CryptoCampagne

Thomas Funke
Fachbereich Informatik
Universität Hamburg

Die Tour

- Intro & Motivation
- Public Key Encryption
- Alice and Bob
- Web of Trust
- OpenPGP

Motivation or “why the hell bother”

- Kommunikation ohne ungewollte Zuhörer
- Sicherstellen von Informationsquellen

- Freiheit
- Kryptografie als Gebiet der Informatik
- Unterstützung von Straftaten?
- Weils geht

Public Key Encytption

Einführung, Erläuterung, Vor- und Nachteile

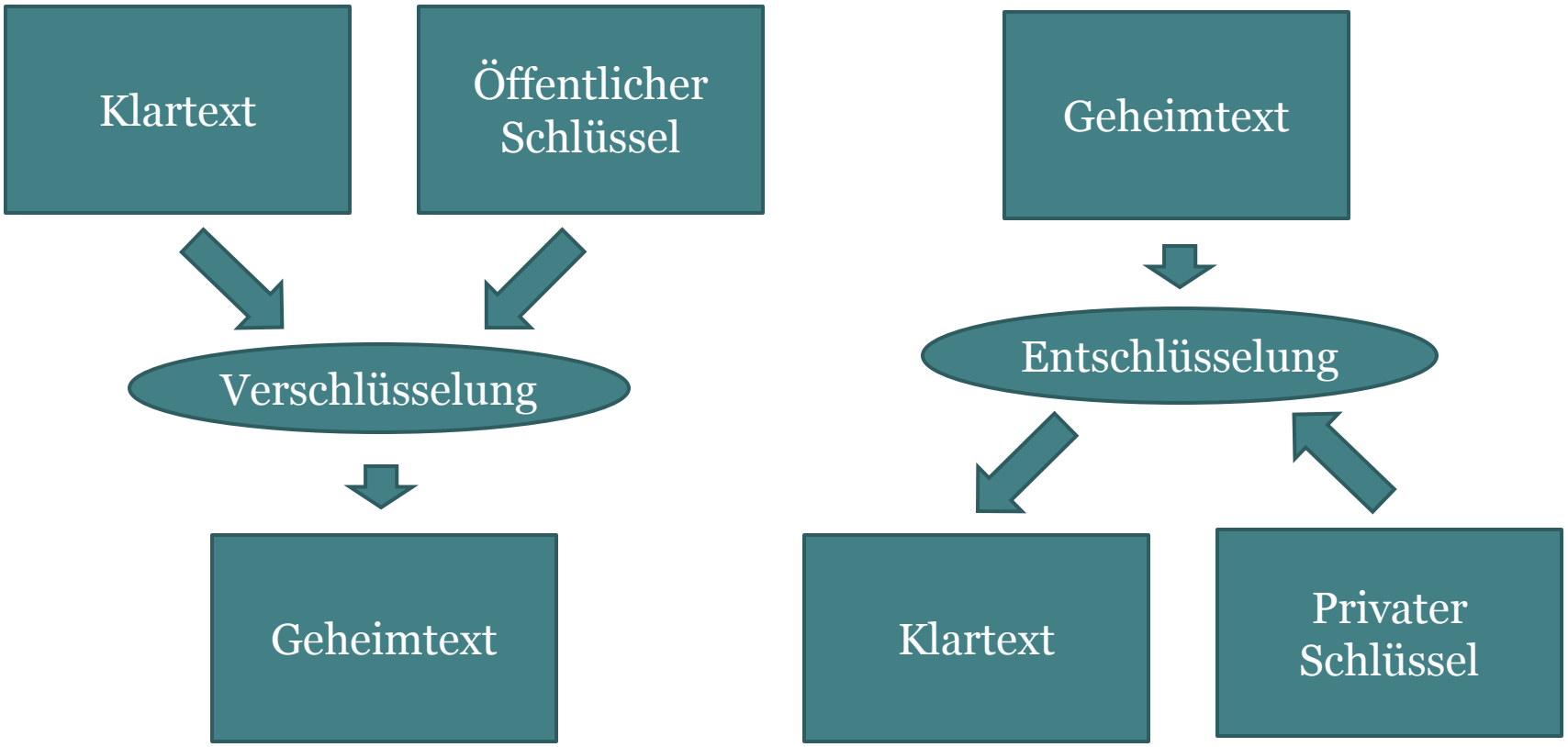
Einführung

- es handelt sich um Cryptoverfahren
- verschlüsseln und signieren von Texten
- Arbeiten mit zwei Schlüsseln

Nice Graphics

Nice Graphics

Nice Graphics



Die Schlüssel

- Public Key
  - Wird veröffentlicht
    - In der Regel auf einem Keyserver
  - Zum Verschlüsseln und Verifizieren
- Private Key
  - Wird geheim gehalten
  - Zum Entschlüsseln und Signieren
- Gehören zu einem Paar.
  - Man soll nicht von einem auf den anderen Schließen können

Die Schlüssel

- Public Key
  - Wird veröffentlicht
    - In der Regel auf einem Keyserver
  - Zum Verschlüsseln und Verifizieren
- Private Key
  - Wird geheim gehalten
  - Zum Entschlüsseln und Signieren
- Gehören zu einem Paar.
  - Man soll nicht von einem auf den anderen Schließen können

Die Schlüssel

- Public Key
  - Wird veröffentlicht
    - In der Regel auf einem Keyserver
  - Zum Verschlüsseln und Verifizieren
- Private Key
  - Wird geheim gehalten
  - Zum Entschlüsseln und Signieren
- Gehören zu einem Paar.
  - Man soll nicht von einem auf den anderen Schließen können

Vor- und Nachteile

zu symmetrischen Verfahren

Vorteile

- Verteilungsproblem: die Public Keys können einfach ausgetauscht werden
- Public Keys müssen nicht geschützt werden.

Nachteile

Vor- und Nachteile

zu symmetrischen Verfahren

Vorteile

- Verteilungsproblem: die Public Keys können einfach ausgetauscht werden
- Public Keys müssen nicht geschützt werden.

