Seminar
Konzepte von Betriebssystem-Komponenten

Web of Trust, PGP, GnuPG

von Tobias Sammet

tobias.sammet@informatik.stud.uni-erlangen.de

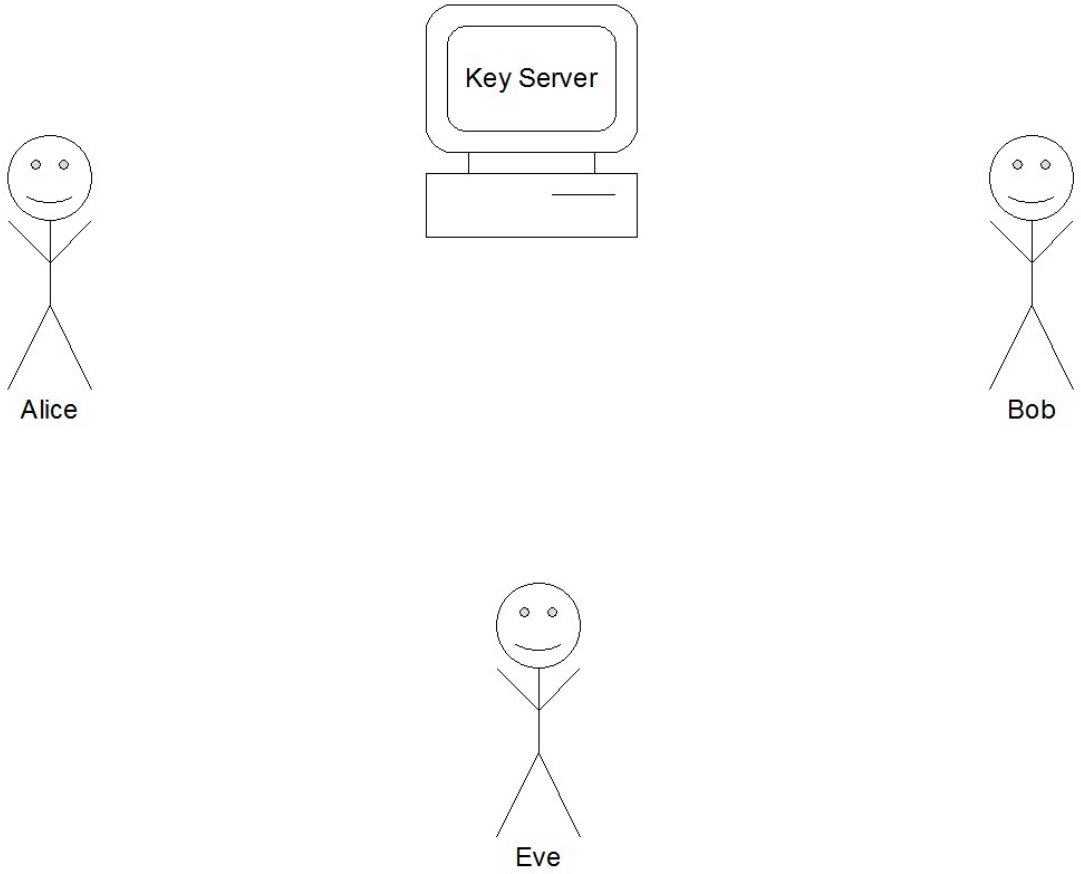
16. Juni 2010

Motivation

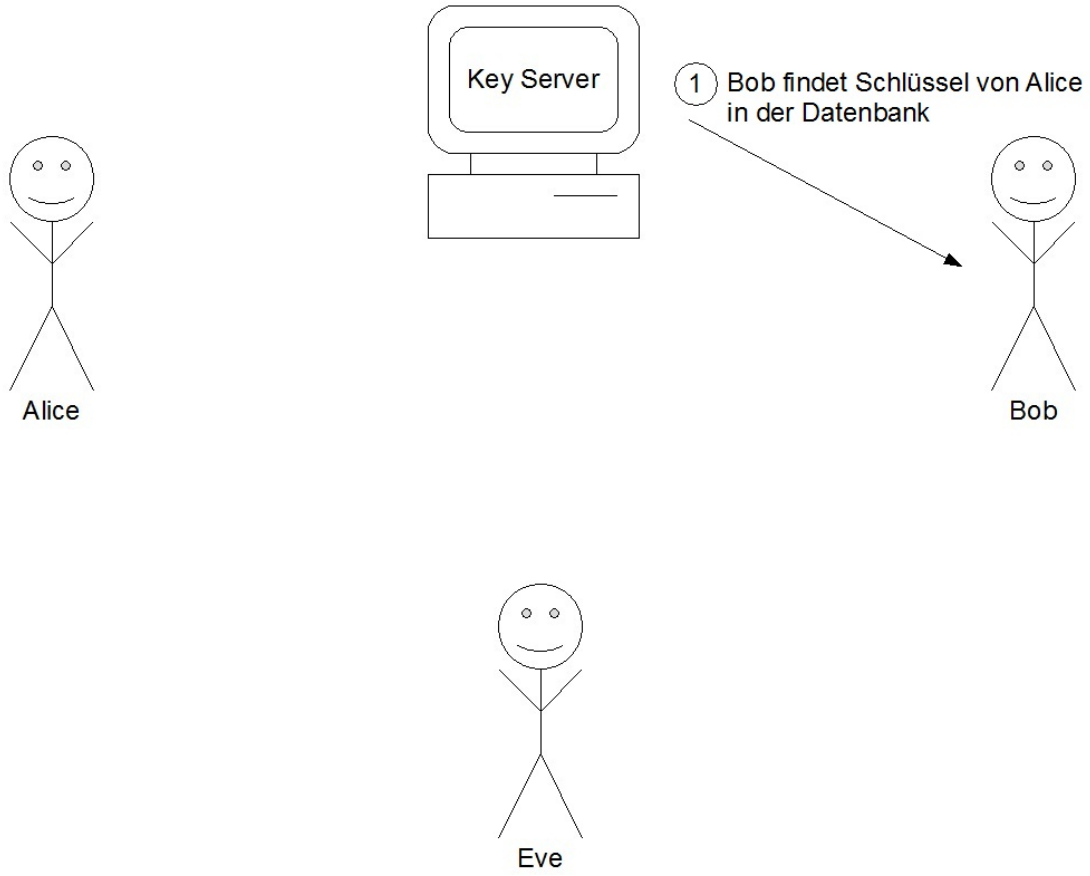
- Szenario: E-Mail-Verschlüsselung
  - Angreifer generiert Schlüssel für existierende E-Mail Adresse
  - Versenden der verschlüsselten Nachricht an Zielperson, aber:
    - E-Mail kommt bei Zielperson an, allerdings unleserlich
    - E-Mail kommt bei Zielperson nicht an, weil sie vom Angreifer abgefangen wurde

      („*Man-in-the-Middle-Problem*“)

