E-Mail-Verschlüsselung mit OpenPGP

Asynchrone Verschlüsselung

Tim Schlotfeldt

Webmontag, 19.07.2010

Was bringt Verschlüsselung?

Vertrauliche Kommunikation

SMTP-Dialog

```
S: 220 smtp.example.com.invalid ESMTP Postfix
C: HELO relay.example.org.invalid
S: 250 Hello relay.example.org.invalid, I am gl...
C: MAIL FROM:<bob@example.org.invalid>
S: 250 Ok
C: RCPT TO:<alice@example.com.invalid>
S: 250 Ok
C: RCPT TO:<theboss@example.com.invalid>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Hallo Alice.
C: ich kann es dir nicht per E-Mail nicht erzählen.
C: Bis später, Bob
C: ...
```

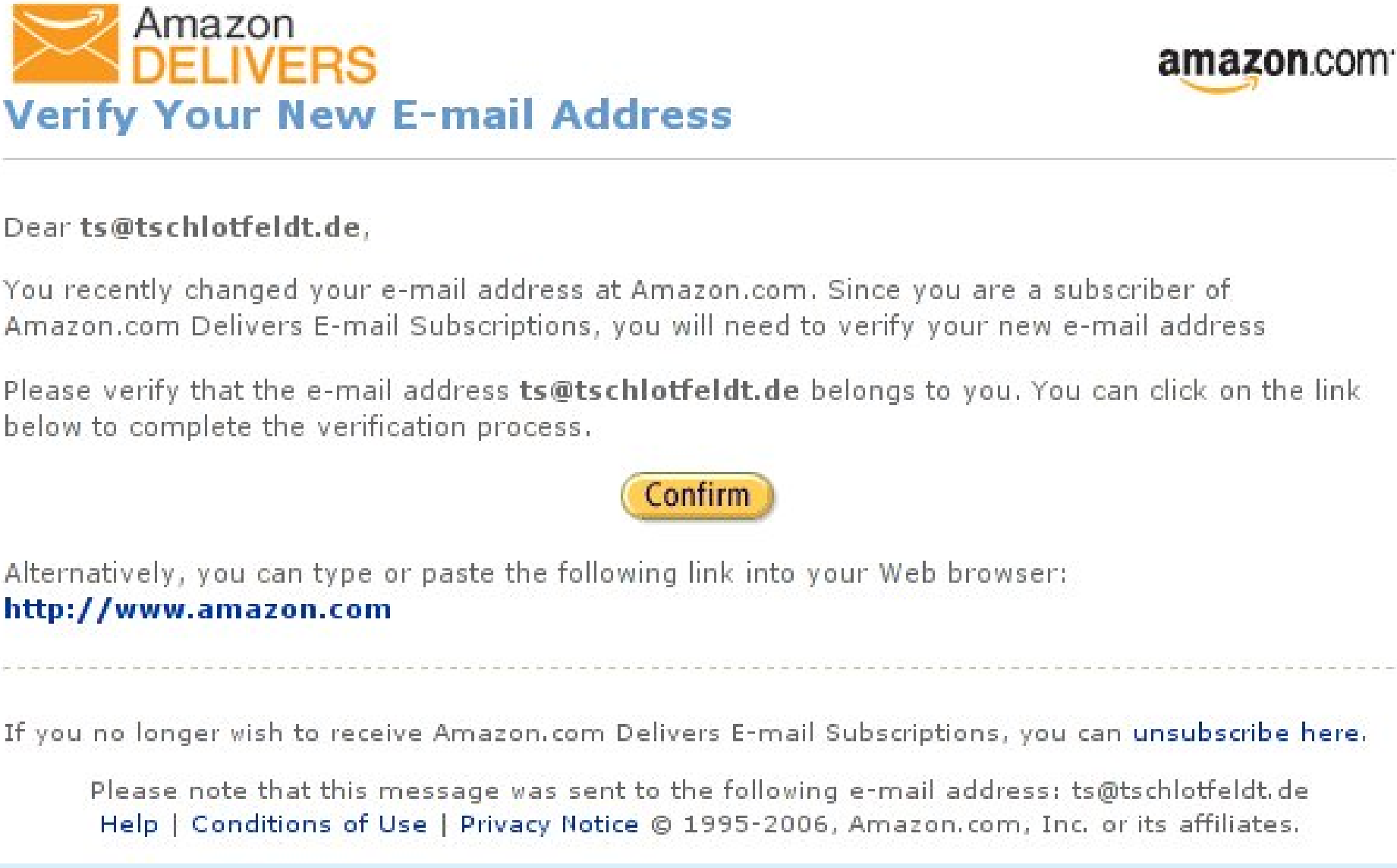
Integrität

Sehr geehrte Frau Mayer,
hiermit bestätige ich die Bestellung von 2 Laptops der Marke ...