Nachteile

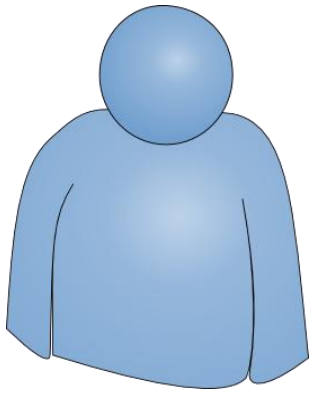
- Rechenaufwendig → langsam
- Man-in-the-middle, Schlüssel können vorgetäuscht werden

Alice & Bob

Or: „why Eve is evil“

Wer ist eigentlich Alice?

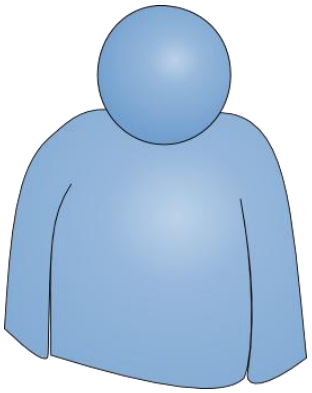
- Alice möchte Bob eine Mail senden
- Bob möchte wissen, wer die Mail gesendet hat
- Eve möchte ungewünschte und böse Dinge tun



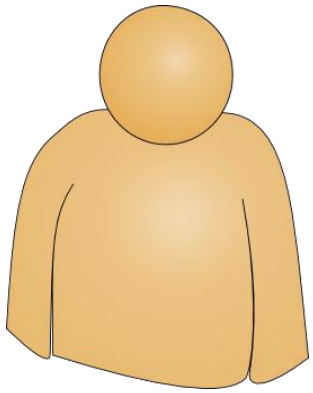
Alice

Wer ist eigentlich Alice?

- Alice möchte Bob eine Mail senden
- Bob möchte wissen, wer die Mail gesendet hat
- Eve möchte ungewünschte und böse Dinge tun



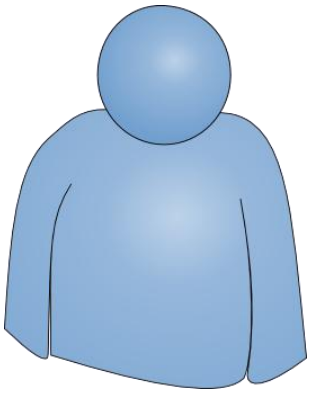
Alice



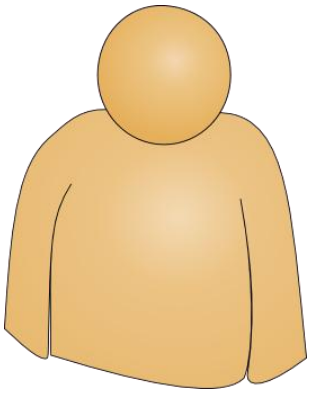
Bob

Wer ist eigentlich Alice?

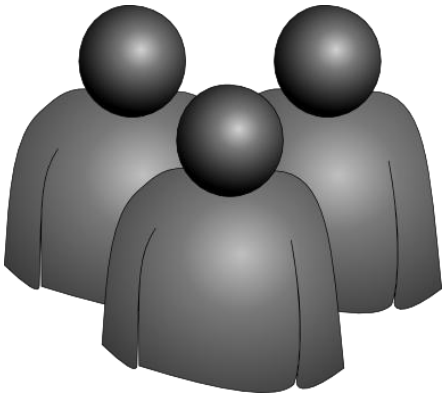
- Alice möchte Bob eine Mail senden
- Bob möchte wissen, wer die Mail gesendet hat
- Eve möchte ungewünschte und böse Dinge tun