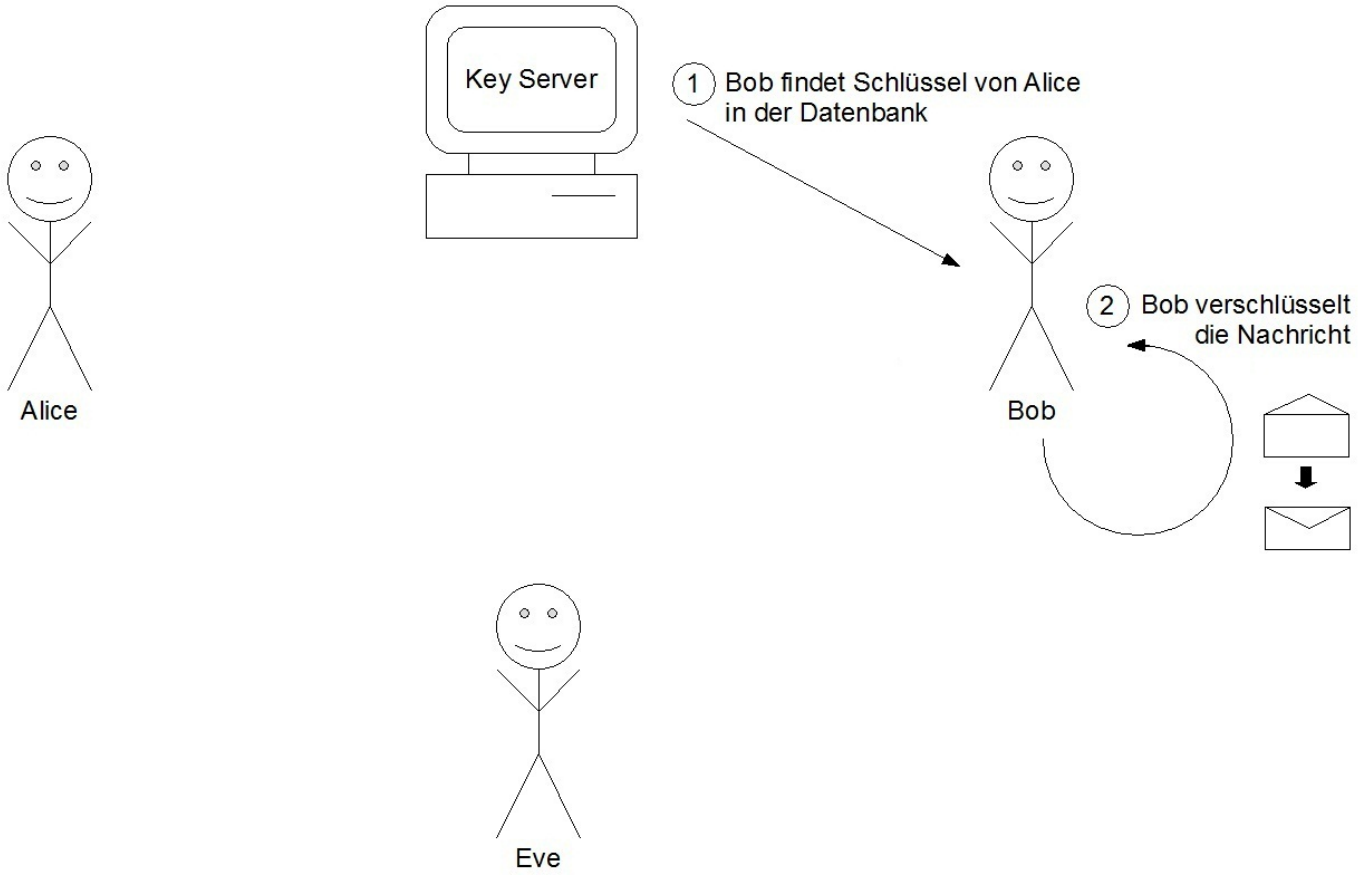
Motivation



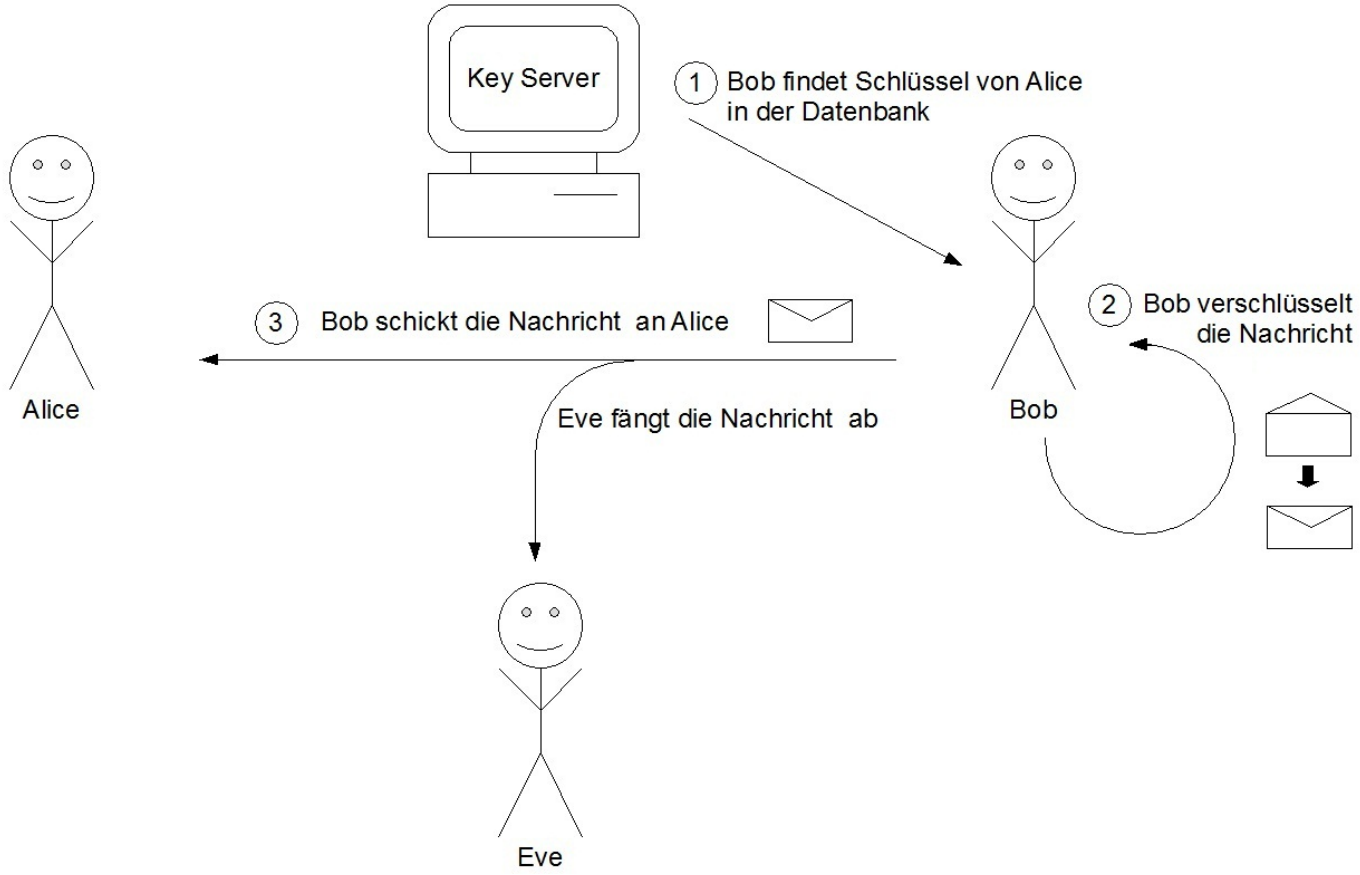
Motivation


Key Server
1
Bob findet Schlüssel von Alice
in der Datenbank
Alice
Bob
Eve

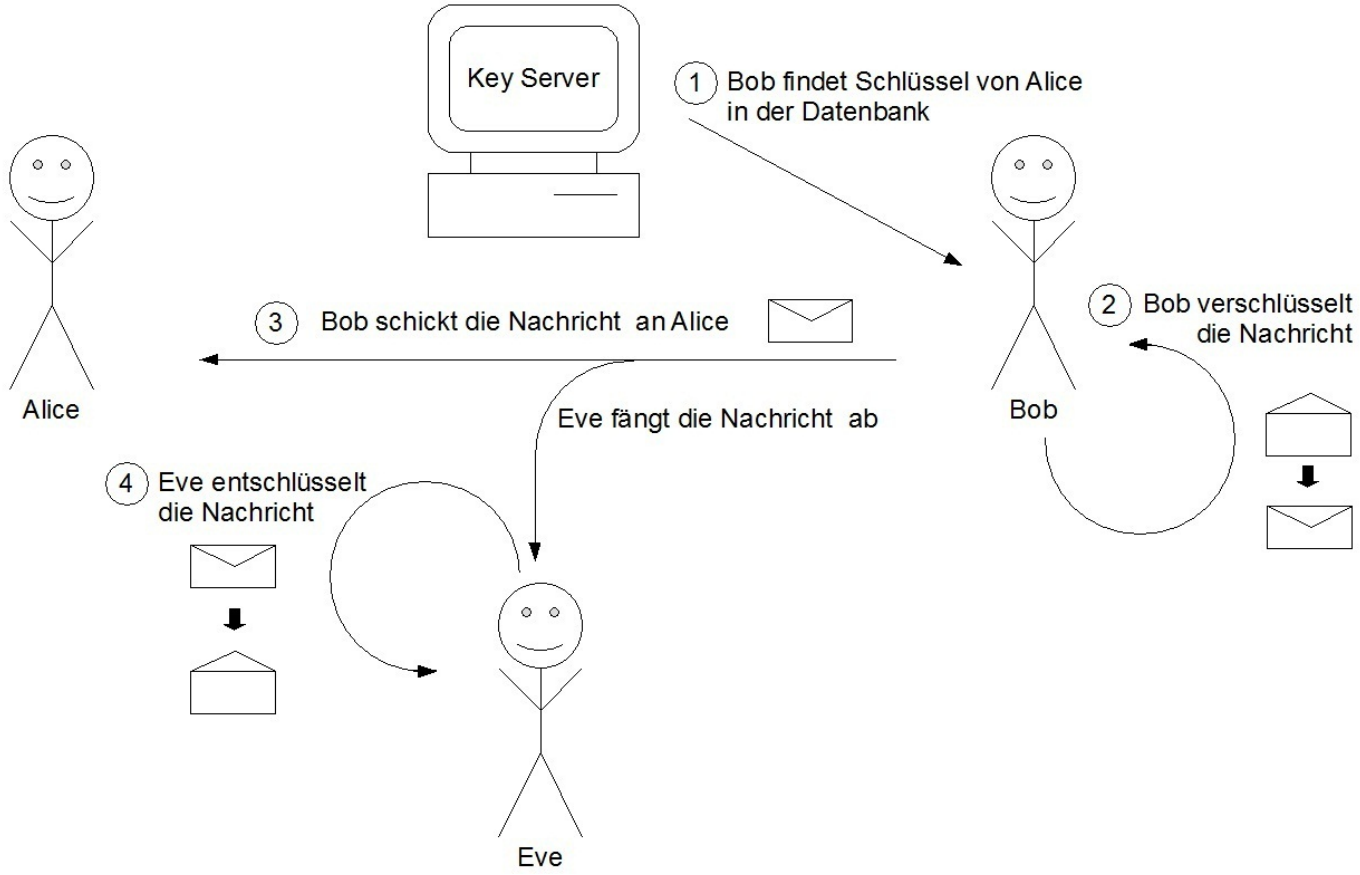
Motivation


Key Server
1 Bob findet Schlüssel von Alice in der Datenbank
Alice
Bob
2 Bob verschlüsselt die Nachricht
Eve

