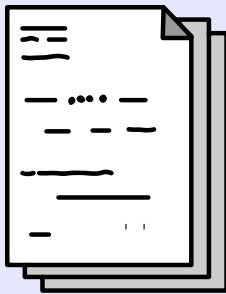
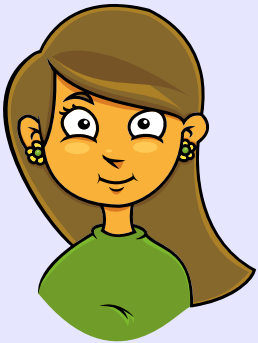
Alice an Bob: Entschlüsseln

Privat

Öffentlich

Privat

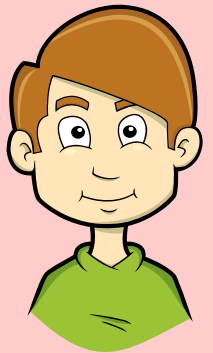
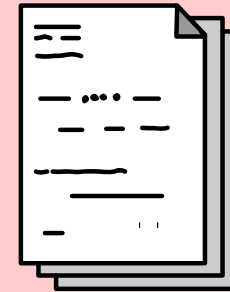
Alice



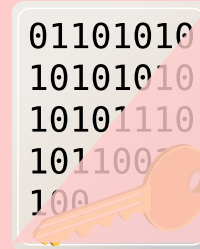
public key (Alice)

public key (Bob)

Bob



private key (Bob)



Bob an Alice

Privat

Öffentlich

Privat

Alice

Bob

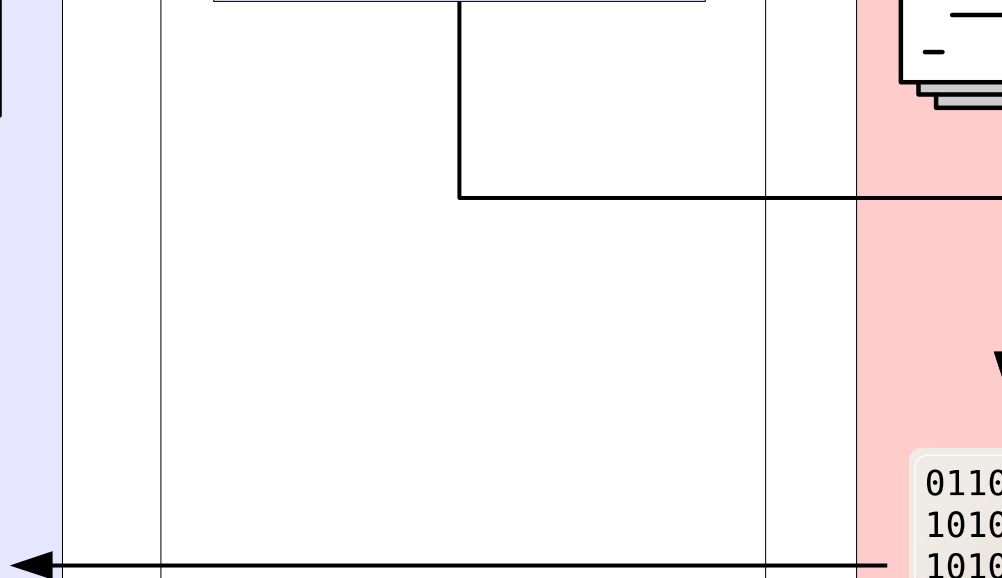
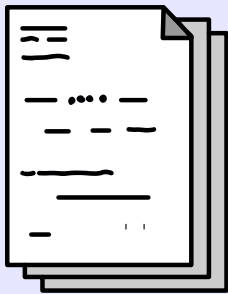
private key (Alice)

public key (Bob)

public key (Alice)

01101010
10101010
10101110
10110010
100

01101010
10101010
10101110
10110010
100



Asymmetrische Verschlüsselung

- 2 Schlüssel (1 Paar) pro Nutzer, einer davon geheim
- Jeder kann Nachricht an Bob **verschlüsseln**
- Nur Bob kann Nachricht an Bob **entschlüsseln**
- Es gibt keinen Austausch geheimer Schlüssel
- Privater Schlüssel muss geheim bleiben,
also: nur auf dem eigenen Rechner sein

Teil 3:

In der Praxis

3.1 Manuell mit JavaScript

3.2 Browser-Plugin Mailvelope

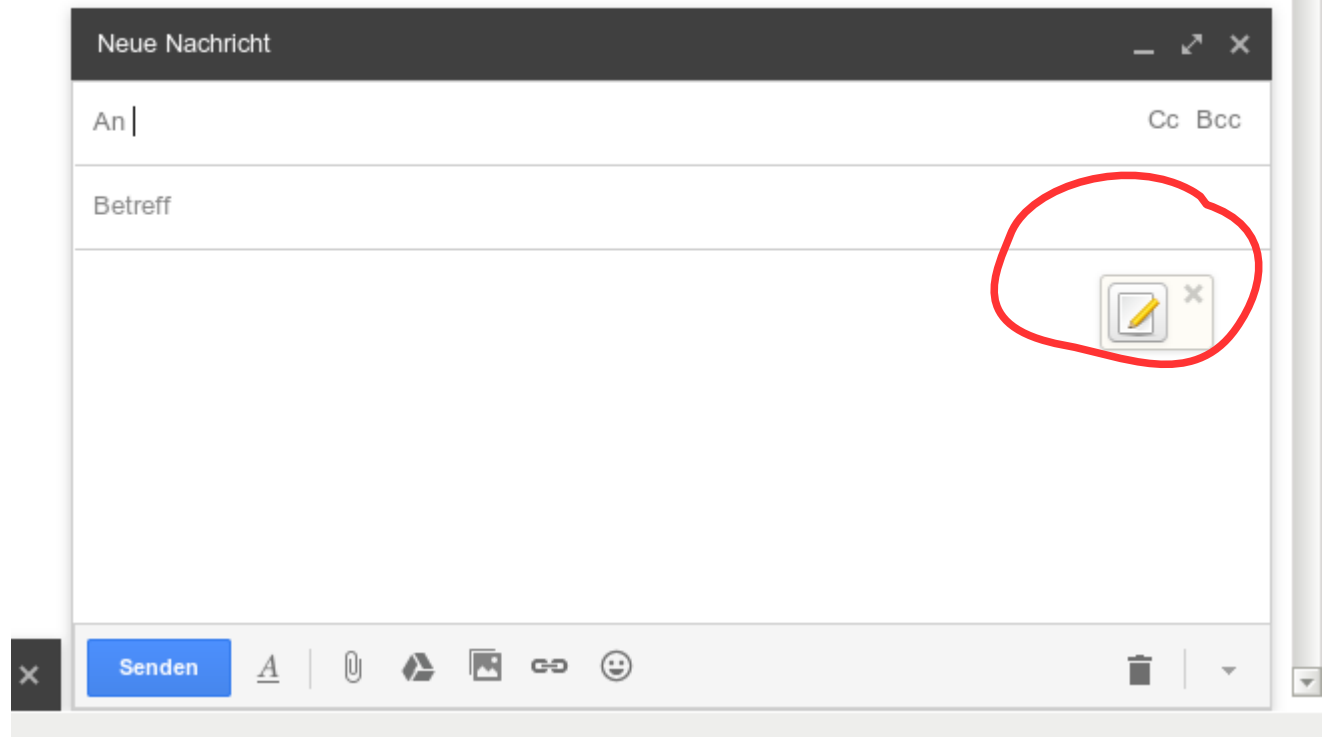
- Firefox/Chrome
- voreingestellt für die meisten Webmail-Anbieter, weitere hinzufügbare
- ermöglicht Schlüsselverwaltung und -erzeugung
- ersetzt/ergänzt Textfeld



1. Nach der Installation...

2. ...Schlüssel importieren oder erzeugen...