Alice

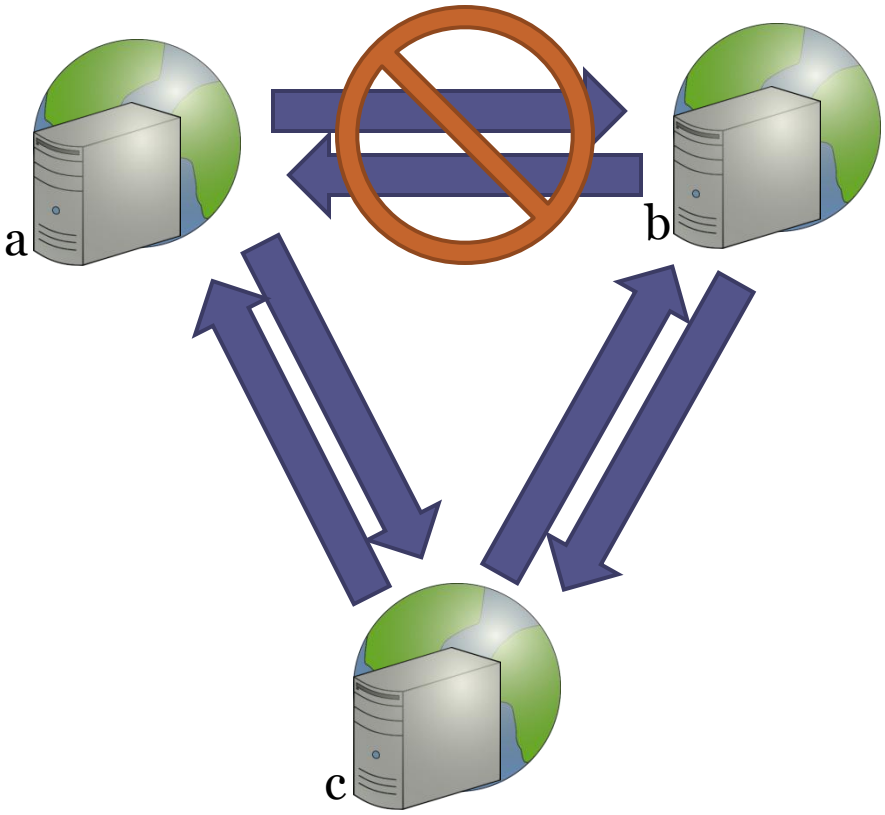


Bob



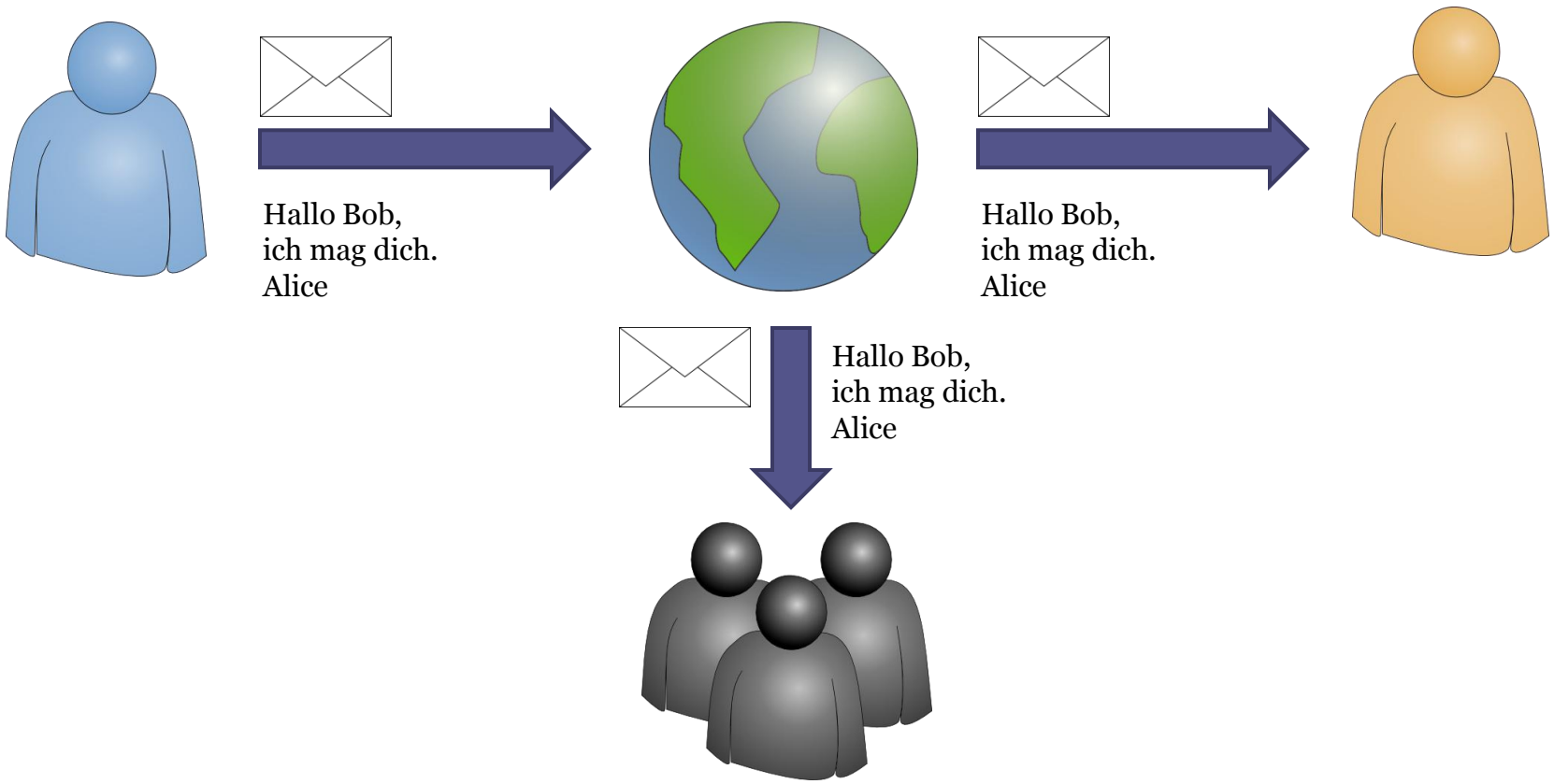
Eve

Warum Eve böse Dinge tun kann



Konventionelle Art

Eavesdropping



Eavesdropping

```
thomas@thomas-n220:~$ traceroute mail.gmx.net
traceroute to mail.gmx.net (213.165.64.20), 30 hops max, 60 byte packets
1  lo1.br10.asham.de.hansenet.net (213.191.76.25)  26.223 ms
2  ge-7-1-8-0.xd01.asham.de.hansenet.net (62.109.72.102)  38.600 ms
3  ae9-0.cr01.weham.de.hansenet.net (62.109.72.5)  47.684 ms
4  ae4-0.cr01.fra.de.hansenet.net (213.191.66.73)  80.131 ms
5  ae0-0.xd02.fra.de.hansenet.net (62.109.69.30)  79.929 ms
6  ae1-0.pr03.decix.de.hansenet.net (213.191.66.142)  64.181 ms
7  decix.bb-d.fra3.fra.de.oneandone.net (80.81.192.123)  48.739 ms
8  te-3-3.bb-d.bs.kae.de.oneandone.net (212.227.120.9)  56.781 ms
9  ae-4.gw-diste.bs.kae.de.oneandone.net (212.227.121.194)  56.580 ms
10 mail.gmx.net (213.165.64.20)  63.995 ms
```

Get out Eve

- Alice und Bob wollen nun sicher kommunizieren. Keiner soll die Nachricht:
  - Lesen
  - Verändern
  - Nochmal abschicken

  können.
- Symmetrische Verschlüsselung fällt weg, da ein sicherer Kanal für ein Passwort benötigt wird. → Public Key Verfahren