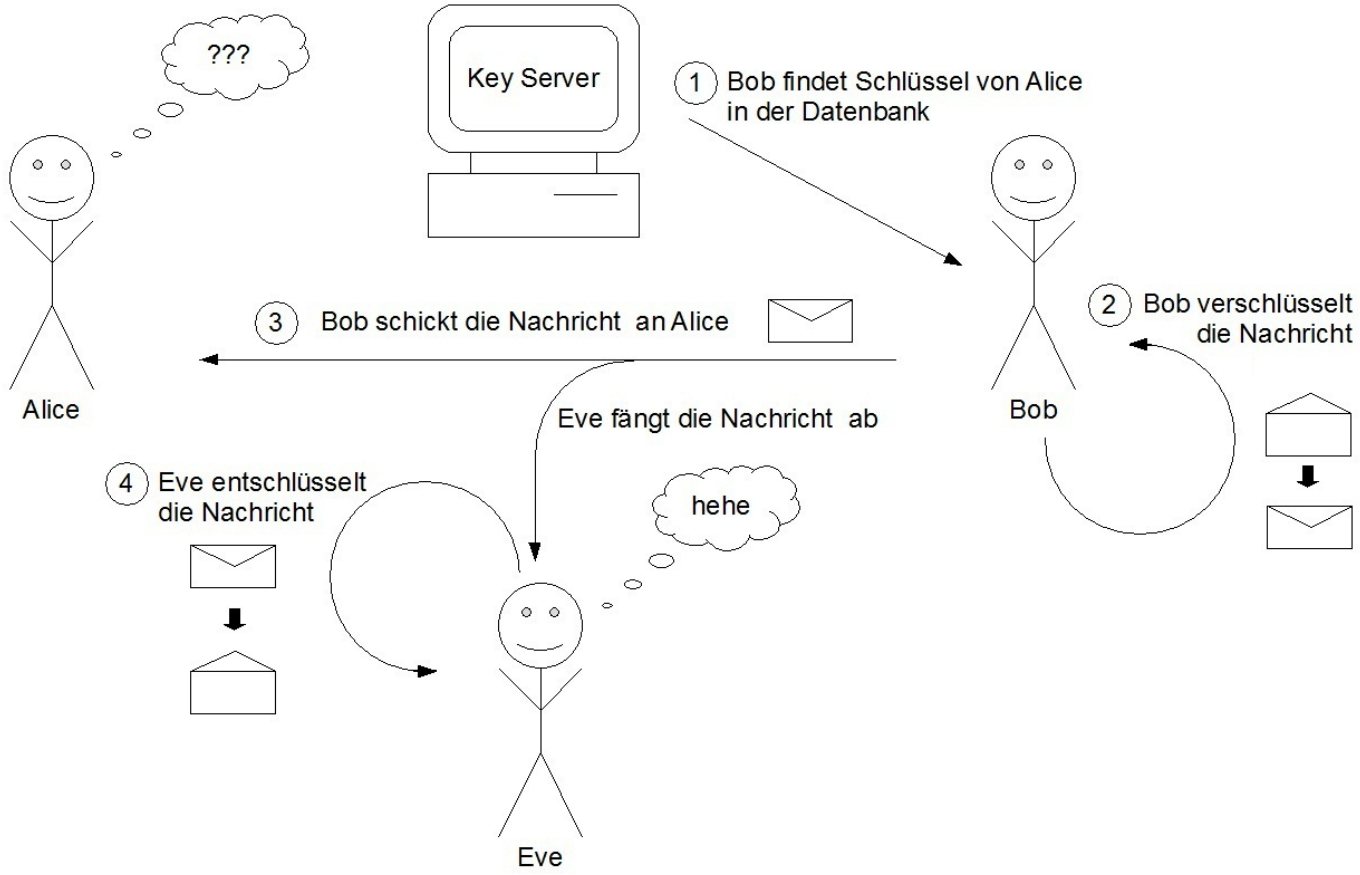
Motivation


Key Server
1 Bob findet Schlüssel von Alice in der Datenbank
Alice
3 Bob schickt die Nachricht an Alice
Eve fängt die Nachricht ab
Bob
2 Bob verschlüsselt die Nachricht
Eve

Motivation


Key Server
1 Bob findet Schlüssel von Alice in der Datenbank
Alice
Bob
2 Bob verschlüsselt die Nachricht
3 Bob schickt die Nachricht an Alice
Eve fängt die Nachricht ab
4 Eve entschlüsselt die Nachricht
Eve

Motivation


???
Key Server
1 Bob findet Schlüssel von Alice in der Datenbank
Alice
Bob
2 Bob verschlüsselt die Nachricht
3 Bob schickt die Nachricht an Alice
Eve fängt die Nachricht ab
4 Eve entschlüsselt die Nachricht
hehe
Eve

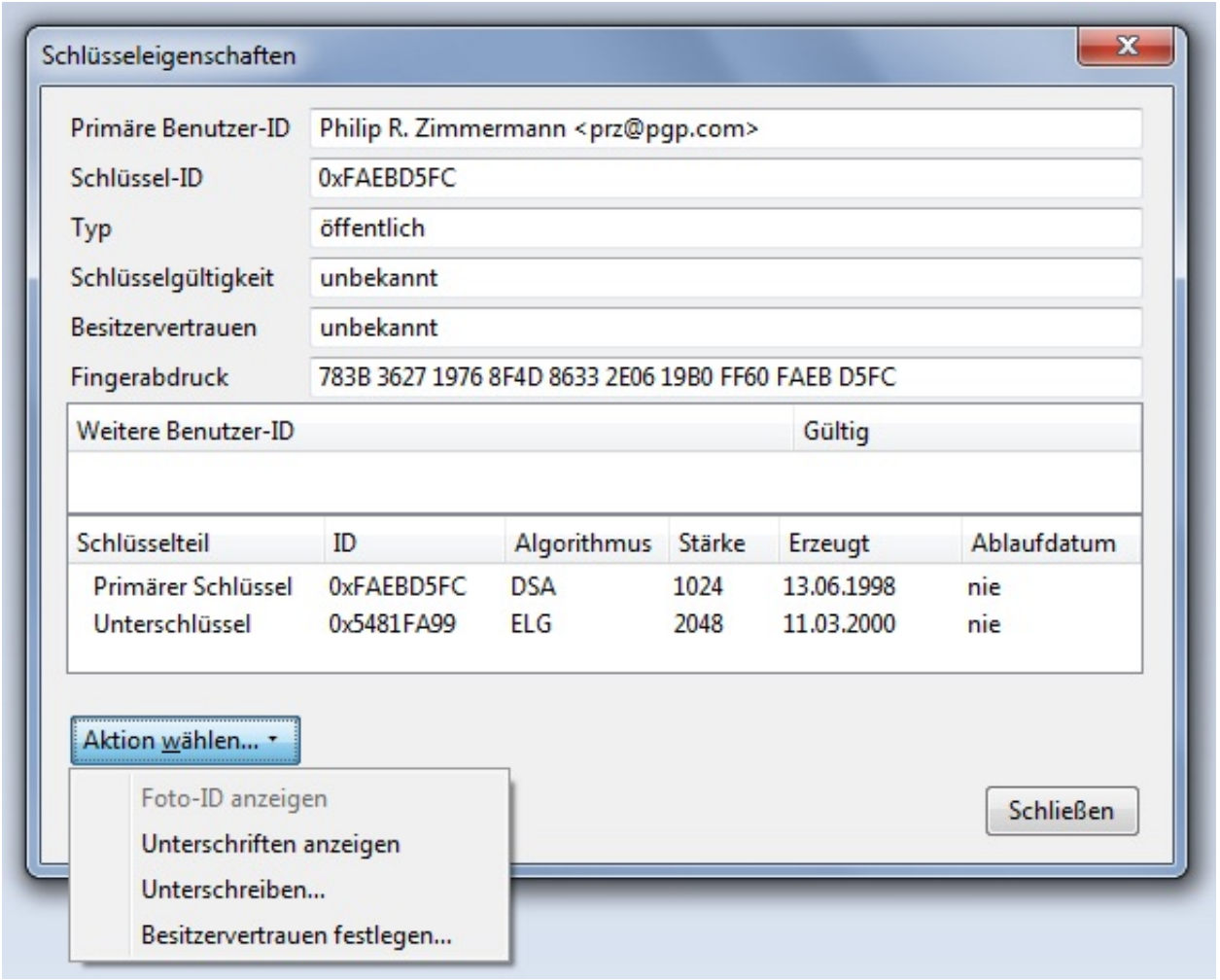
Gliederung des Vortrags

- Motivation
- **Web of Trust (WOT)**
  - **Was ist das Web of Trust?**
  - **Trust Model**
- Pretty Good Privacy
- Gnu Privacy Guard
- Zusammenfassung

Web of Trust - Allgemeines

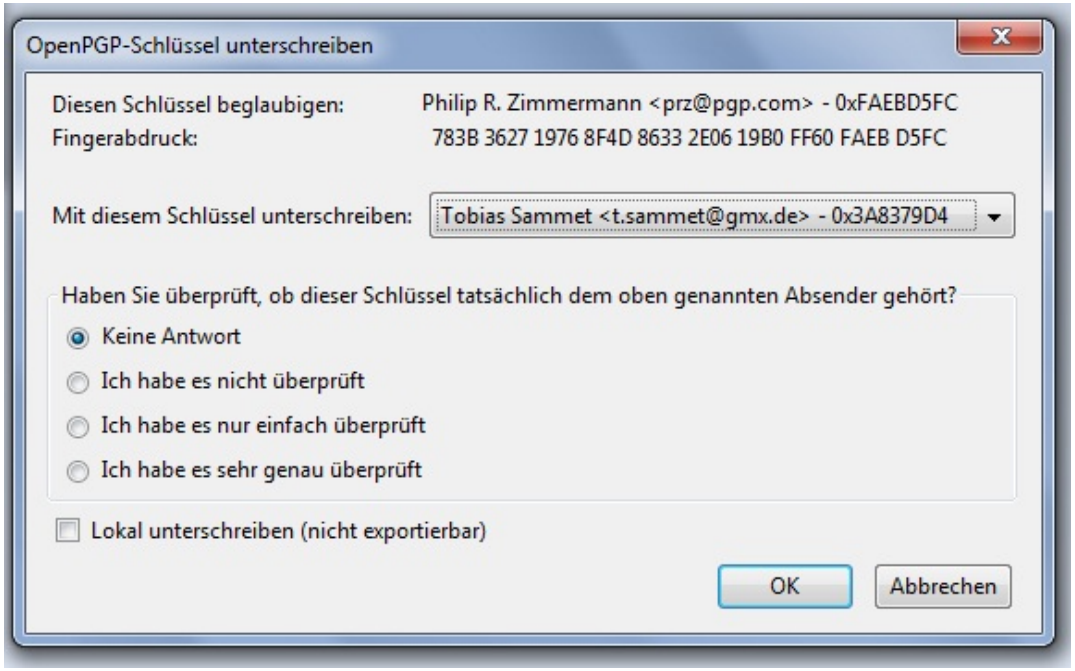
- Idee: Vorbeugung eines solchen Szenarios durch ein dezentrales Vertrauensmodell: *Web of Trust (WOT)*
- Entscheidung über die Gültigkeit (*Validity*) und die Vertrauenswürdigkeit (*Trustability*) eines fremden öffentlichen Schlüssels durch ein digitales Zertifikat

