Using PGP/GnuPG and S/MIME w

Tilman Linneweh <tilman@arved.de

Introduction:

- PGP/GnuPG
- The Web of Trust
- S/MIME
- Certificate Handling
- Summary

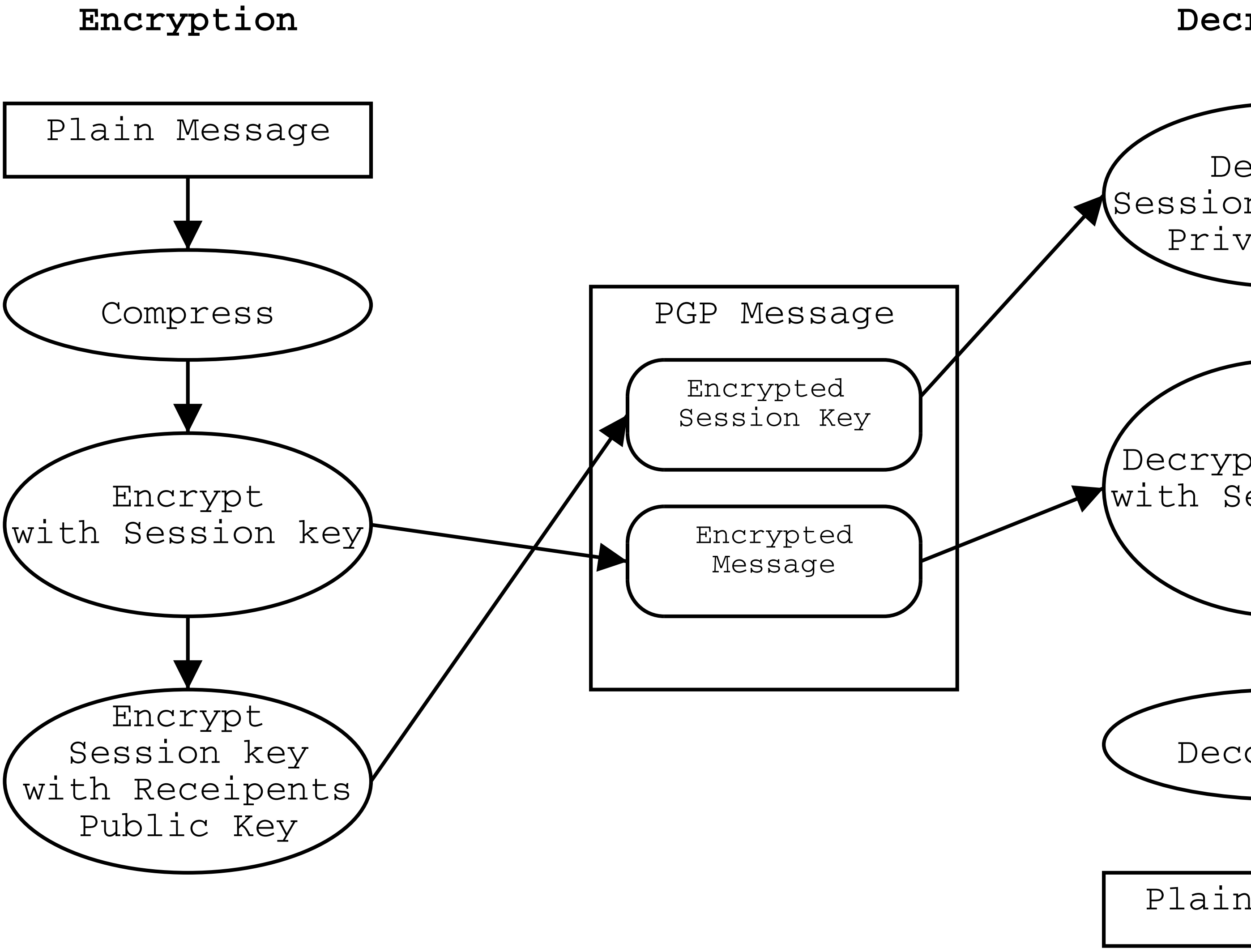
Email is insecure:

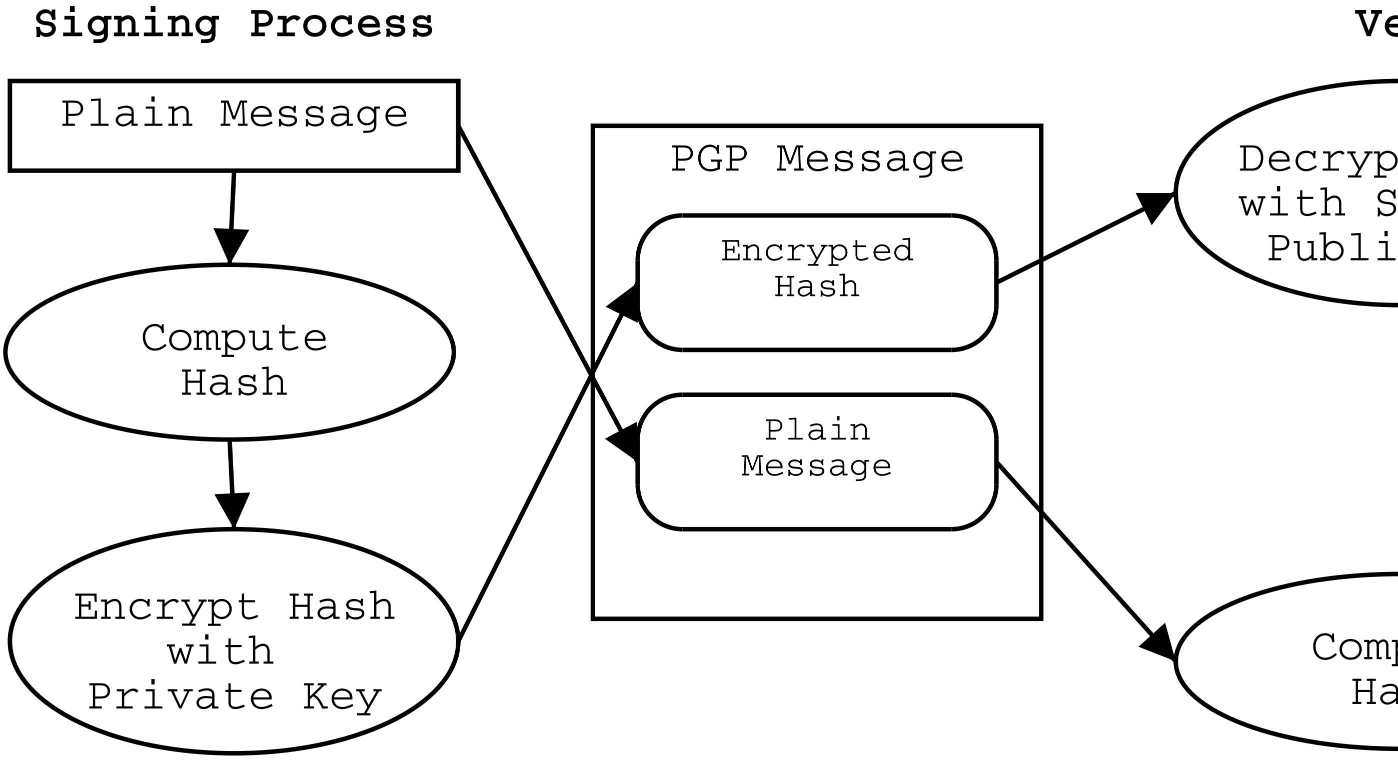
- Messageformat in cleartext.
- No authentication of the Sender

That's why we need Public Key encryption in Emai

PGP History:

- 1991 Phil Zimmermann released ”Pretty Good
  - violated patents for RSA and IDEA algorithm
  - illegal exported from the USA
- 1997 PGP 5.0 released by PGP Inc., exported from the U
- 1998 RFC 2440 Definition of the OpenPGP Message For
- 1999 Werner Koch released the ”GNU Privacy Guard” (G