Sehr geehrte Frau Mayer,
hiermit bestätige ich die Bestellung von 200 Laptops der Marke ...

Authentizität

Von Amazon?


Amazon DELIVERS

amazon.com

Verify Your New E-mail Address

Dear **ts@tschlotfeldt.de**,

You recently changed your e-mail address at Amazon.com. Since you are a subscriber of Amazon.com Delivers E-mail Subscriptions, you will need to verify your new e-mail address

Please verify that the e-mail address **ts@tschlotfeldt.de** belongs to you. You can click on the link below to complete the verification process.

Confirm

Alternatively, you can type or paste the following link into your Web browser:
http://www.amazon.com

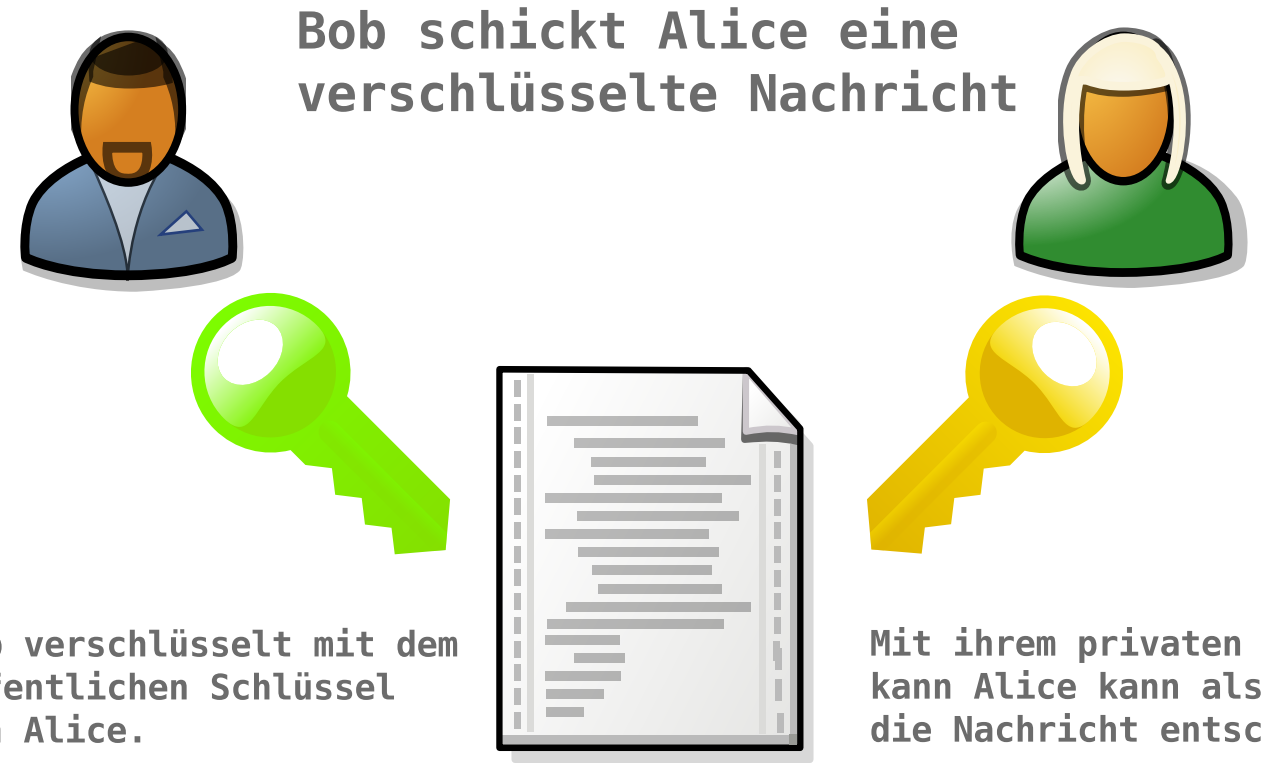
If you no longer wish to receive Amazon.com Delivers E-mail Subscriptions, you can unsubscribe here.