Web of Trust - Funktionsweise



Web of Trust - Funktionsweise

- Überprüfung der Authentizität und Integrität eines fremden öffentlichen Schlüssels (= *Gültigkeit*)
  - Keine Überprüfung (*undefined*)
  - Einfache Überprüfung (*marginal*)
  - Genaue Überprüfung (*complete*)



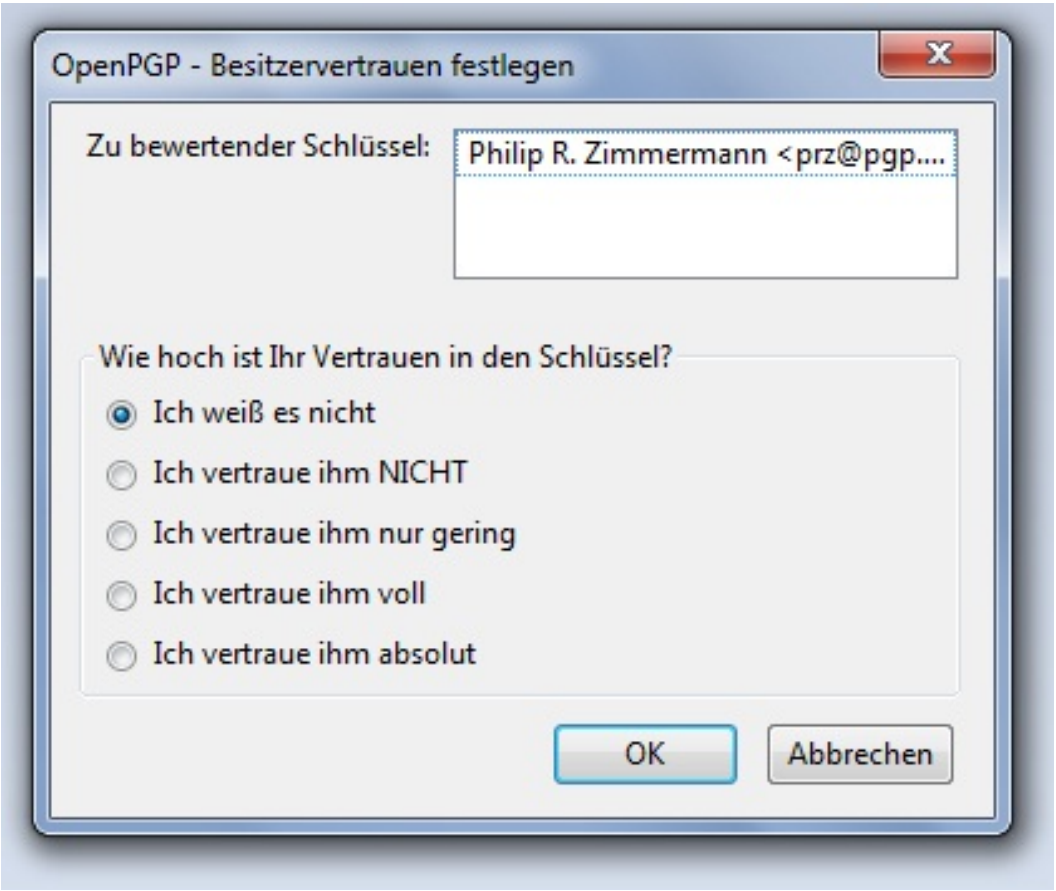
Web of Trust - Funktionsweise

- Signierung des digitalen Zertifikats mit eigenem privaten Schlüssel

  (*Key Signing*)
  - sog. *Key Signing Parties*
- Aussprechen eines pers. Vertrauens zu der Person

  (transitiv wirkendes *Trust Model)*
  - Kein Vertrauen (*Untrusted*)
  - Teilweises Vertrauen (*Marginally trusted*)
  - Volles Vertrauen (*Fully trusted*)
  - Absolutes Vertrauen (*Ultimately trusted*)