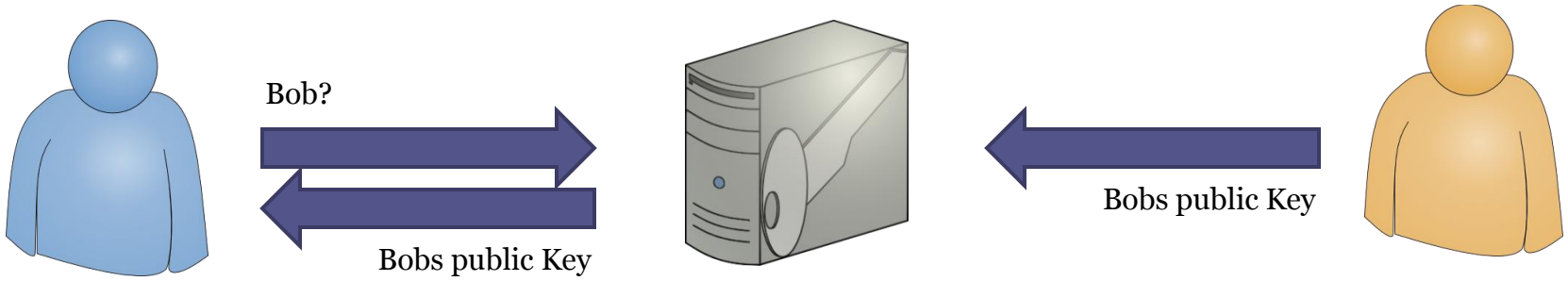
Get out Eve

- Alice und Bob wollen nun sicher kommunizieren. Keiner soll die Nachricht:
  - Lesen
  - Verändern
  - Nochmal abschicken

  können.
- Symmetrische Verschlüsselung fällt weg, da ein sicherer Kanal für ein Passwort benötigt wird. → Public Key Verfahren

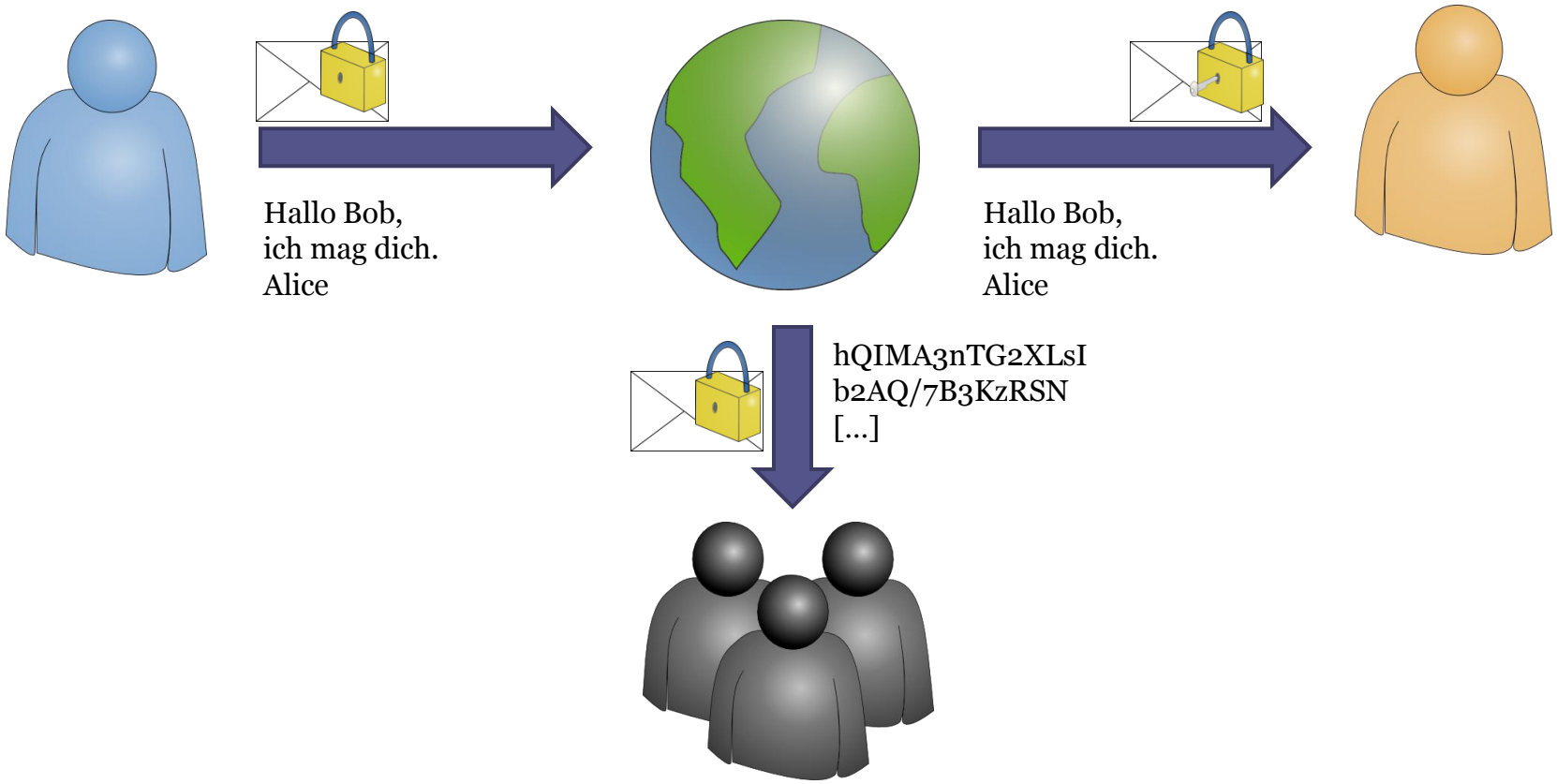
Keyserver

- Keyserver
  - Speichern öffentliche Schlüssel
  - Erlauben eine Suche nach Schlüsseln
  - Geben jedem diese Schlüssel frei raus