Encryption
Decr
Plain Message
Compress
Encrypt
with Session key
Encrypt
Session key
with Receipents
Public Key
PGP Message
Encrypted
Session Key
Encrypted
Message
De
Sessio
Priv
Decryp
with Se
Deco
Plain


Signing Process
Ve
Plain Message
Compute Hash
Encrypt Hash with Private Key
PGP Message
Encrypted Hash
Plain Message
Decryp with S Publi
Comp Ha

On the Internet, nobody knows you're a

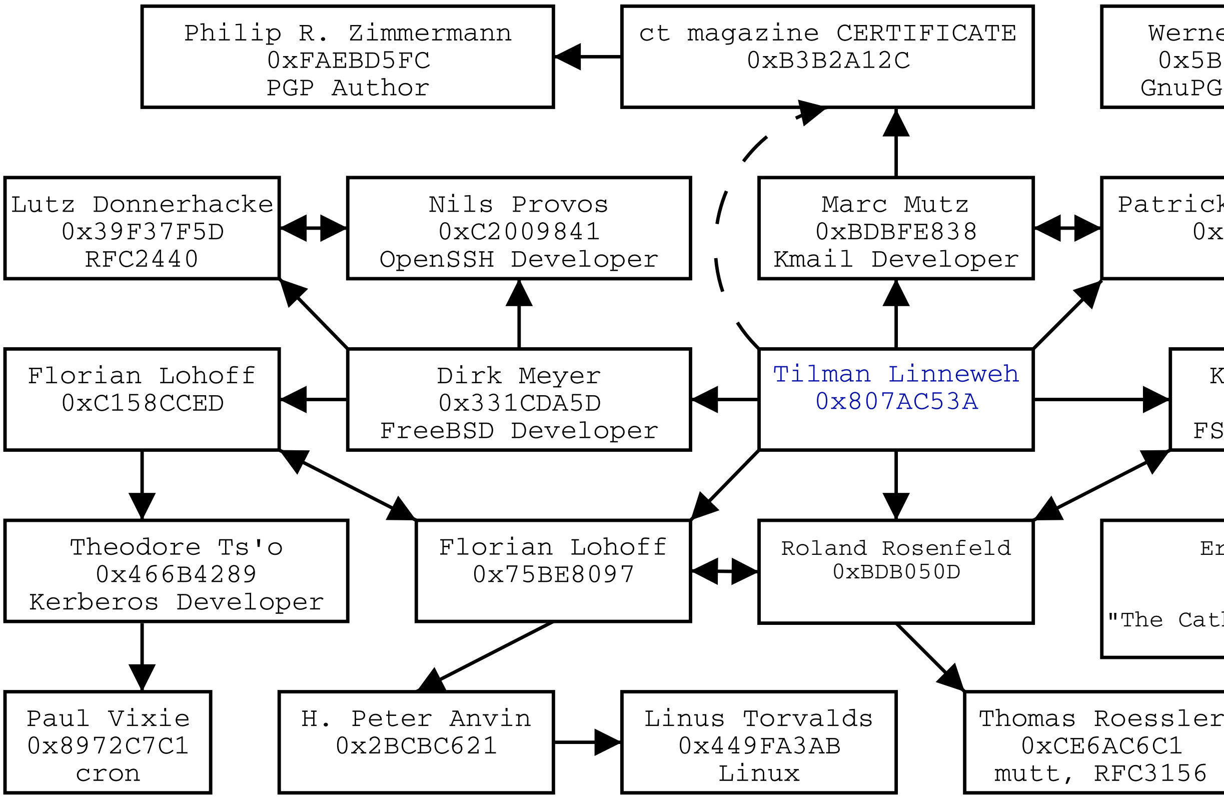
How can Alice determine, if the PGP Key ”Bob” i

Alice's possibilities:

- Meet Bob in Reallife and exchange keys
- Exchange via letter or telephone
- Exchange via a third person both trust.

```
pub  1024D/807AC53A 2002-06-03 Tilman Linneweh <arved@FreeBS
     Key fingerprint = A92F 344F 31A8 B8DE DDFA  7FB4 7C22 C
uid                            Tilman Linneweh <tilman@arved
uid                            Tilman Linneweh <e0025974@stu
uid                            Tilman Linneweh <linneweh@zid
uid                            Tilman Linneweh <arved@arved.
sub  1024g/FA351986 2002-06-03 [expires: 2004-06-02]
```

The Web of Trust



Philip R. Zimmermann
0xFAEBD5FC
PGP Author

ct magazine CERTIFICATE
0xB3B2A12C

Werne
0x5B
GnuPG

Lutz Donnerhacke
0x39F37F5D
RFC2440

Nils Provos
0xC2009841
OpenSSH Developer

Marc Mutz
0xBDBFE838
Kmail Developer

Patrick
0x

Florian Lohoff
0xC158CCED

Dirk Meyer
0x331CDA5D
FreeBSD Developer

Tilman Linneweh
0x807AC53A

K
FS

Theodore Ts'o
0x466B4289
Kerberos Developer

Florian Lohoff
0x75BE8097

Roland Rosenfeld
0xBDB050D

Er
"The Catl

Paul Vixie
0x8972C7C1
cron

H. Peter Anvin
0x2BCBC621

Linus Torvalds
0x449FA3AB
Linux

Thomas Roessler
0xCE6AC6C1
mutt, RFC3156

Problems:

- Older Version of PGP are using different algori versions.

- Broken MTAs damage signatures

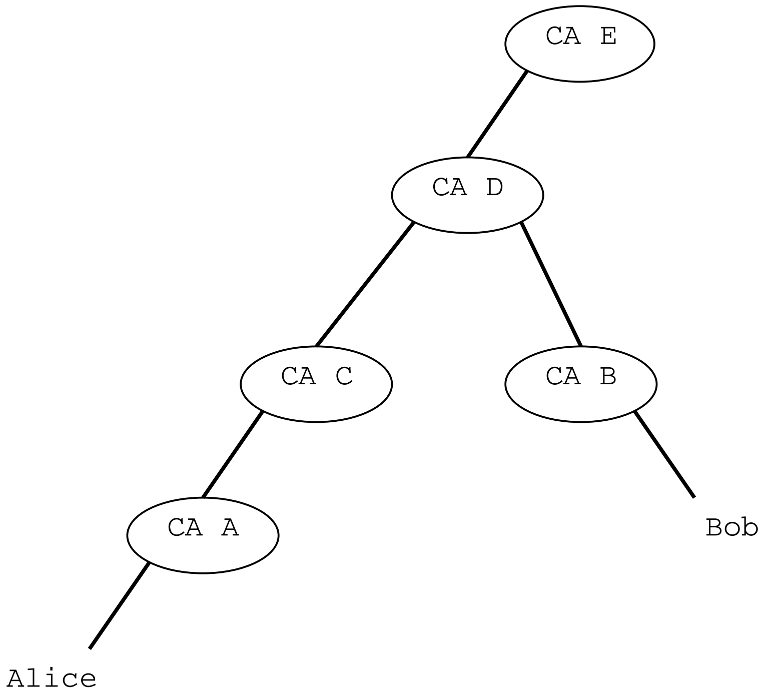
- Two incompatible Standards: PGP inline and P

inline-PGP	*PGP/MIME*
RFC 2440	RFC 3156
text/plain	multipart/encrypted
easier to implement	integration into the
only 7bit ASCII	Attachments & Cha
works with: Outlook, pine...	Eudora, mutt...

S/MIME History

- 1995 RSA Data Security Inc. started develop standard
  - based on X.509
  - extends MIME (data format used to send email)
- 1998 S/MIMEv2
- 1999 S/MIMEv3 released by the IETF S/MIME

Certificate handling:



Problems:

- Smaller Userbase than PGP
- Not every MUA speaks S/MIME
- A certificate costs $$$

Summary:

- Use of Encrypted Email will increase
- Still no Killer Application for Encrypted Email.
- Both standards will coexist, since they have diff