Web of Trust - Funktionsweise

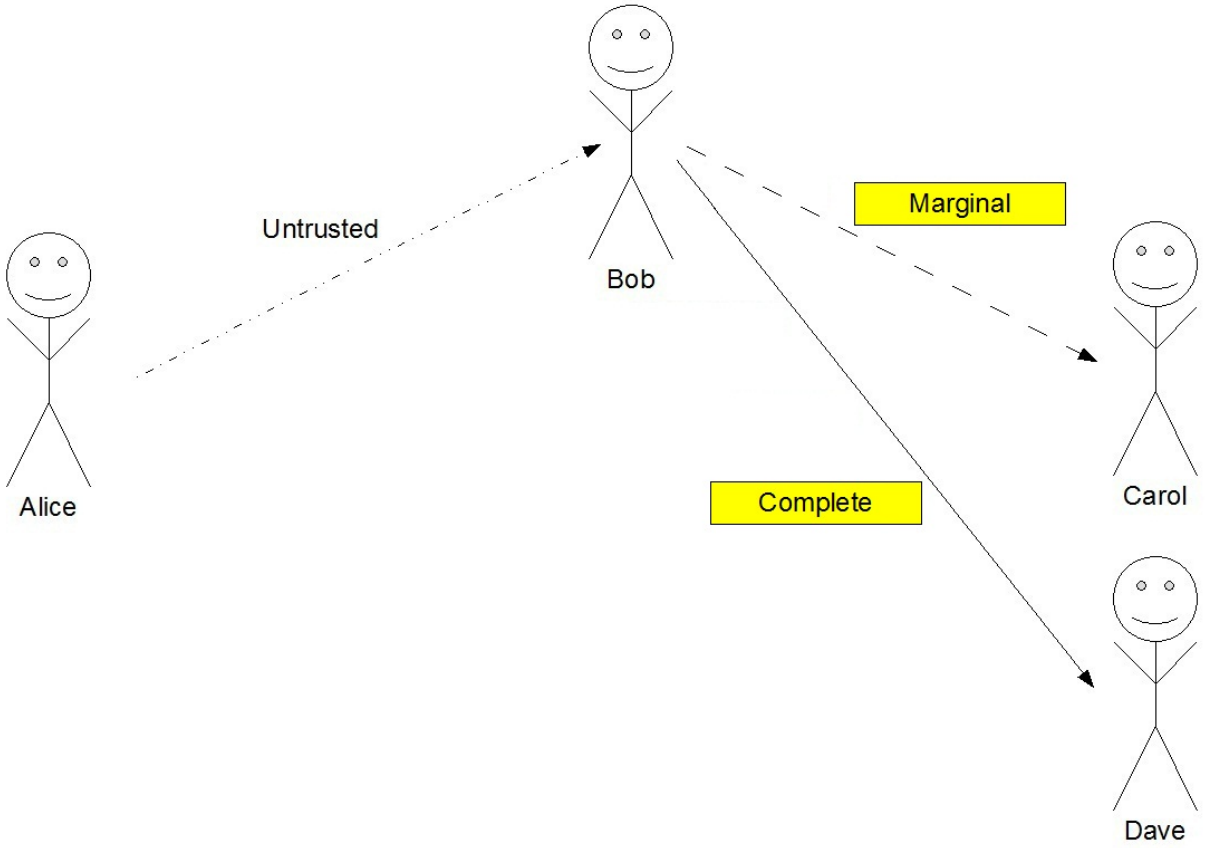


Web of Trust - Funktionsweise

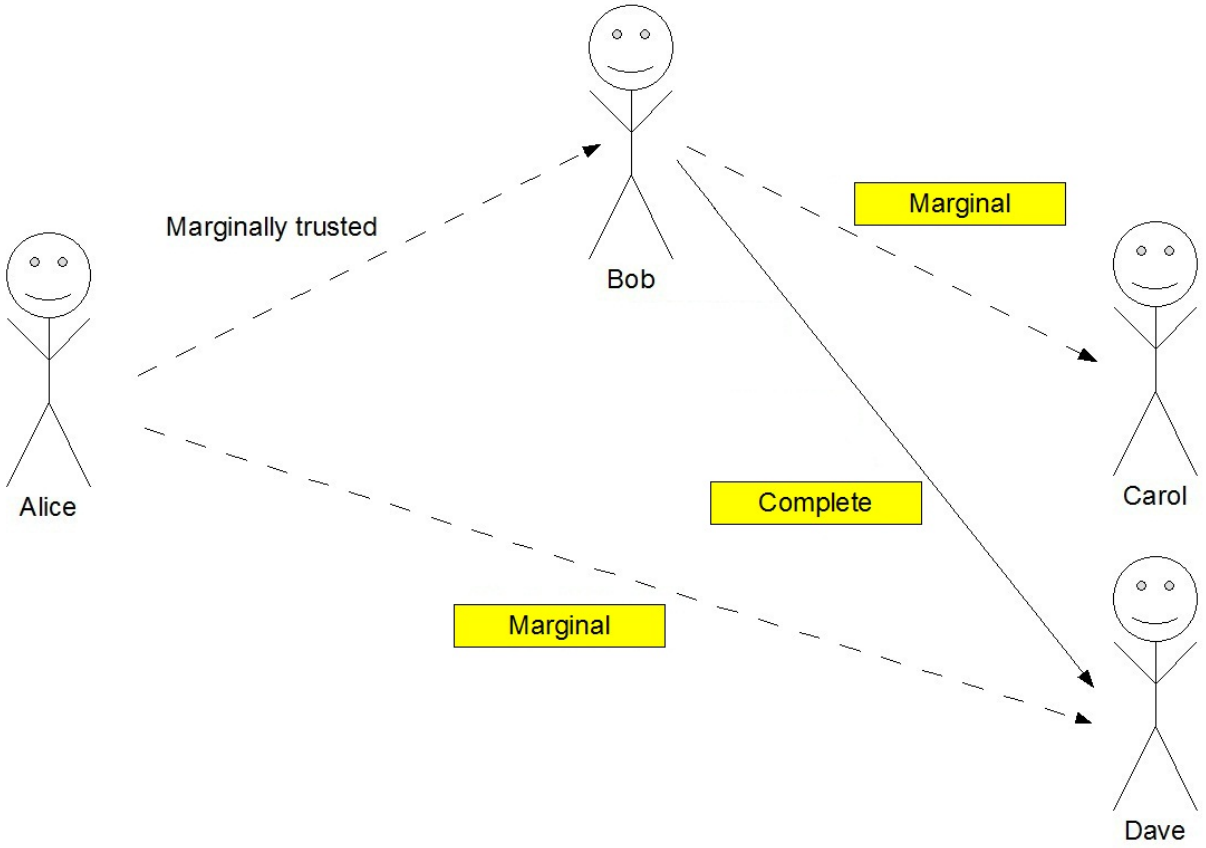
- *Trust Model* mit *Validity* ganz eng verwoben
  - *Validity* zeigt an, ob ich der Echtheit eines Schlüssels vertraue
  - *Trust Model* zeigt an, ob ich der Person hinter dem Schlüssel vertraue

	Undefined	Marginal	Complete
Untrusted	**X**		
Marginally trusted	**X** (Marginal)	**X** (Complete)	**X** (3 x Complete)
Fully trusted		**X** (Marginal)	**X** (Complete)

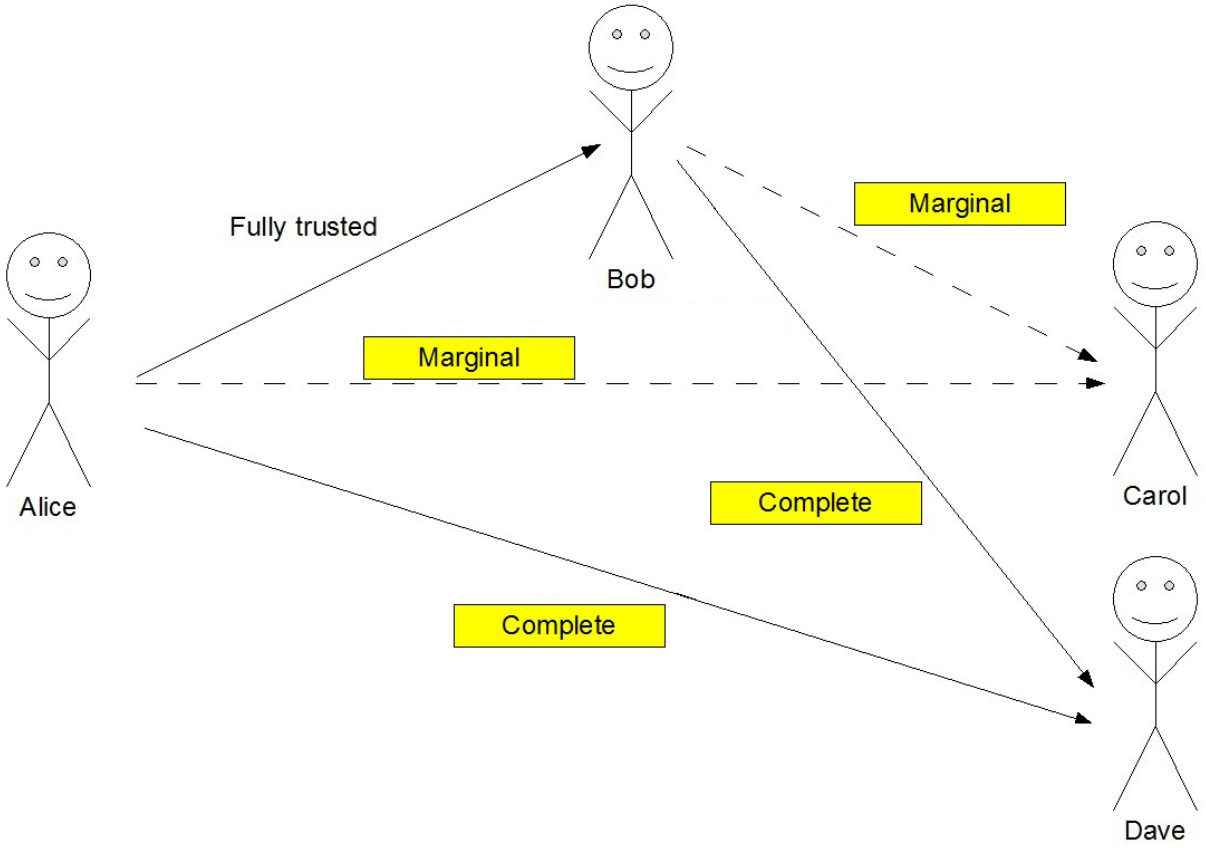
Web of Trust am Beispiel



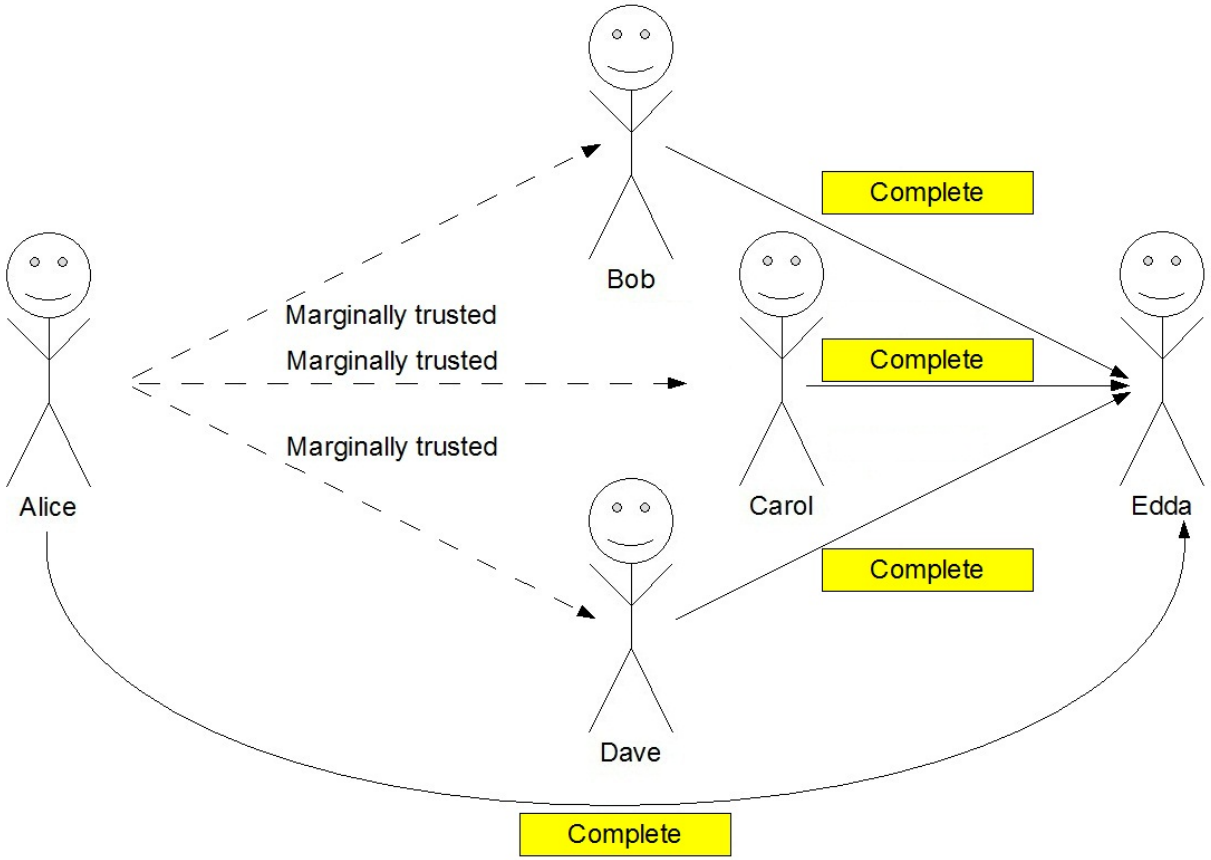
Web of Trust am Beispiel



Web of Trust am Beispiel



Web of Trust am Beispiel



Web of Trust - Fazit

- **(Erwünschter) Idealfall:** Gefälschte Schlüssel und nicht vertrauenswürdige Personen werden sichtbar gemacht
- **Gefahr:** Jeder Teilnehmer des Web of Trust kann die Tür für einen Angreifer öffnen

