Digitally Signing email Why, how ?

Ludovic Hirlimann

Why

- Protects your online identity

- Gives you the power to protect sensible data

- It's not a solution against spam

Signing

- Creates a checksum of the email

- Checksum is based on a Key + content

- Adds that checksum

- Decodes and verifies checksums

How Cert

Demo

How PGP

Demo

Web Of Trust

Works for both system

Is an easy way to give a level of trust to an unknown signature.

Reference

PGP/GPG - http://www.gnupg.org/documentation/faqs.en.html

Digital certificates - http://en.wikipedia.org/wiki/Public_key_certificate

RFC 4880 for PGP and 5751 for S/MIME