Verschlüsseln

Alice schickt Bob eine verschlüsselte Nachricht, Eve kann sie nicht lesen



Spoofing

Alice schickt Bob eine Mail. Eve verändert unbemerkt diese Mail

Spoofing

Eine Demonstation mit telnet

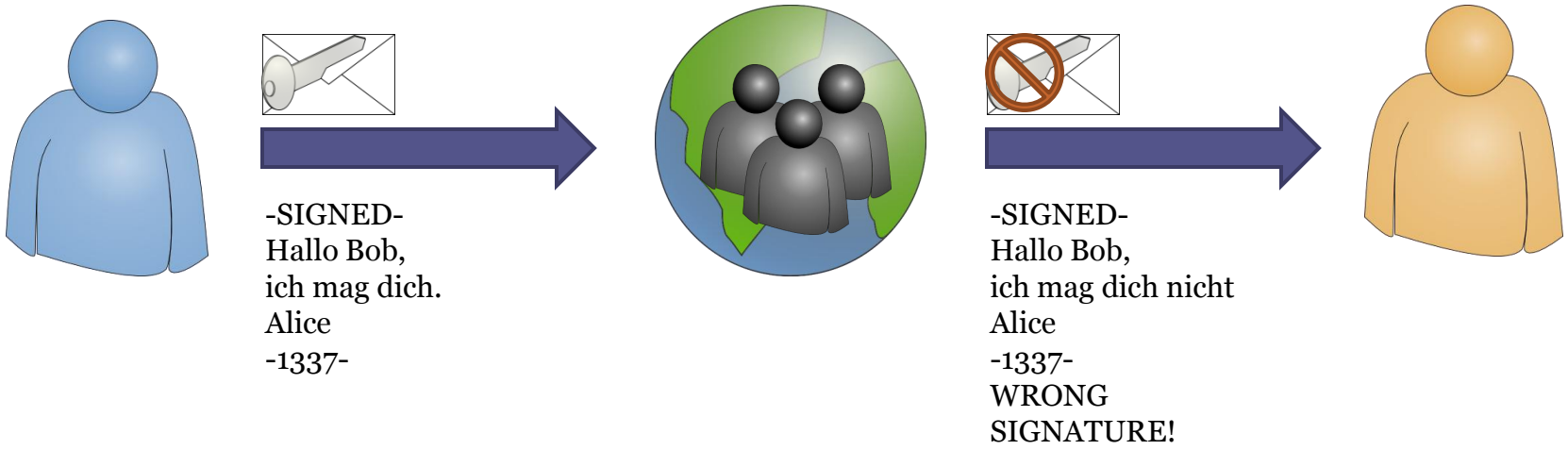
```
$ telnet mail3.netbeat.de 25
Trying 193.254.185.27...
Connected to mail3.netbeat.de.
Escape character is '^]'.
220 mail3.netbeat.de ESMTP
HELO mail3.netbeat.de
250 mail3.netbeat.de
MAIL FROM:<dekan@uni-hamburg.de>
250 ok
RCPT TO:<4tmuelle@informatik.de>
250 ok
```

```
DATA
354 go ahead
From: <dekan@uni-hamburg.de>
To: <4tmuelle@informatik.de>
Subject: Ihre Exmatrikulation
Hallo Muelli,
du bist exmatrikuliert

Pies
.
250 ok 1134425889 qp 21627
QUIT
221 mail3.netbeat.de
Connection closed by foreign
host.
```

Signieren

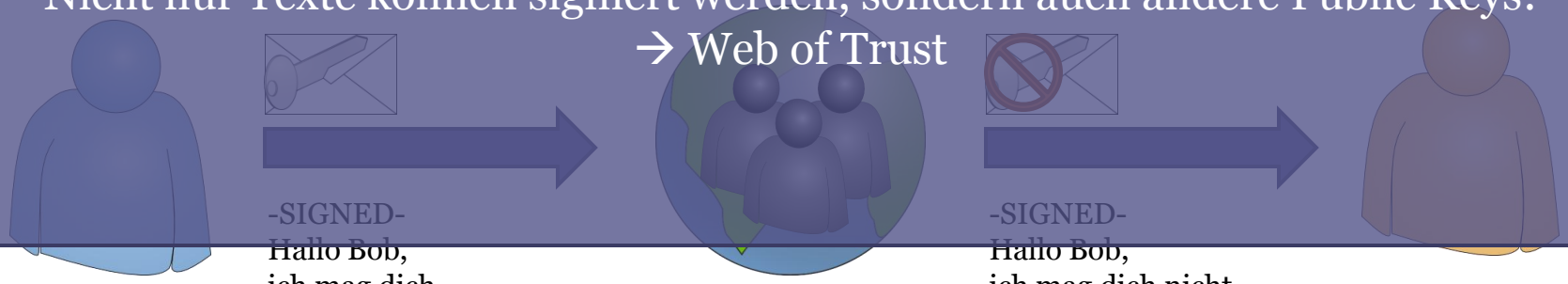
Alice signiert ihre Mail, der Hash stimmt nicht mehr → die Signatur ist ungültig



Signieren

Alice signiert ihre Mail, der Hash stimmt nicht mehr → die Signatur ist ungültig

Nicht nur Texte können signiert werden, sondern auch andere Public Keys!
→ Web of Trust