- **Fazit:**
  - Web of Trust ist ein riesiges Netzwerk gegenseitigen Vertrauens, das die Grundlage für PGP bzw. GnuPG bildet
  - Web of Trust meist im Zusammenhang mit PGP bzw. GnuPG

Gliederung des Vortrags

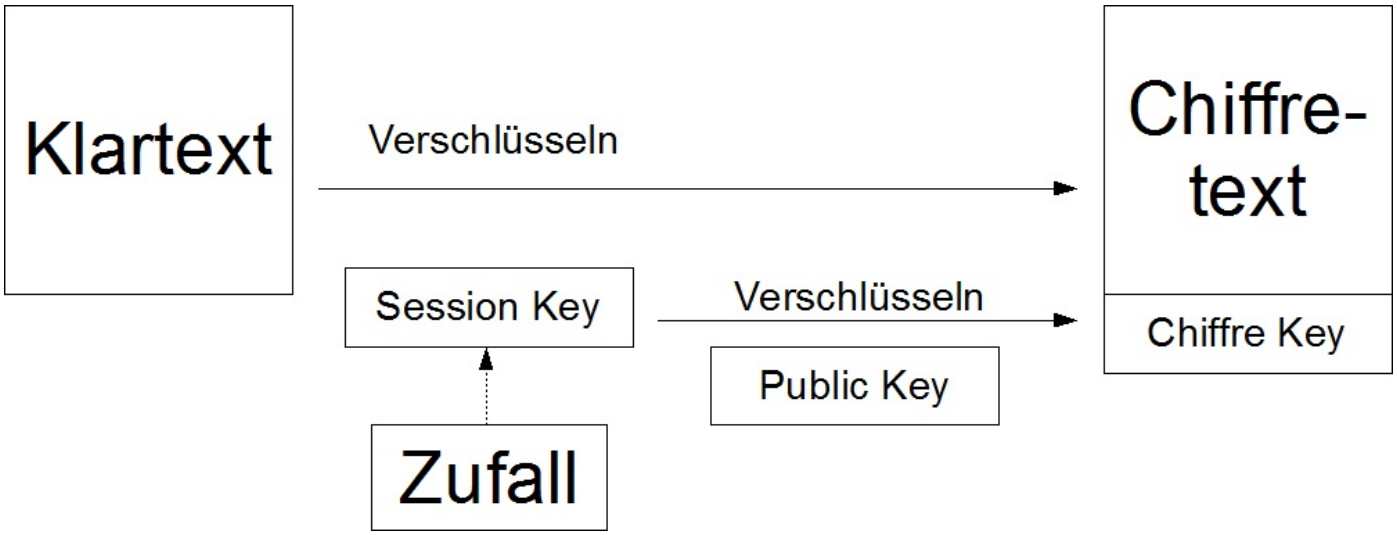
- Motivation
- Web of Trust
- **Pretty Good Privacy (PGP)**
  - **Wie funktioniert Verschlüsseln, Entschlüsseln bei PGP?**
  - **Wie funktioniert Signieren und Verifizieren bei PGP?**
- Gnu Privacy Guard
- Zusammenfassung

Pretty Good Privacy - Allgemeines

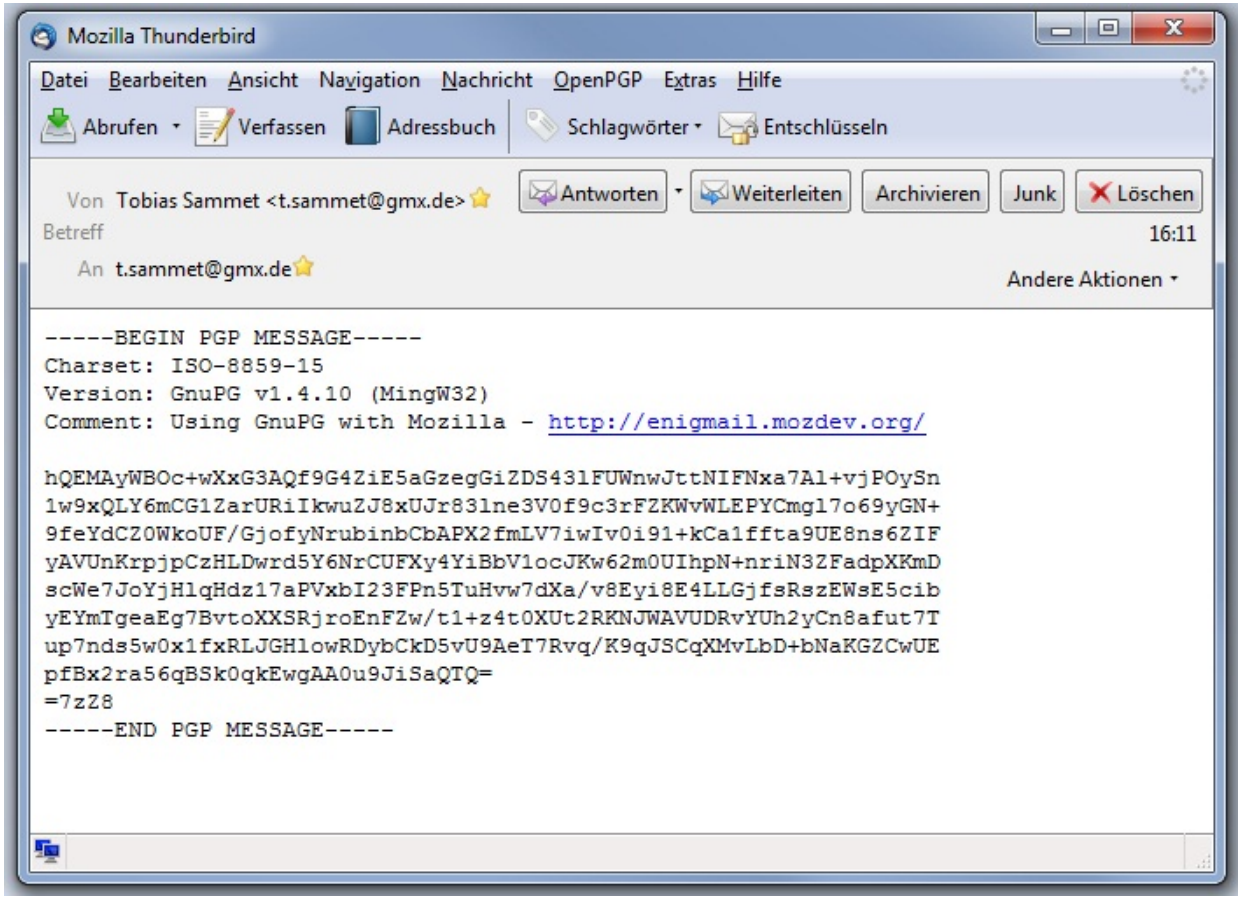
- Kurze Wiederholung:
  - Symmetrische Verschlüsselung
    - Ein Schlüssel für Verschlüsselung und Entschlüsselung
  - Asymmetrische Verschlüsselung
    - Privater, geheimer Schlüssel (*Private Key*)
    - Öffentlich zugänglicher Schlüssel (*Public Key*) auf Key Servern
    - Zusätzlich: Passphrase bei Verwendung des *Private Key*
- Pretty Good Privacy (PGP) ein hybrides Verfahren
  - Verwendung von symmetrischer und asymmetrischer Verschlüsselungstechnik

Pretty Good Privacy - Verschlüsseln

- Funktionsweise:
  - Verschlüsselung (*Encryption*)
    - Symmetrische Verschlüsselung des Klartextes (mit einem zufälligen Session Key)
    - Asymmetrische Verschlüsselung des Session Key (mit dem Public Key des Empfängers)