3. ...dann erscheint Ergänzung zur bisherigen Eingabe.
(als reinen Text verschicken, nicht als HTML)



3.3 Thunderbird-Add-on Enigmail



Schreiben,
Verschlüsseln,
Entschlüsseln,
Aufbewahren von E-Mail

benutzt



Add-on
Enigmail

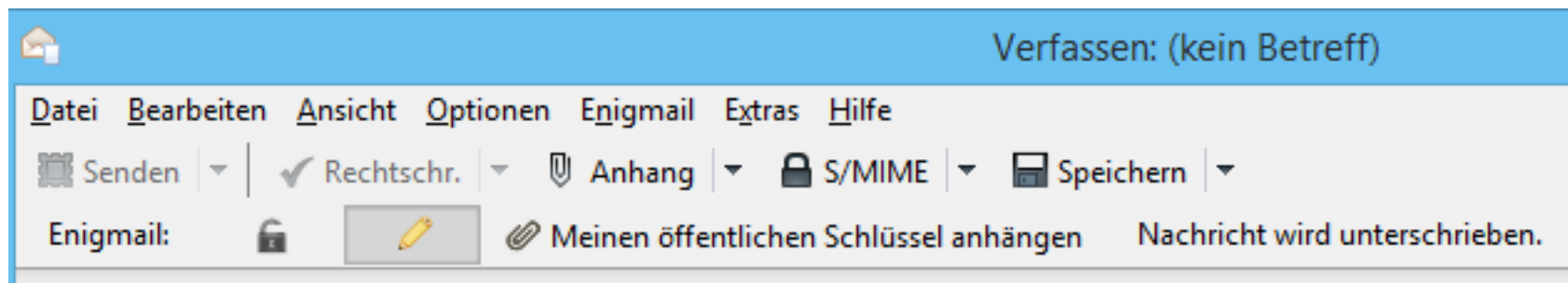
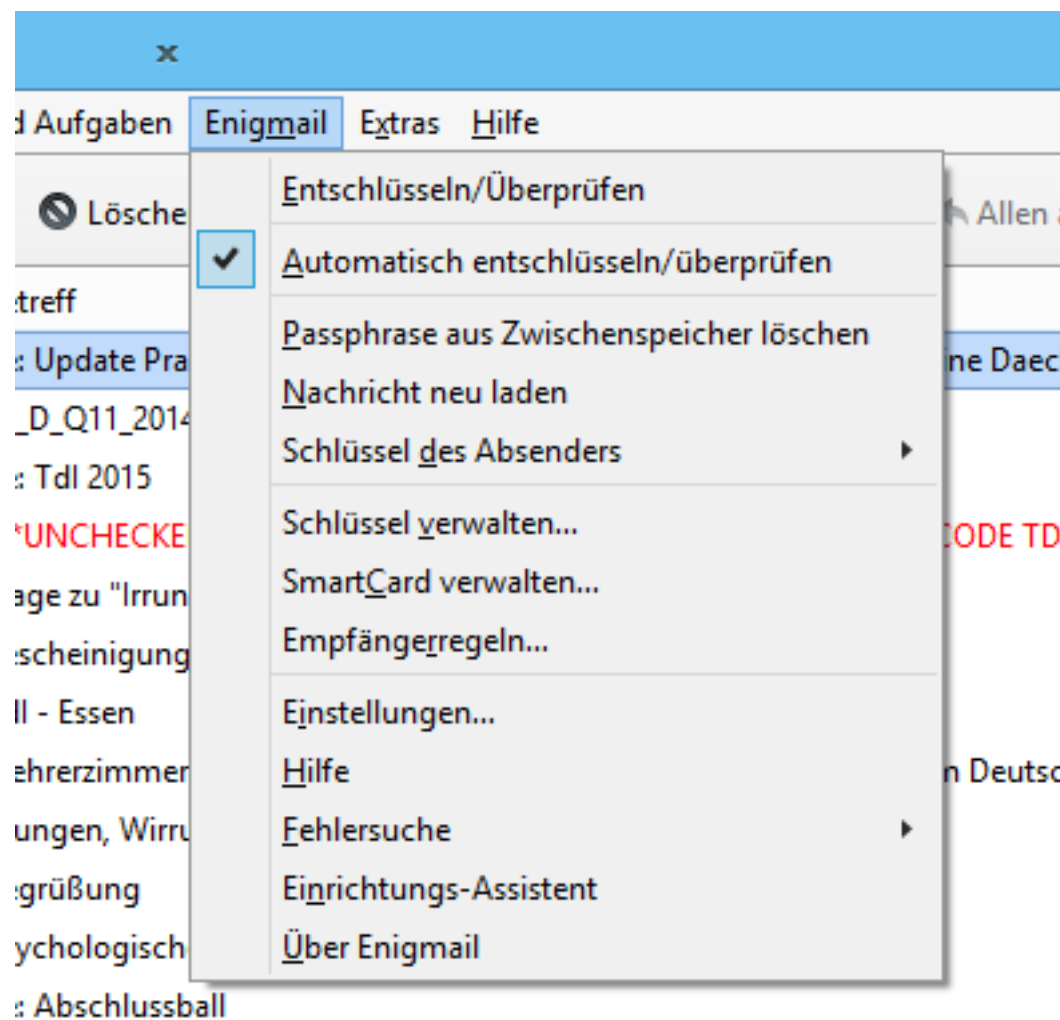


Tatsächliches
Ver-/Entschlüsseln
Verwaltung von Schlüsseln
Erzeugung von Schlüsseln

(unter Linux: GnuPG meist
bereits ohnehin installiert)

3.3 Thunderbird-Add-on Enigmail

- GPG installieren
unter Windows: Gpg4win (evtl. portable):
<http://www.gpg4win.de/>
- Thunderbird installieren:
<https://www.mozilla.org/de/thunderbird/>
- Enigmail installieren
<https://addons.mozilla.org/de/thunderbird/addon/enigmail/>



3.4 Unter Android

- Verwaltung der Schlüssel:
App: APG
- Mailprogramm, das damit arbeitet:
App: K-9 Mail

3.5 Speicherort der Schlüssel

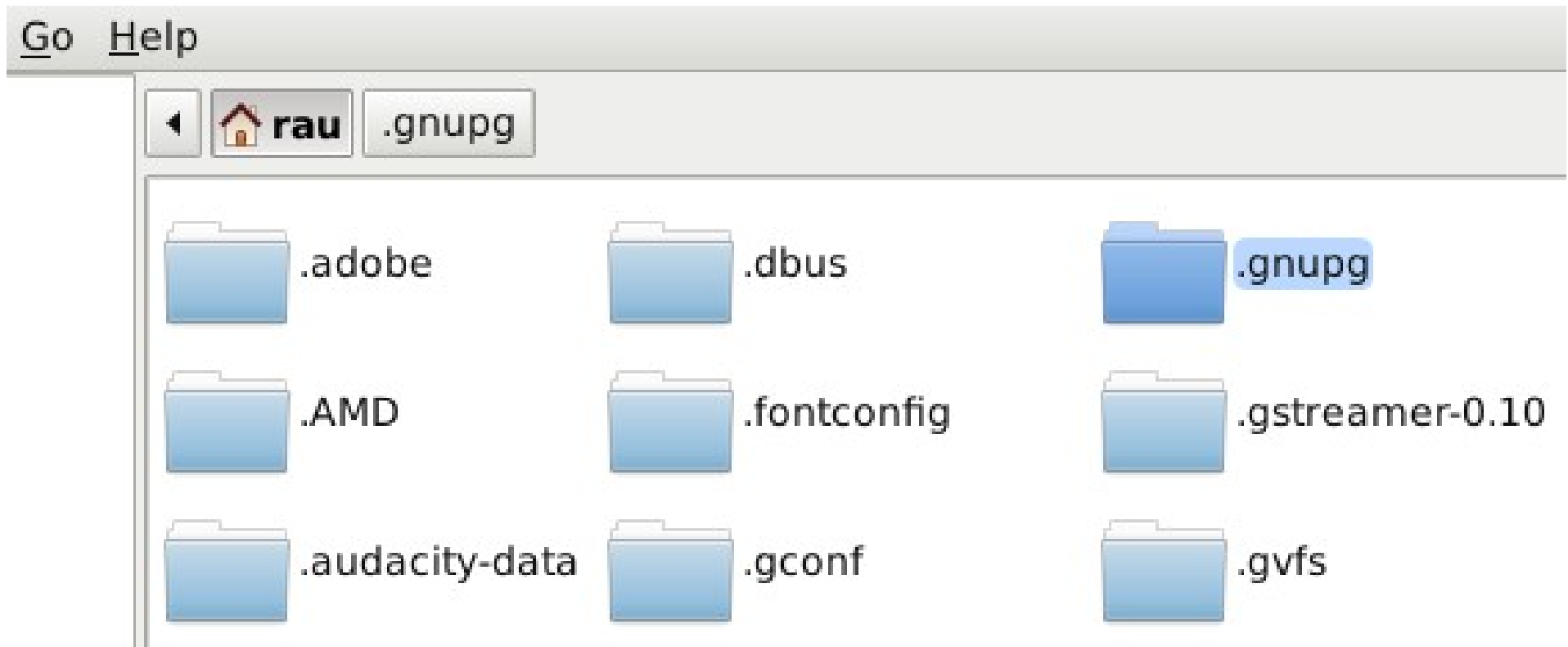
- Gpg4win:

C:\Users\%USERNAME\
%\AppData\Roaming\gnupg\

(AppData: versteckter Ordner;
Speicherort kann geändert werden)

3.5 Speicherort der Schlüssel

- GnuPG unter Linux
(versteckte Ordner mit Strg+H sichtbar machen)



3.5 Speicherort der Schlüssel

- **Mailvelope Firefox (Linux):**
.`mozilla/firefox/[profil]/jetpack/jid1-AqqSMBYb0a8ADg@jetpack/`
- **Mailvelope Firefox (Windows):**
`Profile\jetpack\jid1-AQqSMBYb0a8ADg@jetpack\`
- **Mailvelope Chrome (Windows):**
`C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default\Local Storage\chrome-extension_kajibbejlbohfggdiogboambcijhke_0.localstorage` (kann man z.B. mit SQLite Browser öffnen)

Teil 4:

Hintergrund

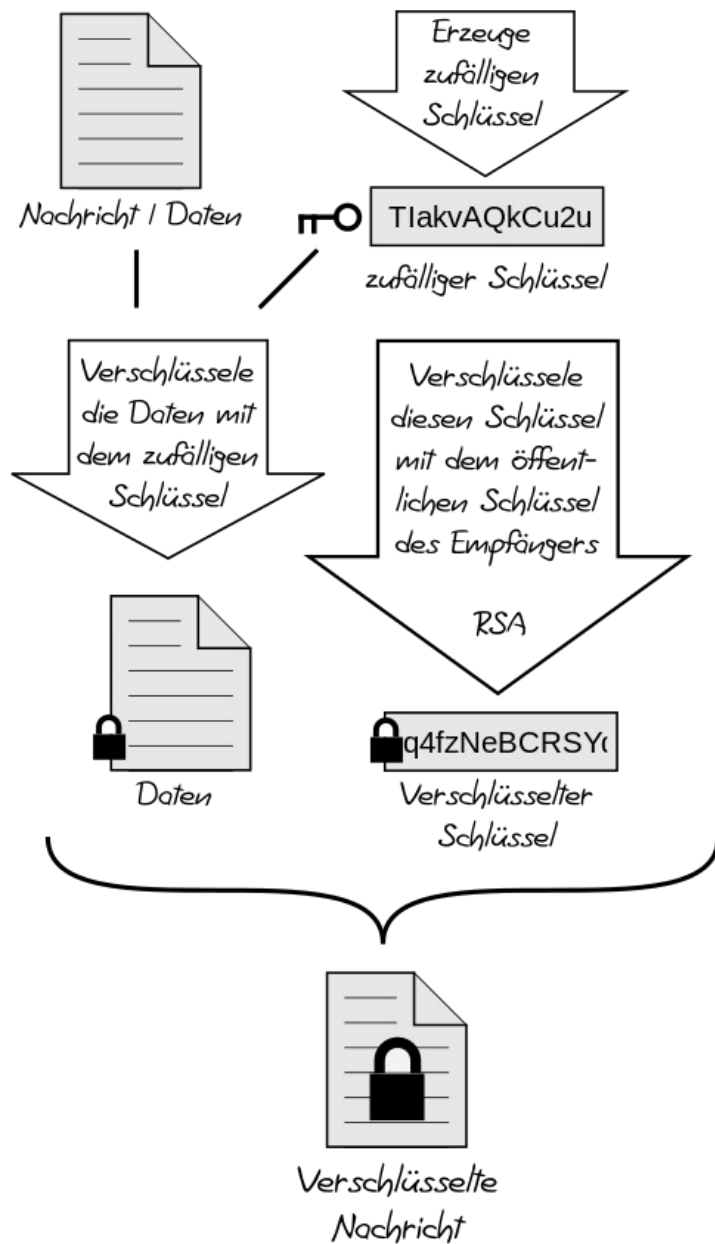
4.1 PGP

- **Pretty Good Privacy**
seit 1991 entwickelt, zur Verschlüsselung von Mails, proprietär
- **OpenPGP**
standardisiertes Datenformat ([RFC 4880](#)), basierend auf PGP
- **GPG (GNU Privacy Guard)**
Implementierung des OpenPGP-Standards, als offene Alternative zu PGP

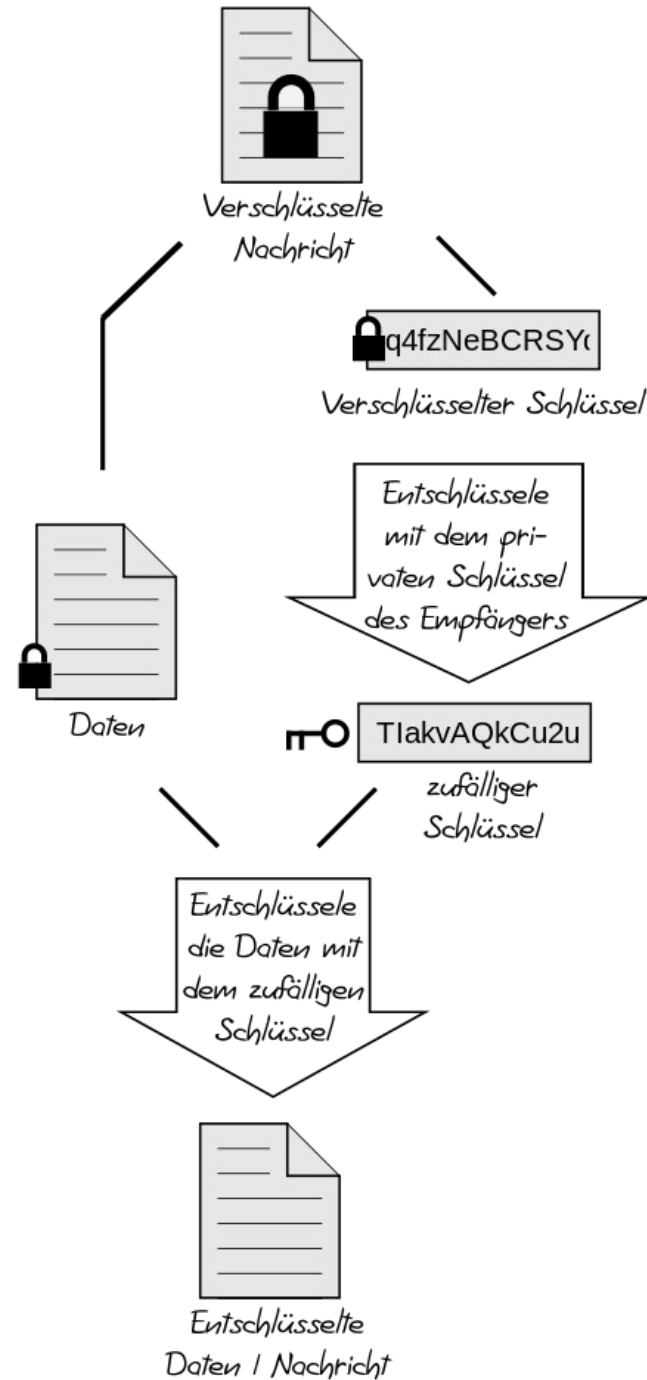
4.1 PGP

1. *Symmetrische* Verschlüsselung mit einem zufällig generierten Schlüssel (session key)
2. Verschlüsselung des Klartexts damit (z.B. AES-Algorithmus)
3. Asymmetrische Verschlüsselung des *session key* mit dem public key des Empfängers (z.B. RSA-Algorithmus)
4. Übermittlung des verschlüsselten session key zusammen mit dem verschlüsselten Klartext