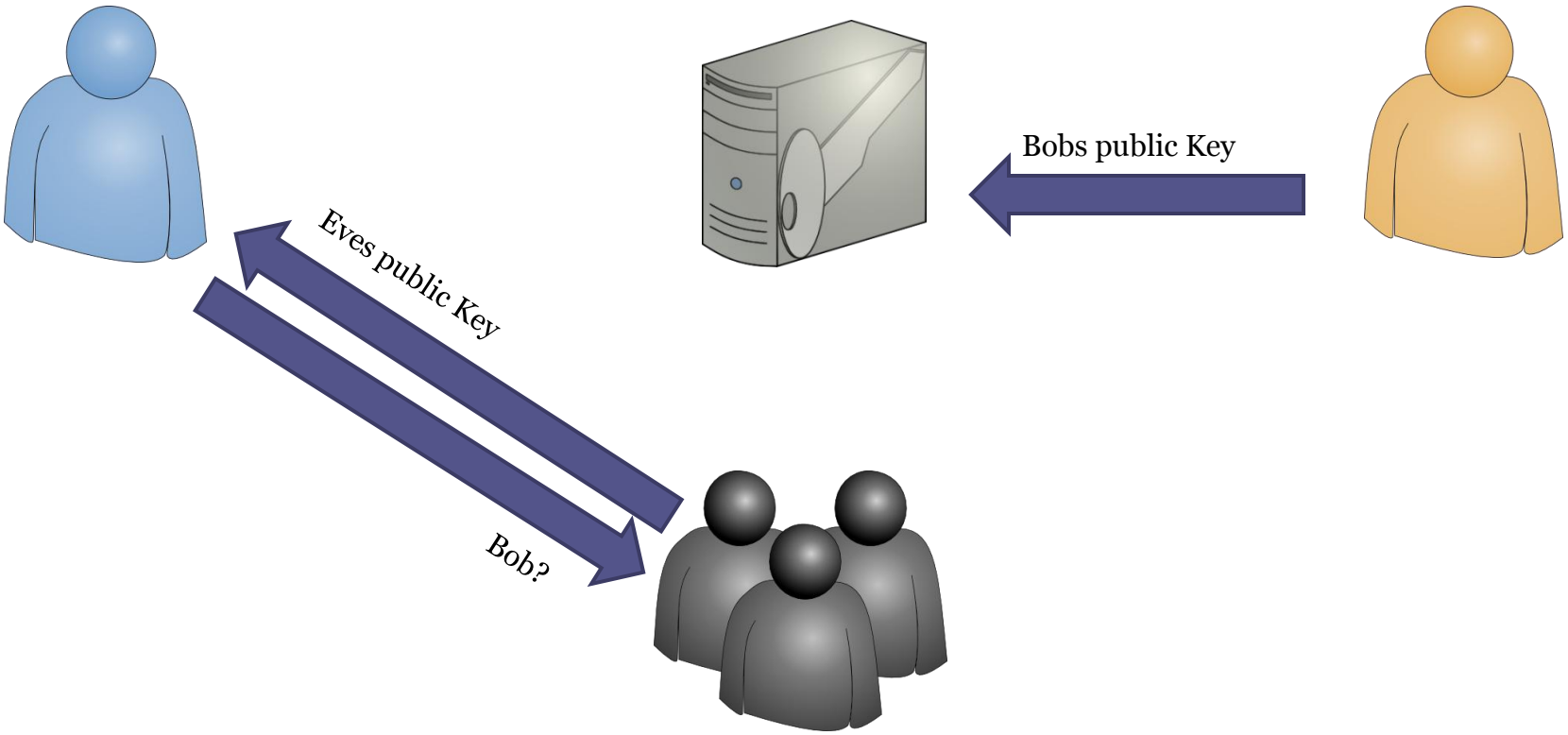


-SIGNED-
Hallo Bob,
ich mag dich.
Alice
-1337-

-SIGNED-
Hallo Bob,
ich mag dich nicht
Alice
-1337-
WRONG
SIGNATURE!

Eve mitten drin

Ein Schlüssel wird vorgetäuscht



Man In The Middle

Eine Nachricht wird vorgetäuscht

Web of Trust

Web ob Trust

- Signieren von Public Keys von Zertifizierungsstellen (Certificate Authority)
  - unflexible Struktur
  - single point of failure
- Signieren von Public Keys mit dem eigenen Private Key
  - Flexibel
  - Selbstheilend → Revocation Certigicate
  - Keinen single pint of failure

Web ob Trust

- Signieren von Public Keys von Zertifizierungsstellen (Certificate Authority)
  - unflexible Struktur
  - single point of failure
- Signieren von Public Keys mit dem eigenen Private Key
  - Flexibel
  - Selbstheilend → Revocation Certigicate
  - Keinen single pint of failure