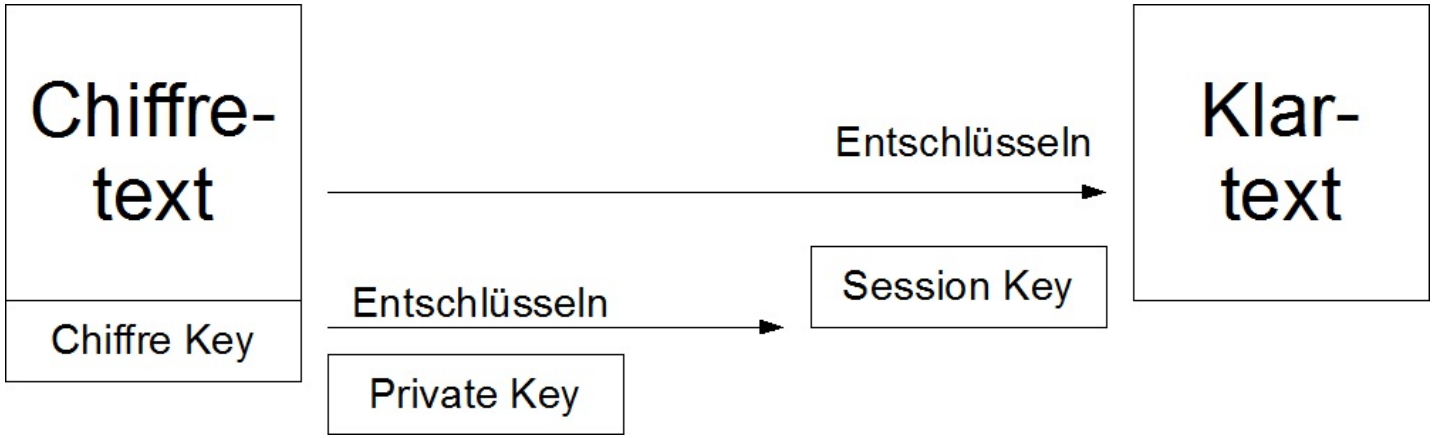


Pretty Good Privacy - Verschlüsseln

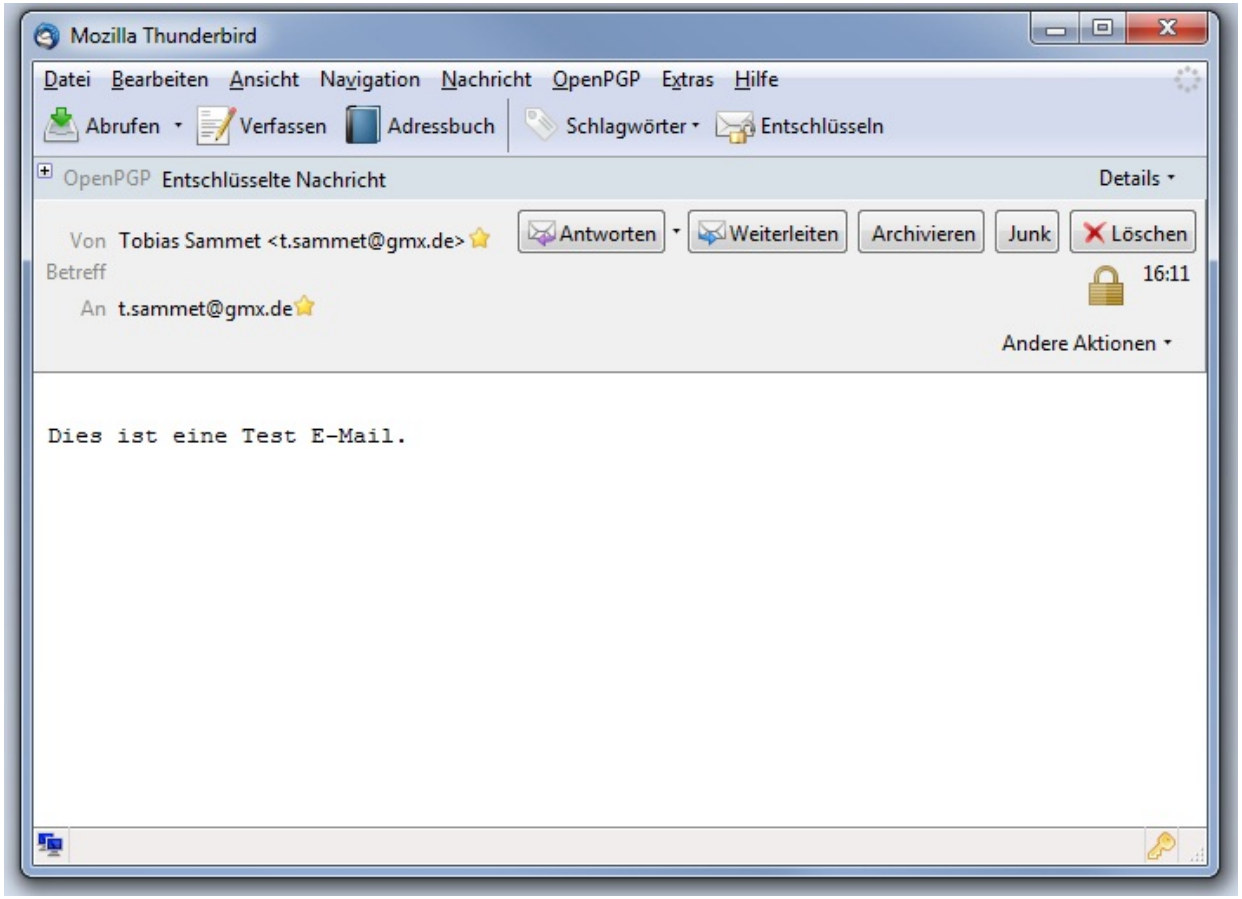


Pretty Good Privacy - Entschlüsseln

- Funktionsweise:
  - Entschlüsselung (*Decryption*)
    - Im Grunde: Umgekehrter Weg zur Verschlüsselung
    - Asymmetrische Entschlüsselung des Session Key (mit dem Private Key des Empfängers)
    - Symmetrische Entschlüsselung des Chiffretextes (mit gerade entschlüsseltem Session Key)

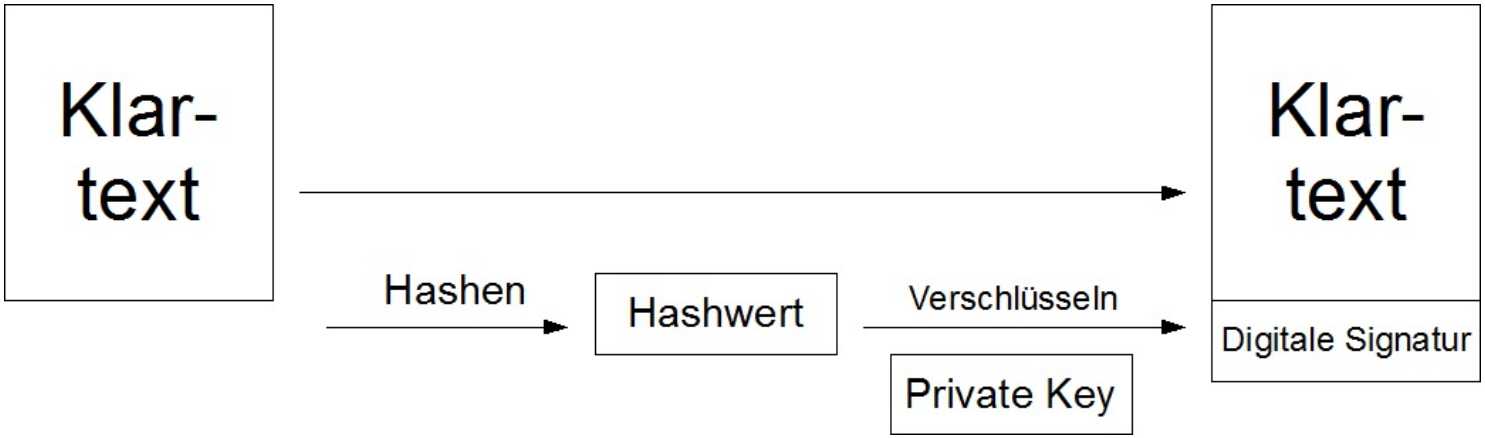


Pretty Good Privacy - Entschlüsseln

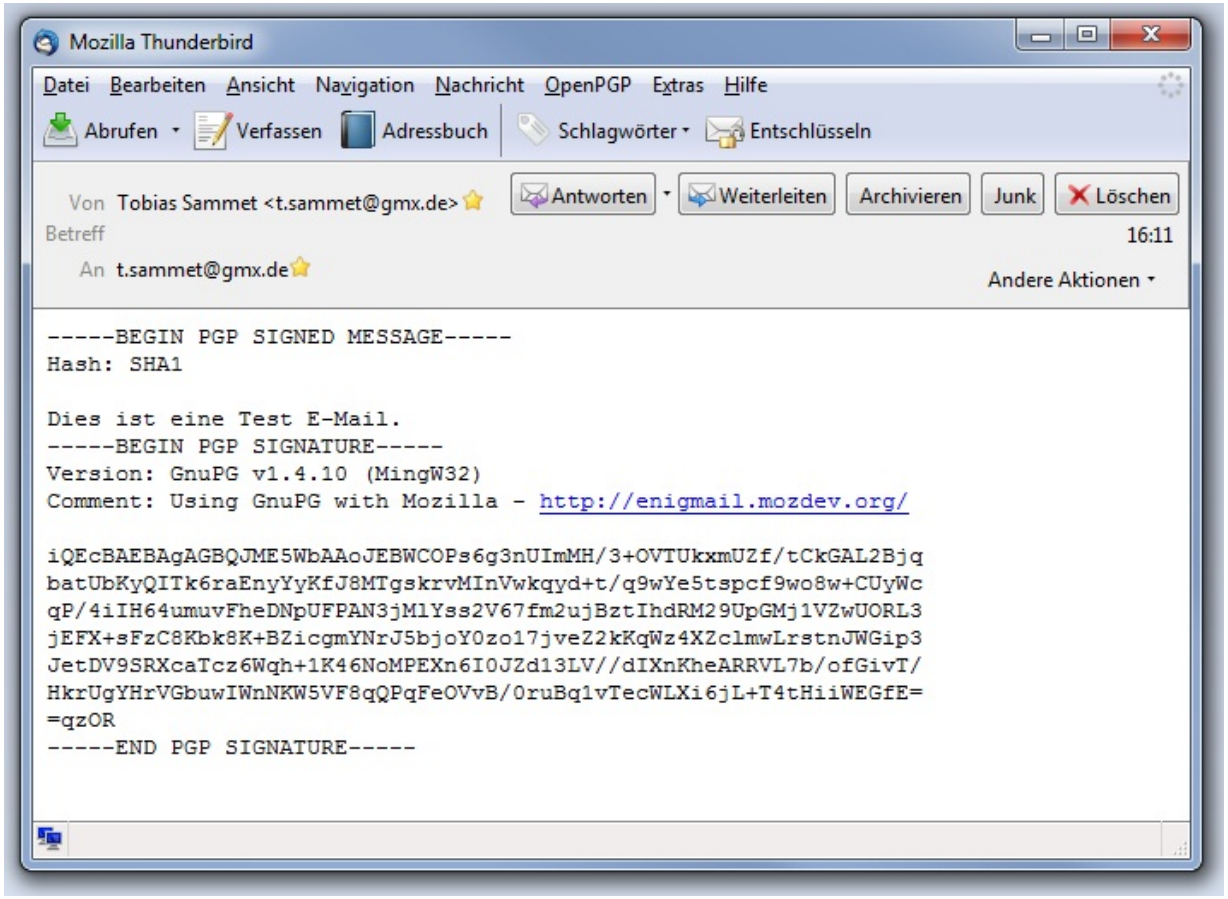


Pretty Good Privacy - Signierung

- Funktionsweise:
  - Signierung
    - Für den Empfänger Möglichkeit zur Überprüfung, ob die Nachricht
      - wirklich vom Absender ist
      - unterwegs verändert wurde
    - Bildung des Hashwertes vom Klartext
    - Asymmetrische Verschlüsselung mit Private Key des Absenders