Verschlüsselung



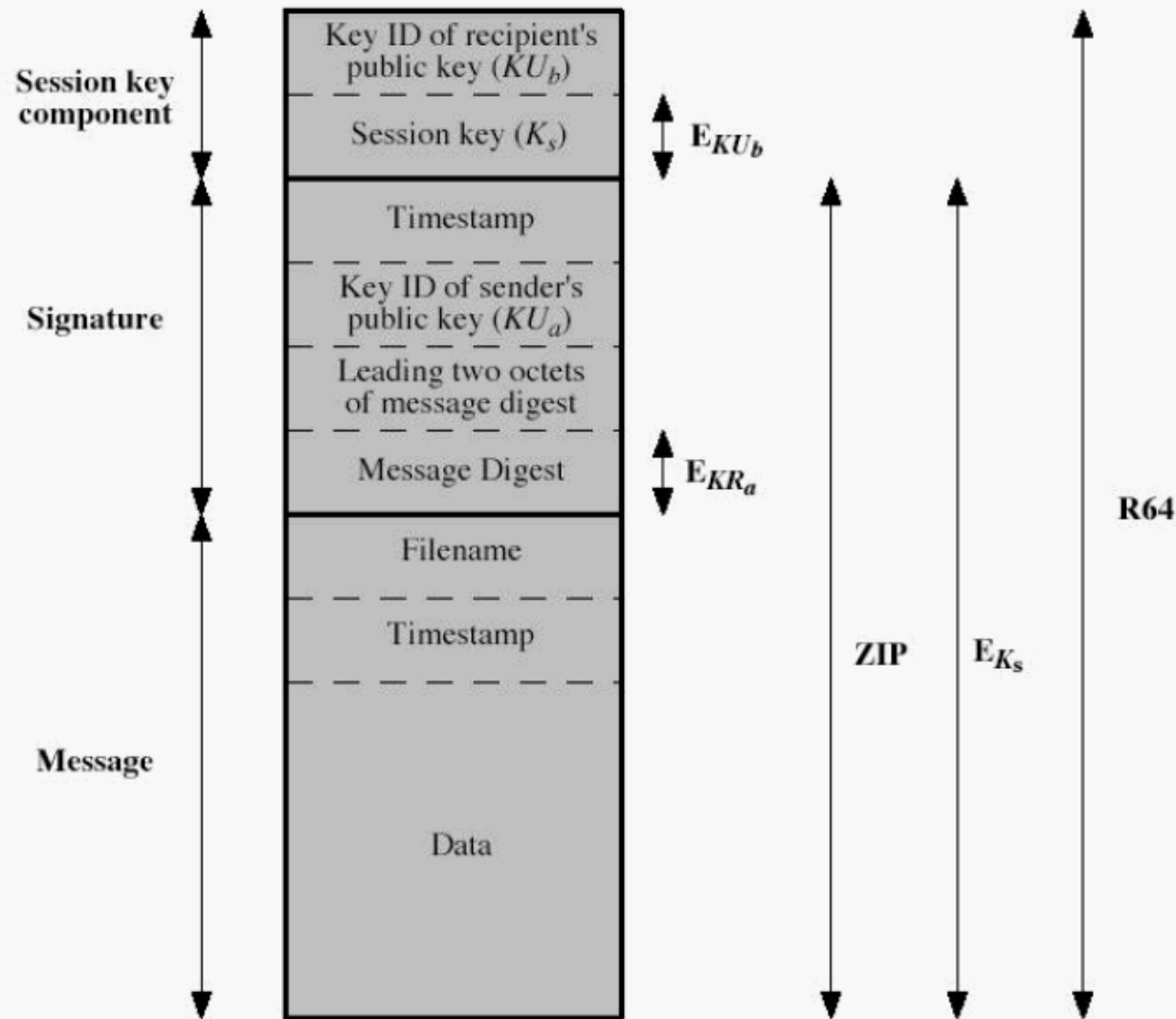
Entschlüsselung



Verschlüsselung mit Signierung: Details

Content

Operation



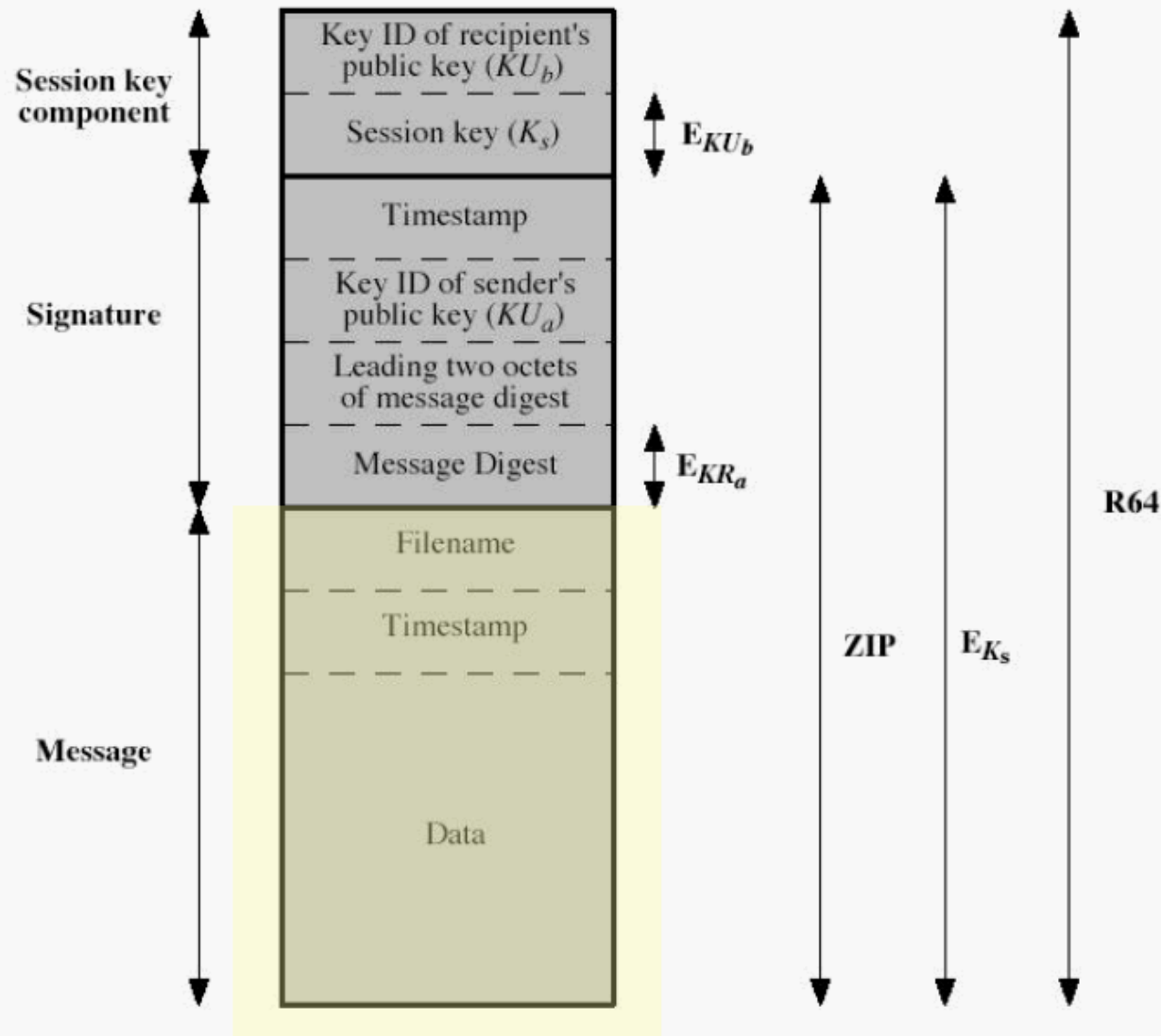
Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

