PGP keysigning

Andrew Cormack
and friends
Why?

Two functions of PGP

- to send secret information
- to prove origin

Already know a message relates to a key

- but not a person

Here establish identity of owner

Trust can be done later, by e-mail
How?

Now

Later
What to sign?

Key looks like this

- mQENAzbbyOwAAAEIALIR3zaj1EL+SyQ46ug7JKHRNSvtXzEymiMnt1Cwn+j3rK0cUIHHoeVCFF6klgr7kzJ7O80li9ySob/Djsh3W644nih1xglFJwT2AMtdfZ6TV3djQRKO8U6d9QNcNrg0gpf/KmX0iugOHJGY3DY5cLbvjZ7cMkP+GTOAReF/30l...

Fingerprint - a 128 bit hash value is better

- DDC3 B5E4 FF84 0BD3 F290 FD48 B73D 1AD9
Trusted Introducers

Follow documented procedure
Verify individuals’
  ■ Identity
  ■ Ownership of key
Sign keys which have been verified
Distribute signed keys to participants
Participants

May rely on trusted introducers

- and sign keys which have been signed by them
- if they are satisfied with the procedure
- and believe it has been followed correctly

Or may do their own verification

- using whatever protocol they choose