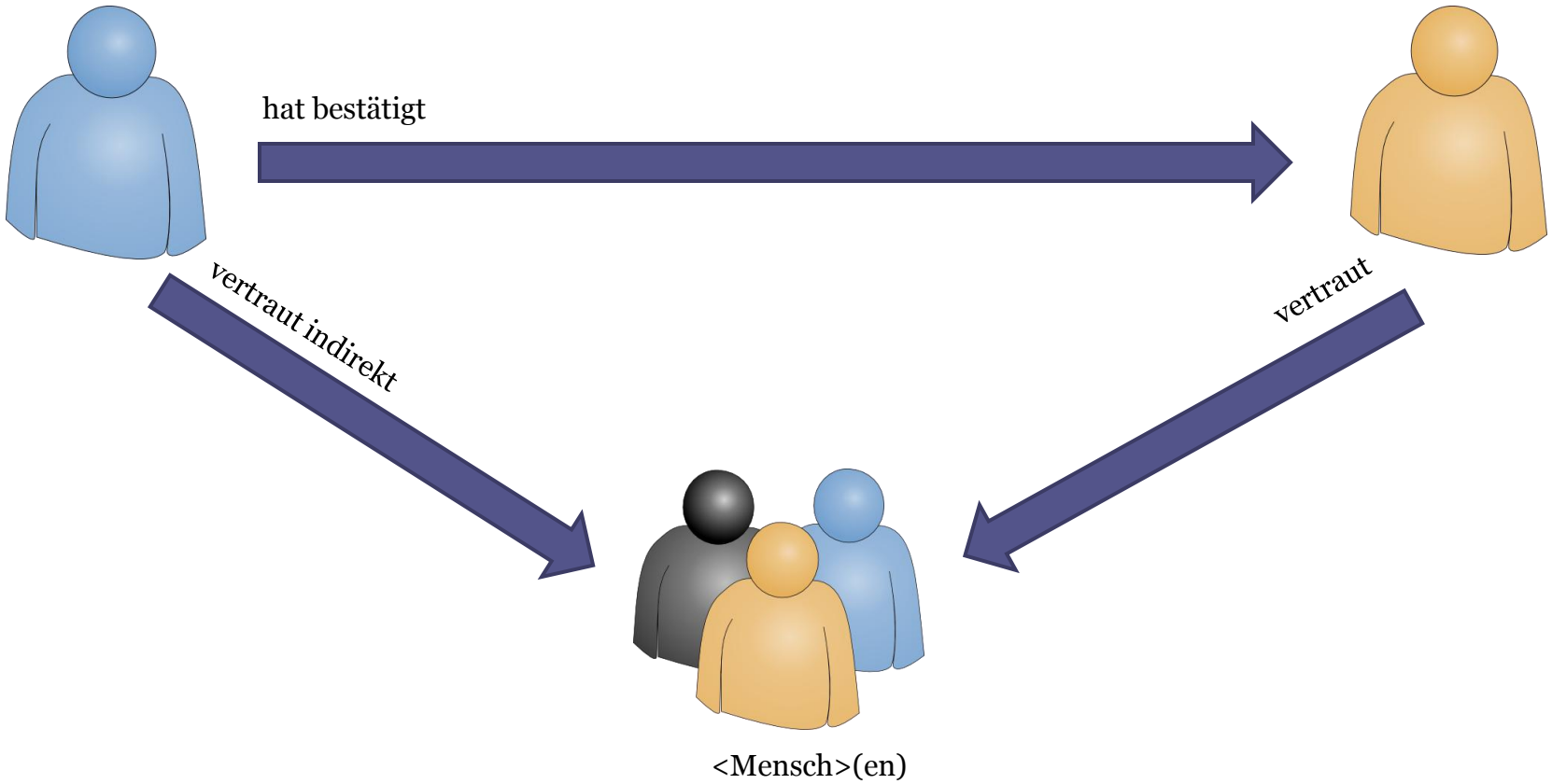
Schlüsseltausch im Web of Trust I

- Alice möchte Bob eine Mail schicken
  - Sie holt seinen Public Key vom Keyserver
  - Sie überprüft ihren Public Key durch Vergleichen des Fingerprints über einen sicheren Kanal mit Bob
  - Sie signiert Bob Public Key mit ihrem Private Key und läd diese Signatur zu einem Keyserver hoch