Content

Operation

- Nachrichteninhalt +

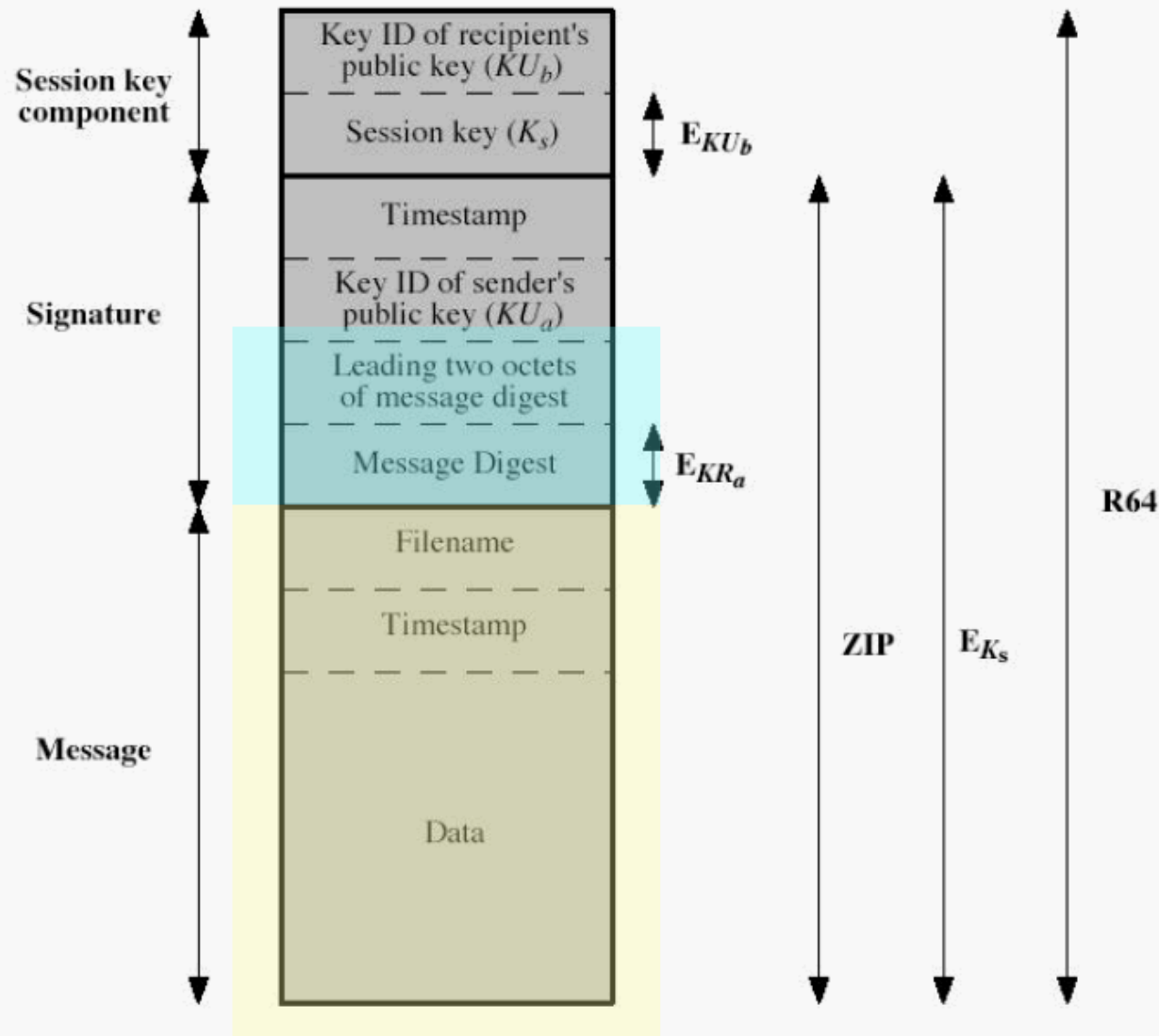


Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

Content

Operation



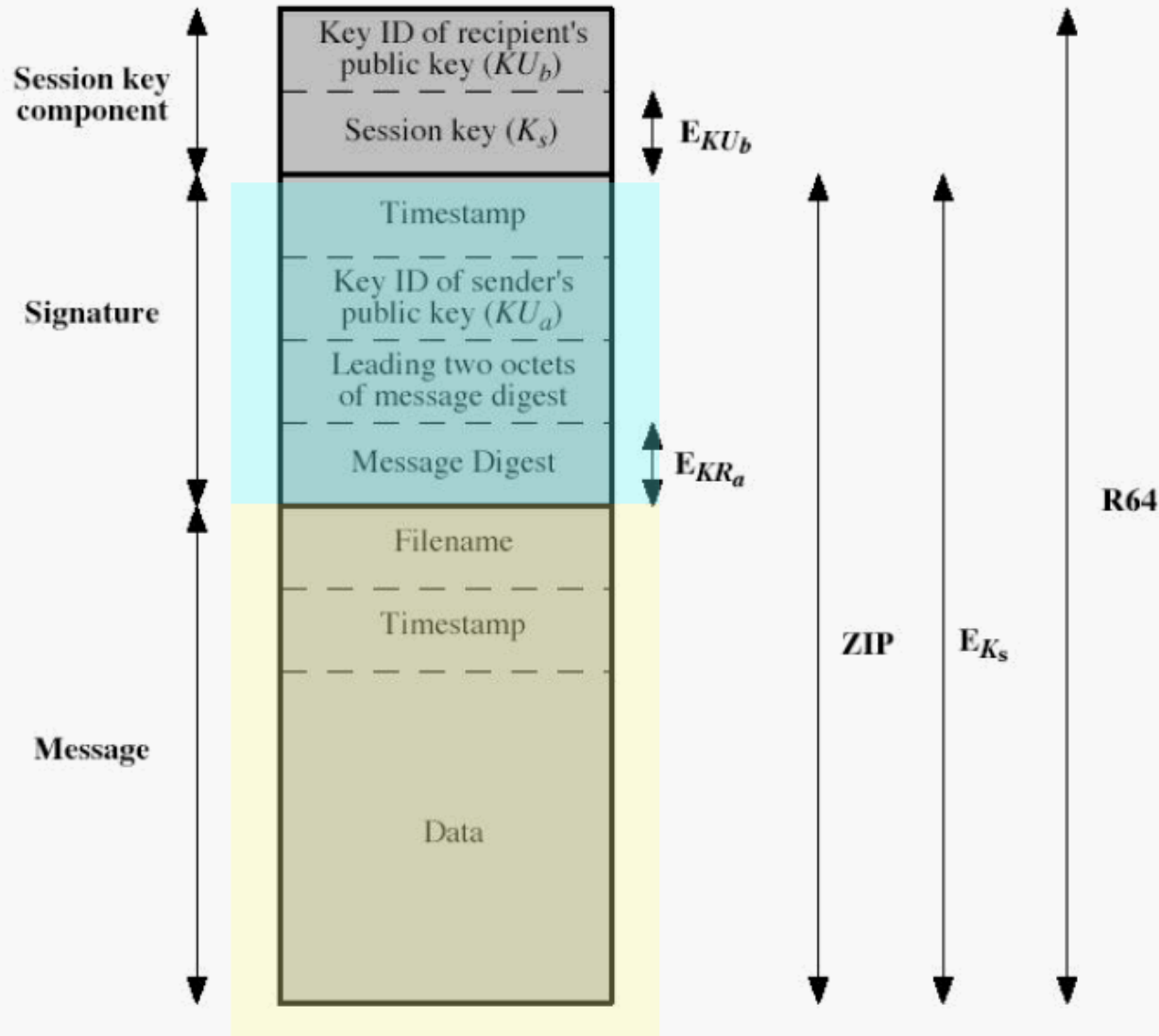
- Nachrichteninhalt +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders +

Notation:

E_{KU_b} = encryption with user b's public key
 E_{KR_a} = encryption with user a's private key
 E_{K_s} = encryption with session key
 ZIP = Zip compression function
 $R64$ = Radix-64 conversion function