Please note that this message was sent to the following e-mail address: ts@tschlotfeldt.de
Help | Conditions of Use | Privacy Notice © 1995-2006, Amazon.com, Inc. or its affiliates.

Asymetrische Verschlüsselung

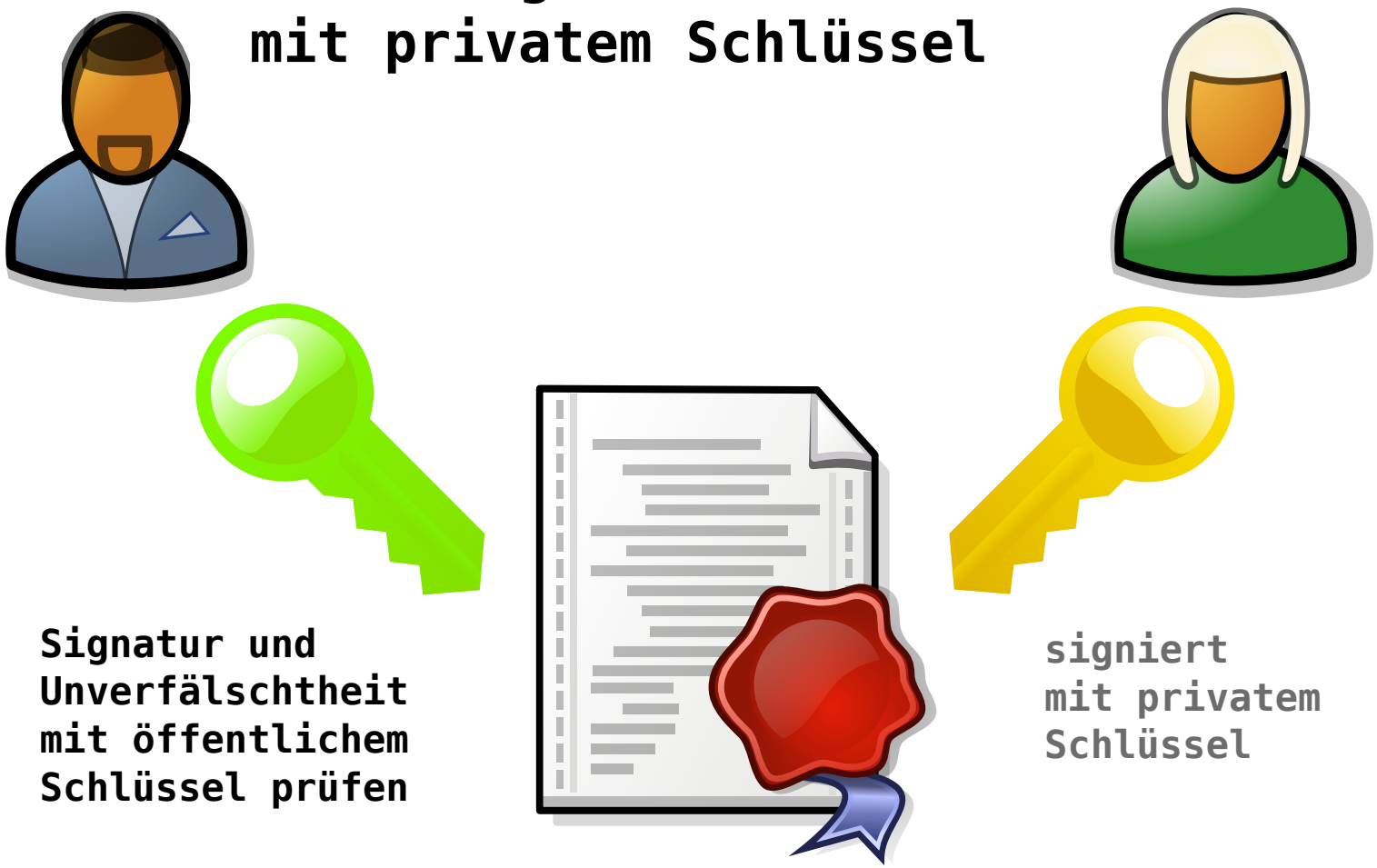
Generierung von Schlüsselpaaren