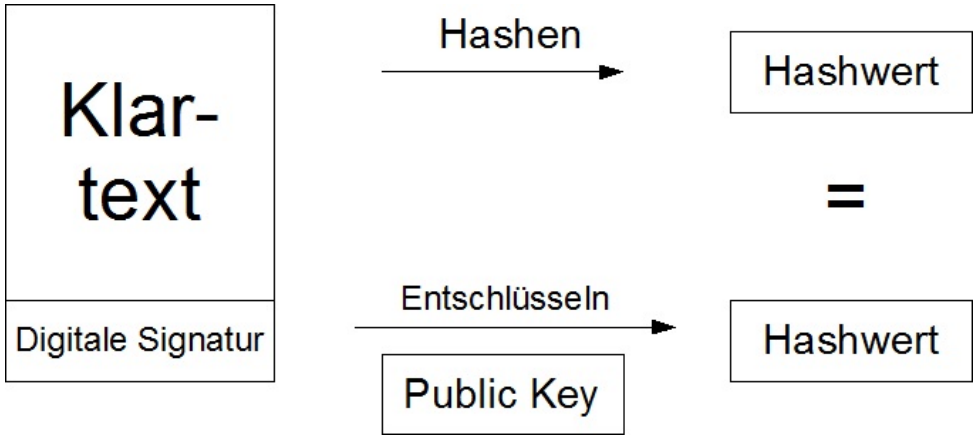


Pretty Good Privacy - Signierung

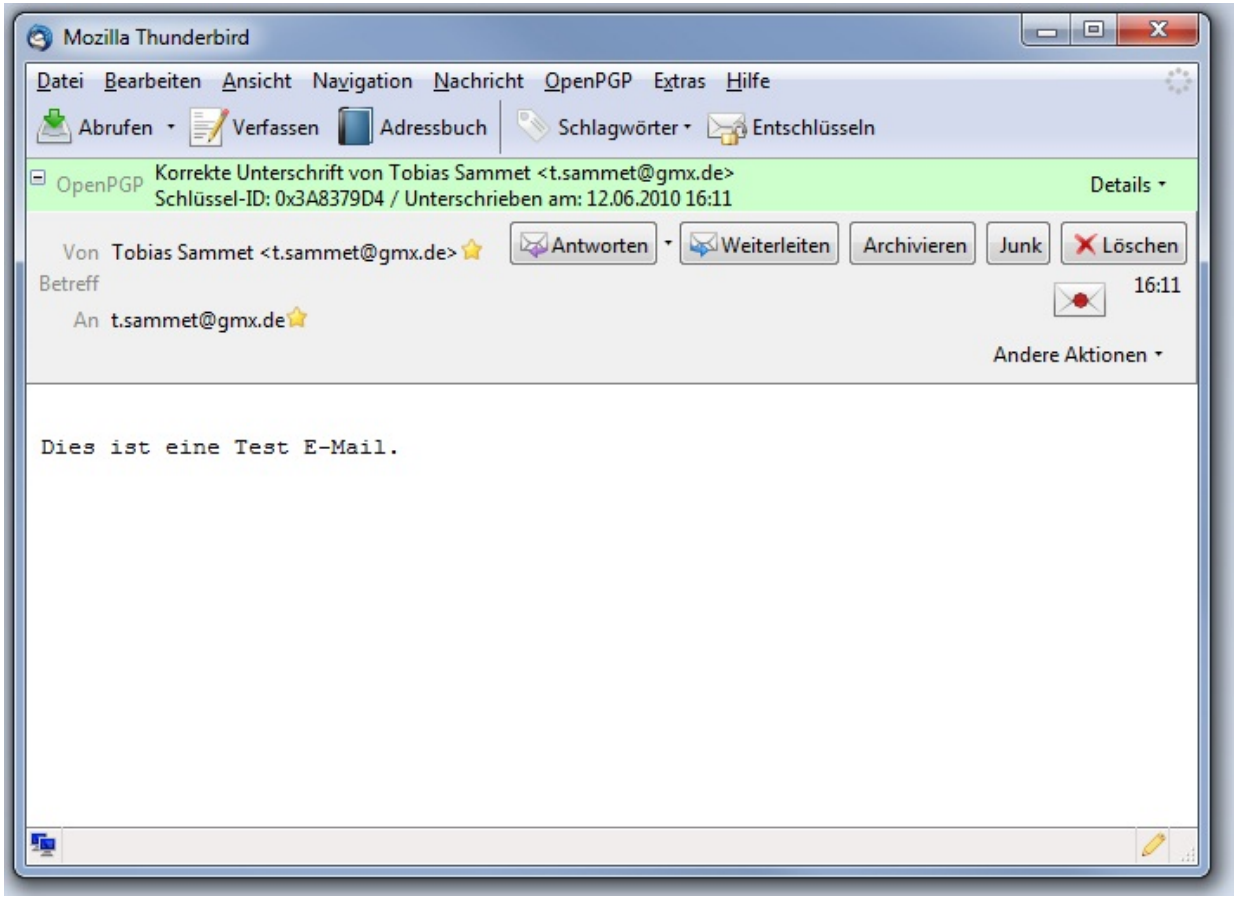


Pretty Good Privacy - Verifikation

- Funktionsweise:
  - Verifikation
    - Im Grunde: Umgekehrter Weg zur Signierung
    - Asymmetrische Entschlüsselung der Signatur mit dem Public Key des Absenders
    - Erneute Bildung des Hashwertes vom Klartext
    - Vergleich des entschlüsselten und erzeugten Hashwertes



Pretty Good Privacy - Verifikation



Gliederung des Vortrags

- Motivation
- Web of Trust
- Pretty Good Privacy
- **Gnu Privacy Guard (GnuPG)**
  - **Gemeinsamkeiten und Unterschiede zu PGP**
- Zusammenfassung

Gnu Privacy Guard

- Gemeinsamkeiten: Identische Funktionsweise zu PGP (OpenPGP-Standard RFC 2440 bzw. RFC 4880)
- Unterschiede:

	GnuPG	**PGP**
Kosten	Kostenlos	Kostenpflichtig
Source	Open Source	Closed Source
Algorithmen (allgemein)	Verwendung von patentfreien Algorithmen	Verwendung auch von patentierten Algorithmen
Algorithmen (symmetrisch)	AES, CAST5, BLOWFISH, TWOFISH, 3DES	AES, CAST5, IDEA, TWOFISH, 3DES
Algorithmen (asymmetrisch)	RSA, ElGamal	RSA, DH
Hash-Alg.	SHA1, MD5	SHA1

Gliederung des Vortrags

- Motivation
- Web of Trust
- Pretty Good Privacy
- Gnu Privacy Guard
- **Zusammenfassung**

Zusammenfassung

- Web of Trust (WOT)
  - Dezentrales Vertrauensmodell, um über Vertrauenswürdigkeit der Teilnehmer zu entscheiden
    - Überprüfung der Authentizität mit Signierung im Erfolgsfall
    - Trust Model
- Pretty Good Privacy (PGP)
  - Software, die hybrides Verfahren zur Ver- und Entschlüsselung verwendet
    - Funktionsweise Verschlüsselung und Entschlüsselung
    - Funktionsweise Signierung und Verifikation
- Gnu Privacy Guard (GnuPG)
  - Gemeinsamkeiten, Unterschiede mit PGP

Quellen

- Mick Tobor, „Verschlüsseln & Signieren“, 2002, Markt-und-Technik-Verlag, München
- Jörg Schwenk, „Sicherheit und Kryptographie im Internet“, 2. Auflage, 2005, Friedr. Vieweg & Sohn Verlag/GWV Fachverlage GmbH, Wiesbaden
- Krzysztof Janowicz, „Sicherheit im Internet“, 2. Auflage, 2006, O‘Reilly Verlag, Köln
- William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, „Firewalls and Internet Security“, 2nd Edition, 2003, Addison-Wesley
- http://www.uni-koeln.de/rrzk/sicherheit/pgp/
- http://www.iks-jena.de/mitarb/lutz/security/pgp/
- http://www.wim.uni-koeln.de/uploads/media/The_PGP_Trust_Model.pdf
- http://www.informatik.uni-hamburg.de/RZ/software/pgp_win/
- http://en.wikipedia.org/wiki/GNU_Privacy_Guard
- http://en.wikipedia.org/wiki/Pretty_Good_Privacy
- http://en.wikipedia.org/wiki/Web_of_trust
- http://www.rubin.ch/pgp/weboftrust.de.html
- http://www.rubin.ch/pgp/pgp.de.html
- http://www.gnupg.org/gph/en/manual/book1.html
- http://www.pgp.com/

Vielen Dank für eure Aufmerksamkeit!