Content

Operation



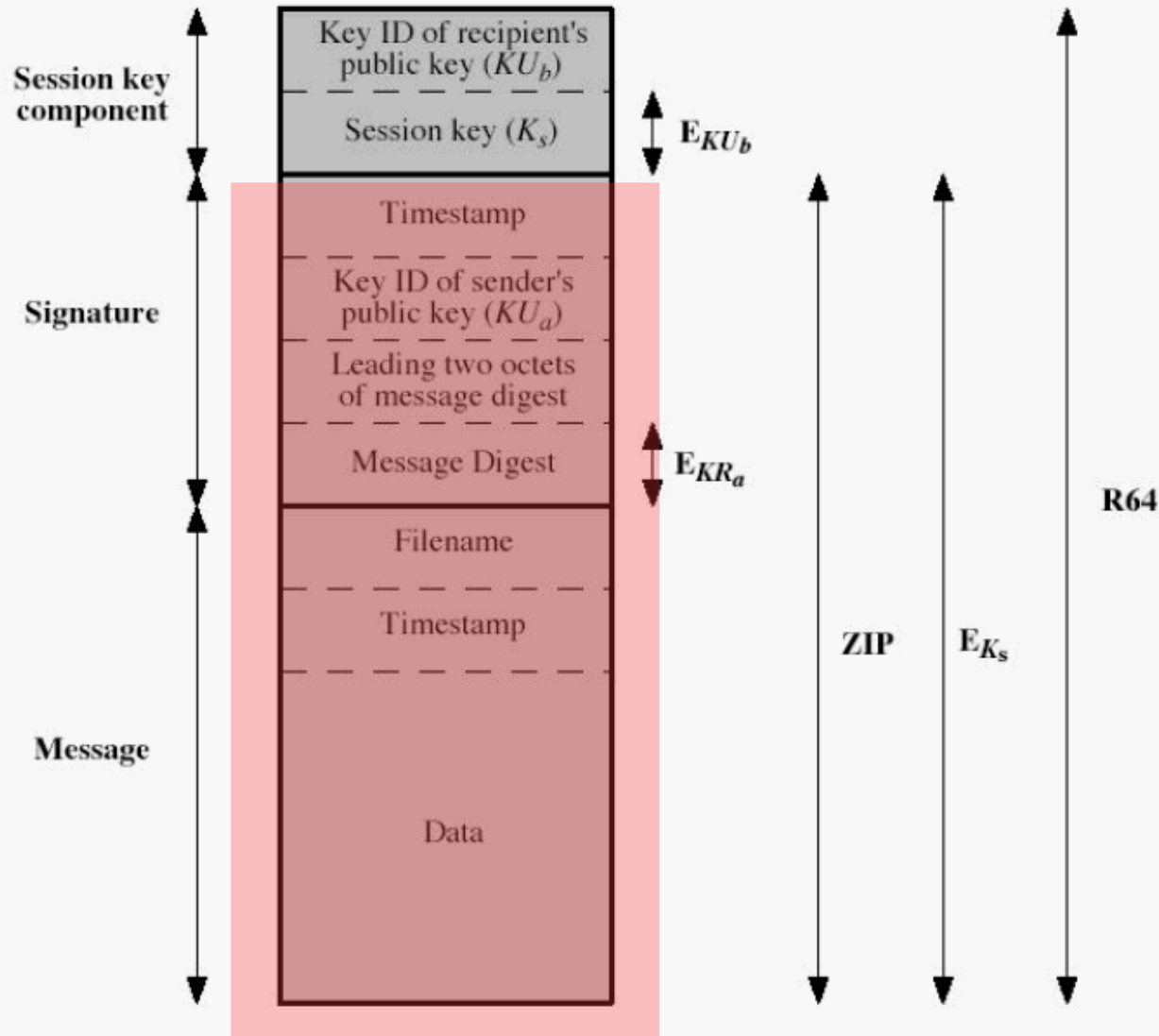
- Nachrichteninhalte +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des öffentlichen Sender-Schlüssels

Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- $R64$ = Radix-64 conversion function

Content

Operation



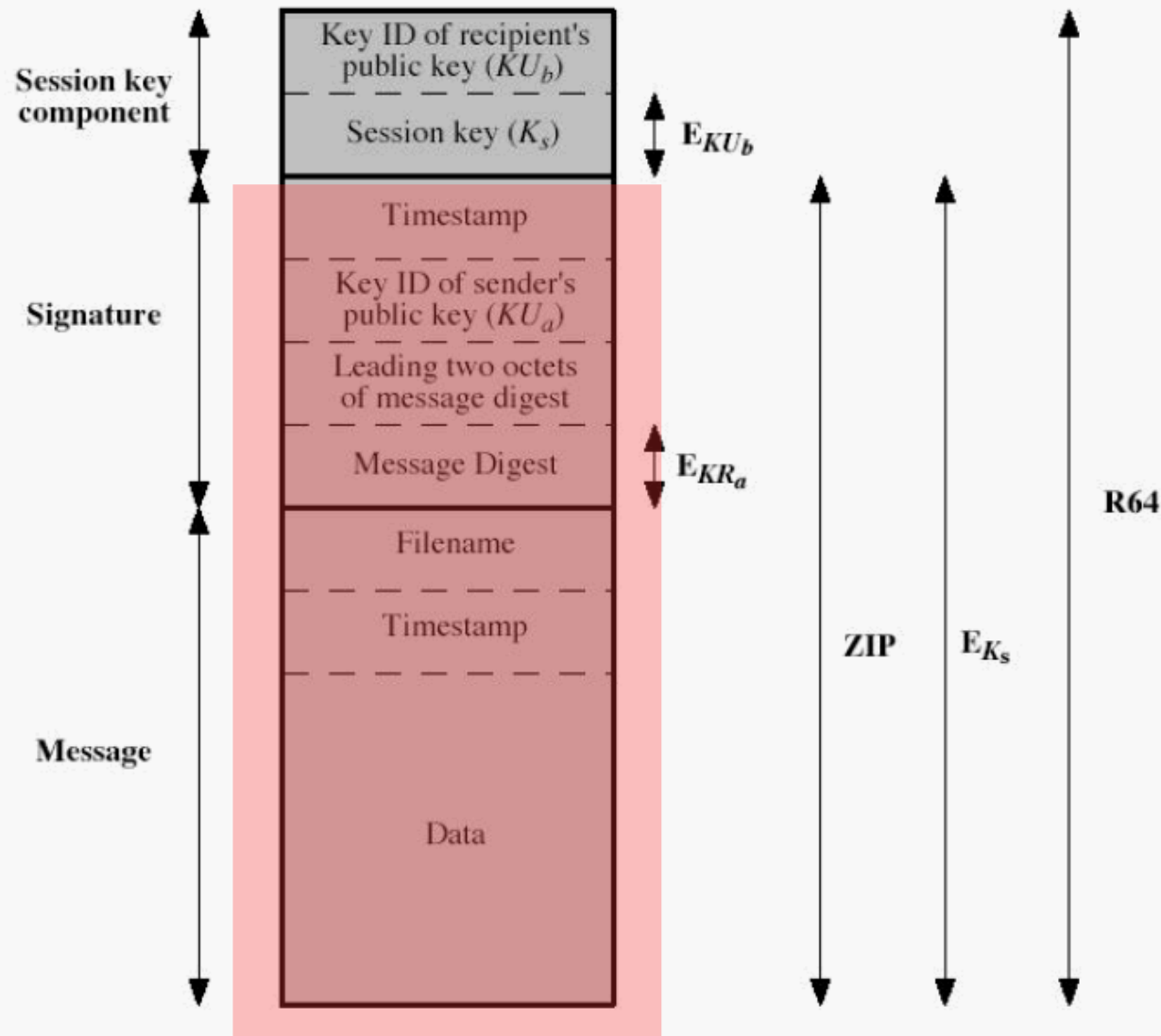
- Nachrichteninhalte +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des öffentlichen Sender-Schlüssels
- das alles gepackt

Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

Content

Operation



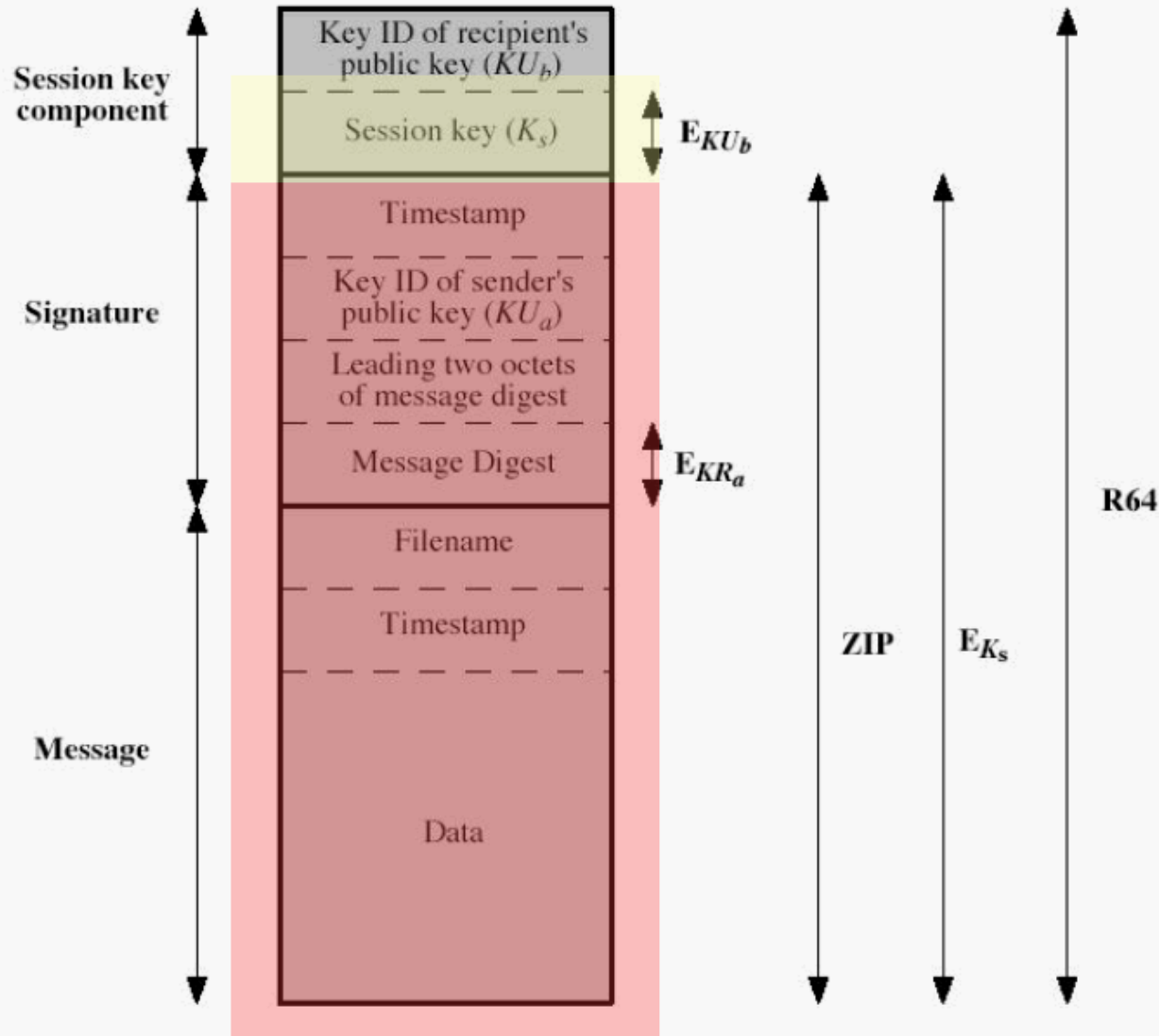
- Nachrichteninhalte +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des öffentlichen Sender-Schlüssels
- das alles gepackt und mit dem session key **verschlüsselt**

Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

Content

Operation



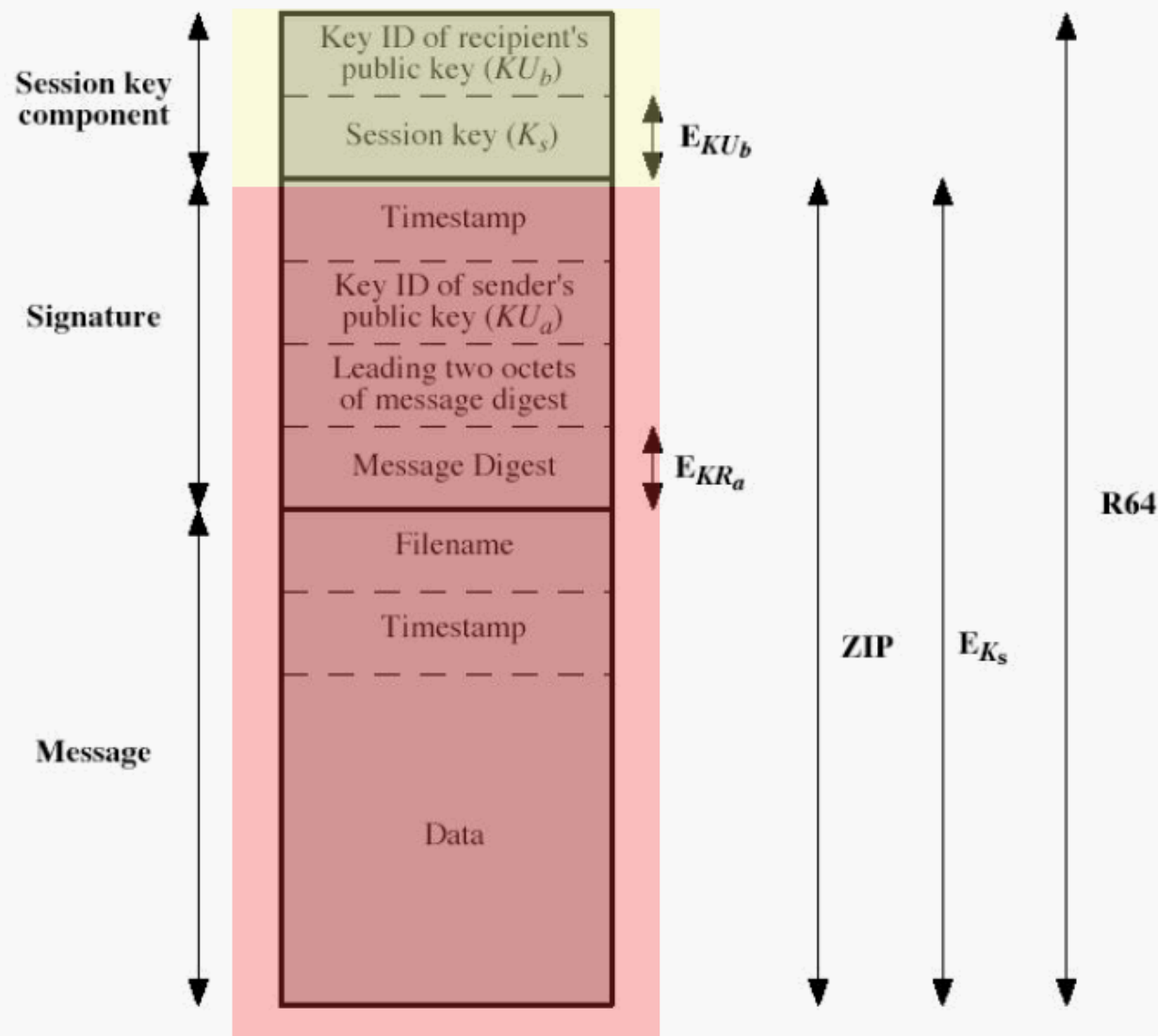
- Nachrichteninhalte +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des öffentlichen Sender-Schlüssels
- das alles gepackt und mit dem session key **verschlüsselt**
- dazu eben dieser mit dem public key des Empfängers **verschlüsselte** session key

Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

Content

Operation



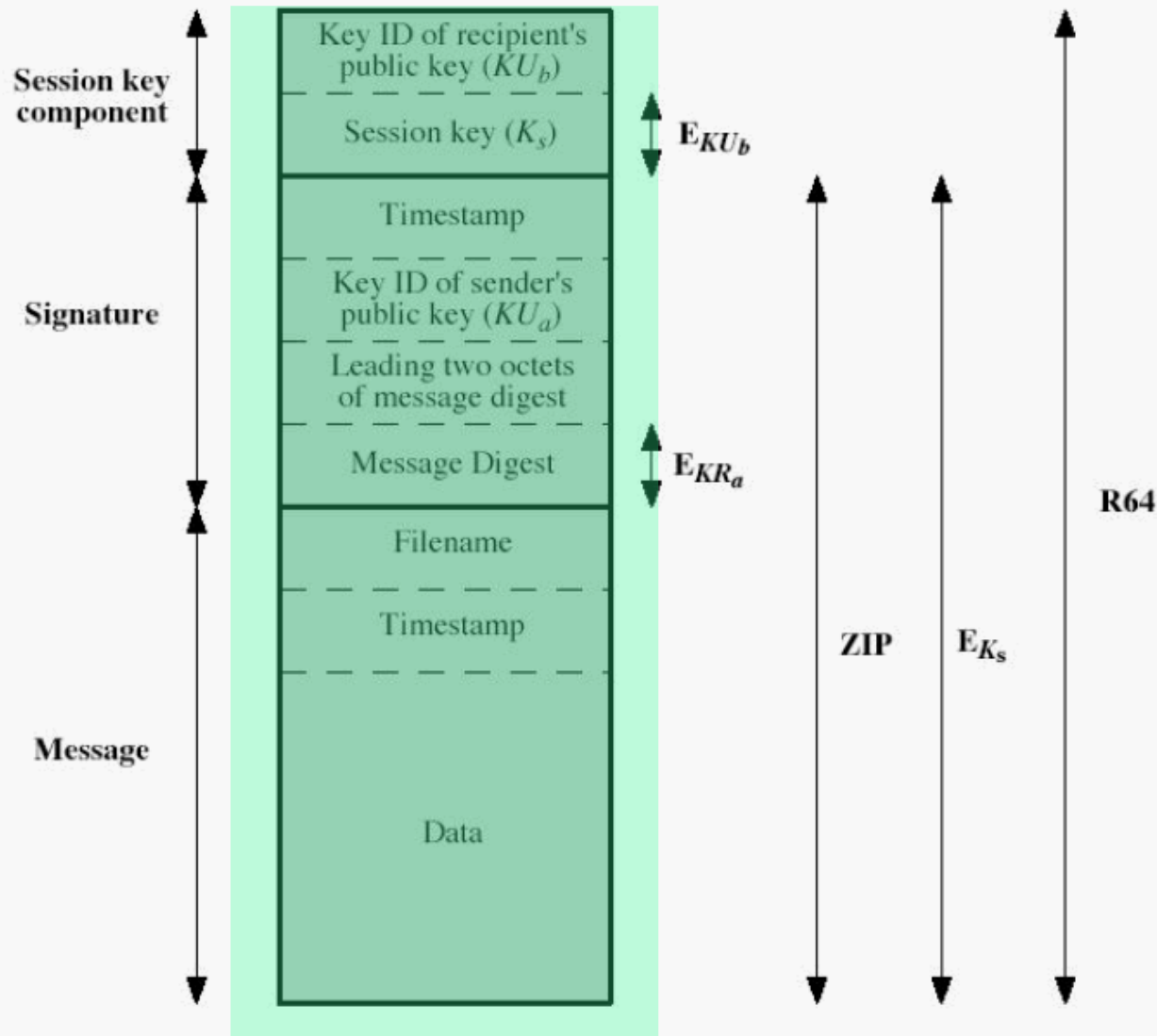
- Nachrichteninhalt +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des *öffentlichen* Sender-Schlüssels
- das alles gepackt und mit dem session key **verschlüsselt**
- dazu eben dieser mit dem public key des Empfängers **verschlüsselte** session key + ID des *öffentlichen* Empfänger-Schlüssels