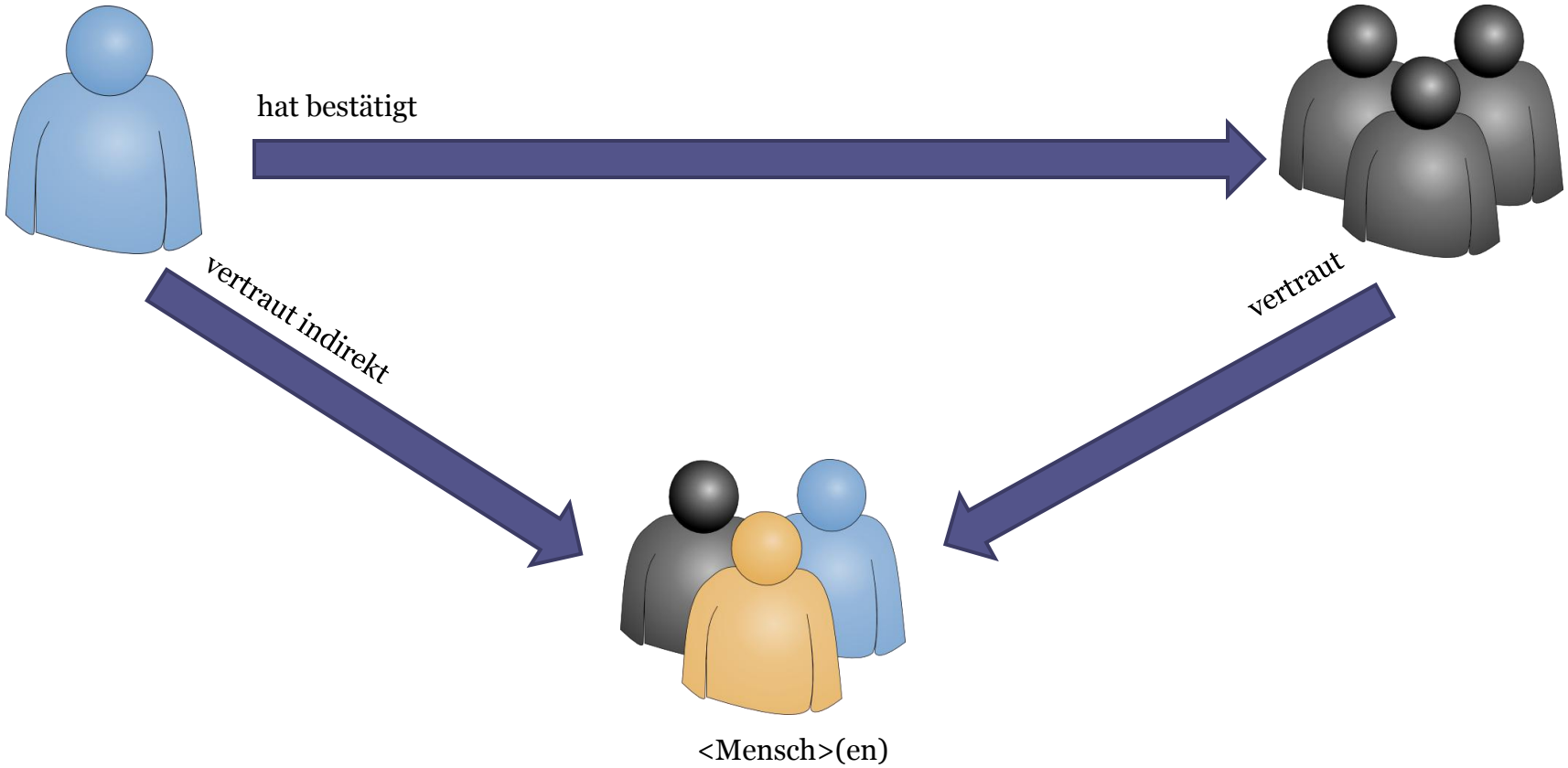
Schlüsseltausch im Web of Trust II

- Alice möchte <Mensch> eine Mail schicken
  - Sie holt <Mensch> s Public Key vom Keyserver
  - Auf dem Keyserver liegt auch die Signatur von Bob
  - Da Alice die Identität von Bob kennt und ihm zutraut, Schlüssel nur nach gründlicher Überprüfung zu signieren, muss sie die Identitätsprüfung von <Mensch> nicht wiederholen

Simples Web of Trust



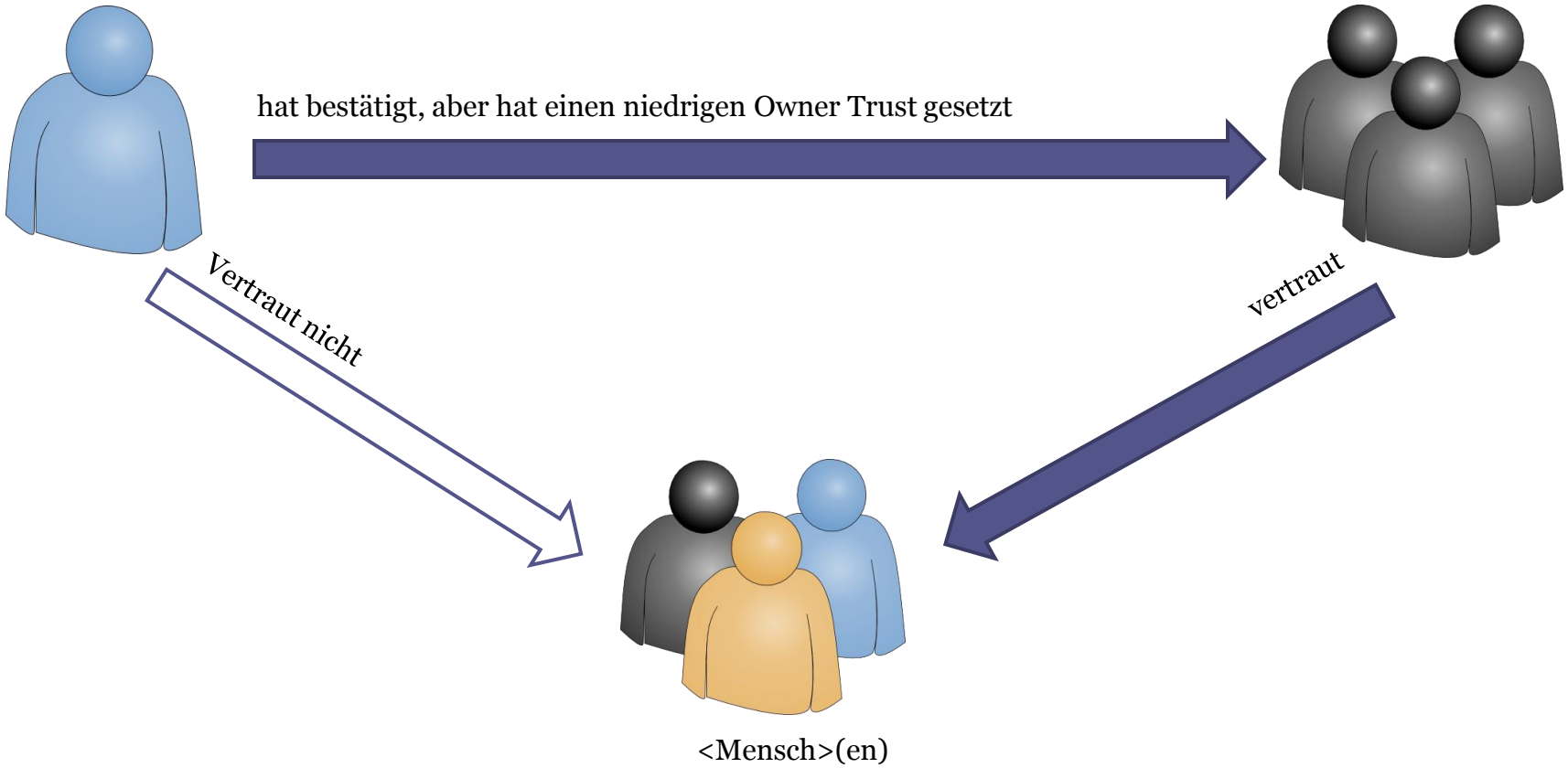
Angriff auf das WoT



Was ist Owner Trust?

- Benutzer bekommen einen „Vertrauens-Wert“ zugewiesen
- Bildet ab, wie sinnvoll jemand mit dem WoT umgeht
- Somit werden Signaturen dieses Benutzers unterschiedlich bewertet
- Wird lokal gespeichert und nicht veröffentlicht

Angriff auf das WoT



Probleme

- signaturVZ – wer verkehrt wann mit wem?
- Metadaten: Wer schreibt wem, wann eine Mail über was?
- Keine plausible deniability

Zusammenfassung

- Mit OpenPGP kann man Botschaften signieren oder verschlüsseln
- Public Key zum verschlüsseln und verifizieren von Signaturen
- Private Key zum entschlüsseln und erstellen von Signaturen
- Man kann andere Public Keys signieren

Quellen

- Cryptocampagne2010.pdf auf mafiasi.de
- http://wikipedia.org/
- http://alfie.ist.org/projects/gpg-party/pgp-party.de.html
- http://hp.kairaven.de/pgp/index.html
- man gpg