Vertraulichkeit



Integrität

Alice signiert ihre Nachricht mit privatem Schlüssel



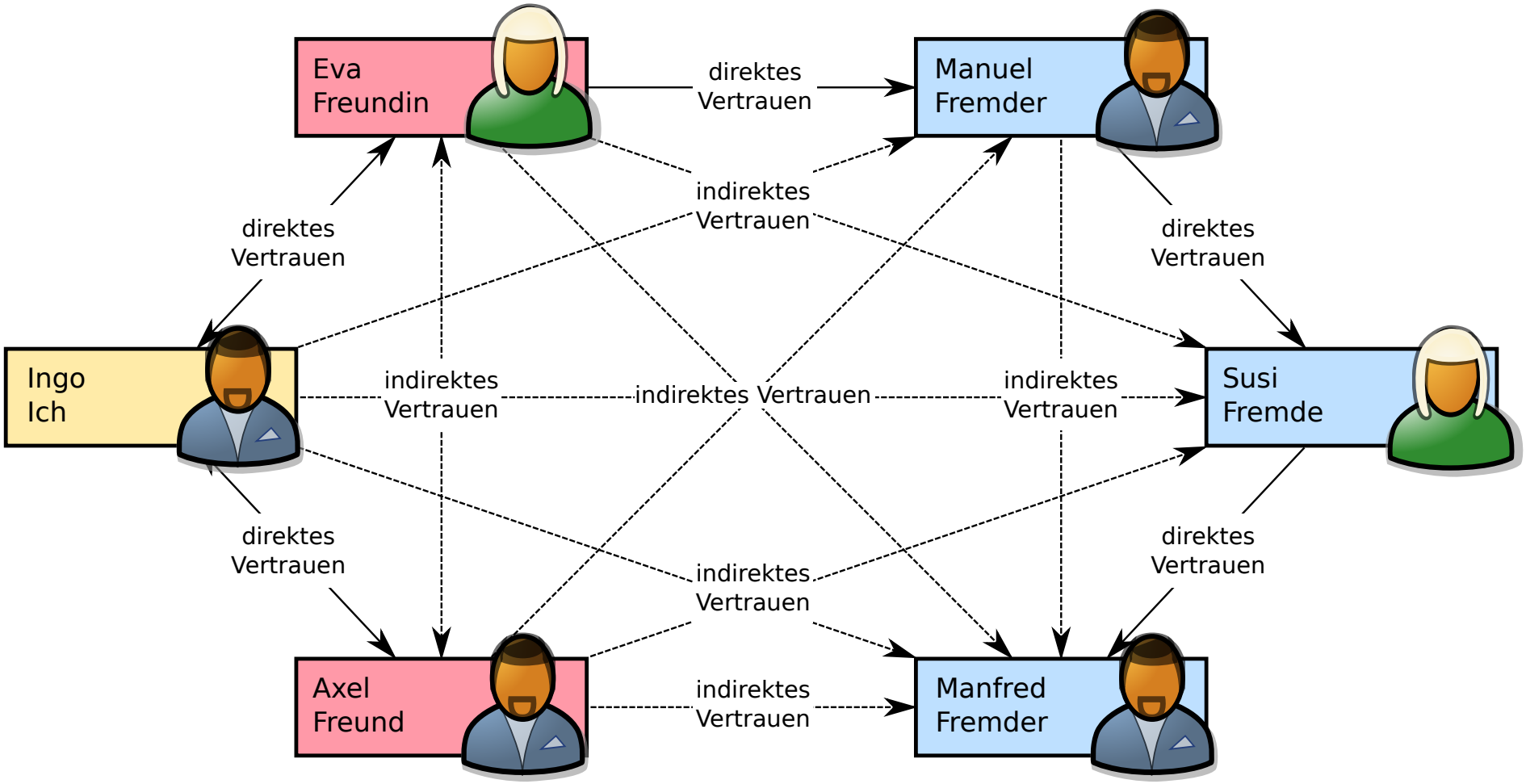
Signatur und Unverfälschtheit mit öffentlichem Schlüssel prüfen

signiert mit privatem Schlüssel

Größtes Problem ist die Sicherstellung der **Authentizität**:

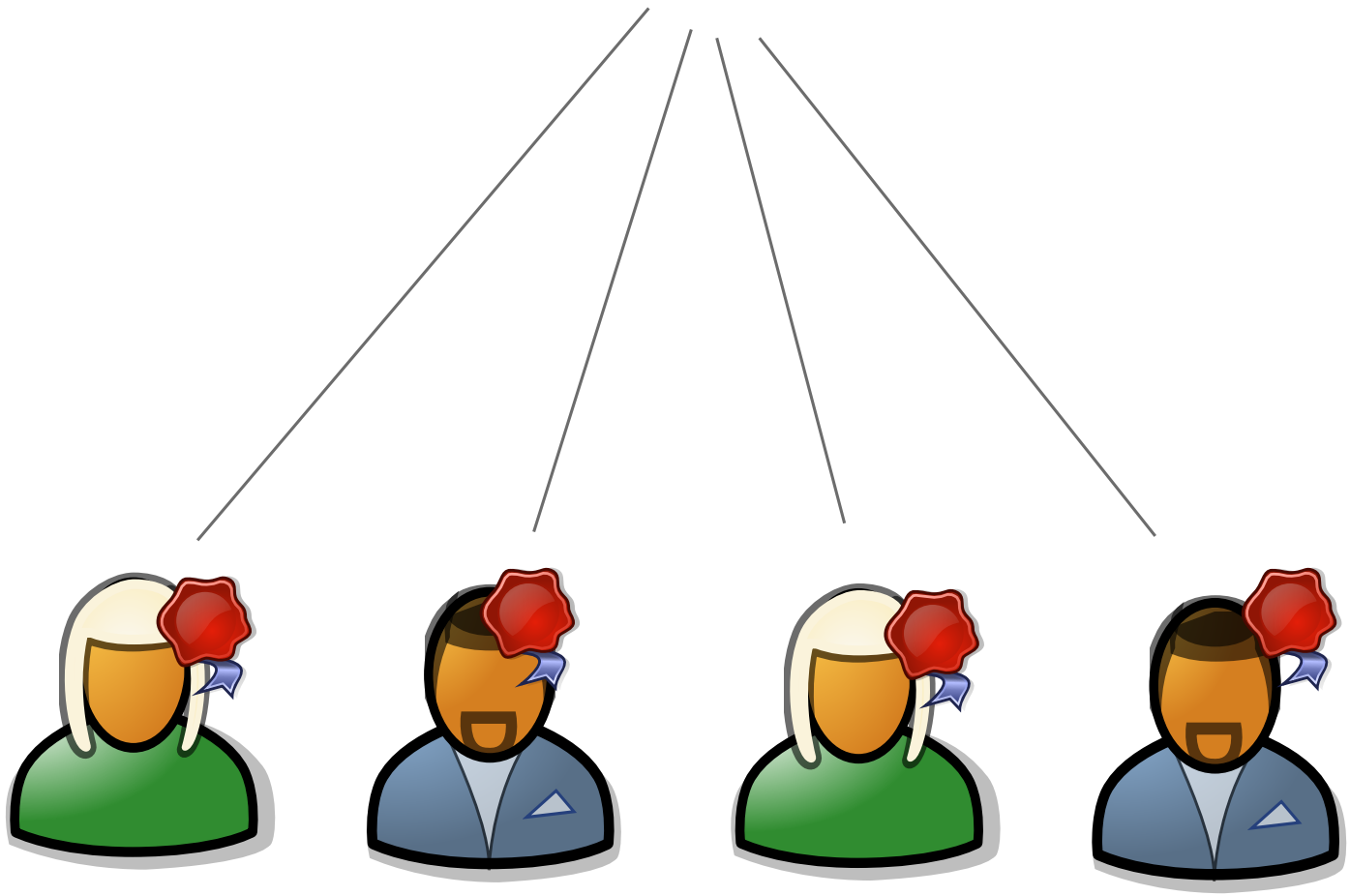
»Stammt diese Nachricht auch wirklich von Alice?«

OpenPGP: Web of Trust



Quelle: Wikipedia

S/MIME: Zentrale Zertifizierungsstellen



Herzlichen Dank!