Notation:

E_{KU_b} = encryption with user b's public key
 E_{KR_a} = encryption with user a's private key
 E_{K_s} = encryption with session key
 ZIP = Zip compression function
 R64 = Radix-64 conversion function

Content

Operation



- Nachrichteninhalt +
- Hash der Nachricht, **verschlüsselt** mit private key des Senders + ID des *öffentlichen* Sender-Schlüssels
- das alles gepackt und mit dem session key **verschlüsselt**
- dazu eben dieser mit dem public key des Empfängers **verschlüsselte** session key + ID des *öffentlichen* Empfänger-Schlüssels
- das alles byteweise nach ASCII konvertiert zum Versand per E-Mail

Notation:

- E_{KU_b} = encryption with user b's public key
- E_{KR_a} = encryption with user a's private key
- E_{K_s} = encryption with session key
- ZIP = Zip compression function
- R64 = Radix-64 conversion function

4.2 RSA

- Asymmetrisches Verschlüsselungsverfahren von Rivest, Shamir und Adleman
- Basis:
Produkt zweier hoher Primzahlen (300+ Stellen)
lässt sich nur sehr aufwendig faktorisieren
- <http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/>

4.3 Wichtigkeit von Öffentlichkeit

- Mathematische Grundlage ist überprüfbar
- Open Source: Software kann grundsätzlich von Fachleuten auf Fehler und Hintertüren überprüft werden
- Veröffentlichung des "Fingerabdrucks" (Hash) einer z.B. für Windows compilierten Fassung
- Nutzer kann den Hash seiner heruntergeladenen Fassung mit dem öffentlich bestätigten Hashwert vergleichen

Teil 5:

Links

Arbeiten im Browser

- Mailvelope
Addon für für Chrome und Firefox
<https://www.mailvelope.com/>

Arbeiten mit Thunderbird

- Windows: Gpg4win
(Erzeugen und Verwalten von Schlüsseln)
<http://www.gpg4win.de/>
- Thunderbird installieren
<https://www.mozilla.org/de/thunderbird/>
- Thunderbird-Addon Enigmail
<https://addons.mozilla.org/de/thunderbird/addon/enigmail/>

Nutzung unter Android

- K-9 Mail (Mailprogramm)
<https://play.google.com/store/apps/details?id=com.fsck.k9&hl=de>
- APG (Schlüsselverwaltung, arbeitet mit K-9 zusammen)
<https://play.google.com/store/apps/details?id=org.thialfihar.android.apg&hl=de>

Lernsoftware und Informationen

- CrypTool: <https://www.cryptool.org/de/>
Open Source E-Learning-Plattform und Software zu Kryptografie, mit didaktischem Begleitmaterial
- Theorie zum RSA-Verschlüsselungsverfahren:
<http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/>

Javascript

- Ausprobieren im Browser mit Javascript:
<http://encrypt.alexanderjank.de/>
<http://www.hanewin.net/encrypt/PGcrypt.htm>

Material 1

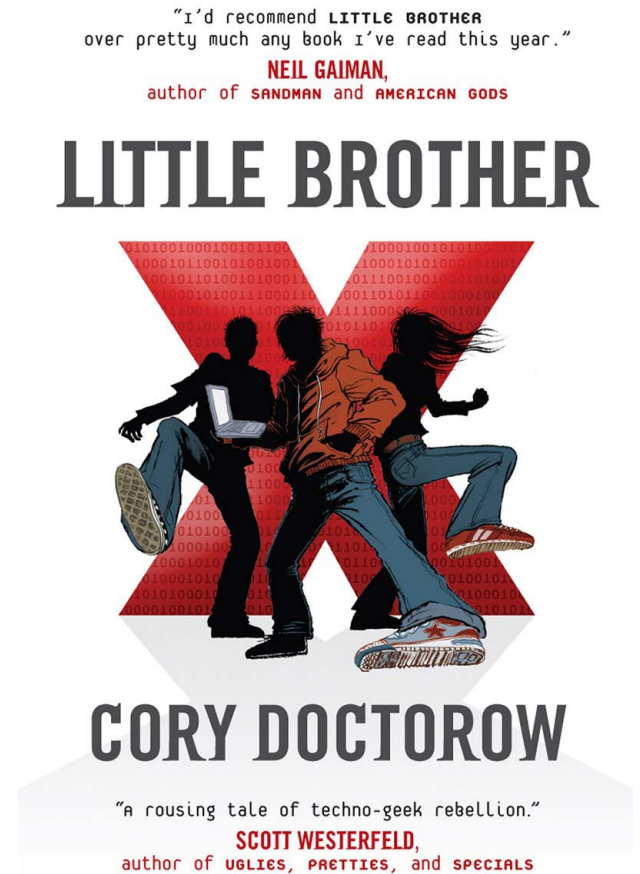
- Edward Snowden erklärt Greenwald die Benutzung von GPG – 2013, anonym, vor der Veröffentlichung:
<https://netzpolitik.org/2014/video-von-snowden-an-greenwald-e-mail-verschluesseleung-fuer-journalisten/>
<https://vimeo.com/56881481>
- Der digitale Briefumschlag (Ende-zu-Ende-Verschlüsselung erklärt):
<https://vimeo.com/17610424>
- PGP illustriert:
<http://www.cem.me/20150621-pgp-poster.html>
- "It's time for PGP to die"
<http://blog.cryptographyengineering.com/2014/08/w>

Material 2

- Last Week Tonight with John Oliver: Edward Snowden on Passwords
<https://www.youtube.com/watch?v=yzGzB-yYKcc>
- Promo-Video für Cryptopartys:
<https://netzpolitik.org/2015/cryptoparty-intro-video/>
- Bericht über Cryptoparty von Edward Snowden 2012:
<http://www.wired.com/2014/05/snowden-cryptoparty/>
- SWR über Cryptopartys (Juni 2015):
<http://www.swr.de/swr2/wissen/impuls-cryptoparty/-/id=661224/did=15658280/nid=661224/1a8lrrr/>

Cory Doctorow, Little Brother

- In naher Zukunft spielender Jugendroman von 2008, unter einer freien Lizenz veröffentlicht, auch deutsch übersetzt
- Kapitel 10: Beschreibung einer Krypto-Party



<http://craphound.com/category/littlebrother/>

Teil 6:

Was noch fehlt

Weiterführendes

- OpenPGP auch: Signieren + Verschlüsseln
- Grundsätzlich: Verwundbarkeit gegenüber Brute Force & Social Hacking
- Gewissheit: Woher weiß man, ob der öffentliche Schlüssel tatsächlich zu der Person gehört, die sie vorgibt? ("Web of Trust" und Kritik daran)
- Alternative Verschlüsselungsmethoden