

Assignment 2

PGP/GPG, S/MIME, Digital Signatures and
Anonymity

Kristoffer Björklund and Nikolaos Papadopoulos

kb222wa@student.lnu.se & np222fc@student.lnu.se

Tools and Requirements

- A capable mail client: Thunderbird
- Supporting applications to work with certificates: OpenSSL
- PGP/GPG apps, additional add-ons.. Figure out what you need!
- Two classmates for correspondence.
- GNU/Linux system
- 9 PAGE LIMIT INCLUDING REFERENCES

Pretty Good Privacy / GNU Privacy Guard

- Created by Phil Zimmerman
- OpenPGP standard → You can read more in RFC 4880
- GNU Privacy Guard as an alternative
- Requires installation of additional software
- KGpg - GUI if someone want to use it

GPG

- You will work with different key-servers
- Old vs New generation
- When sending email to your instructors, make sure both will receive the content

Secure/Multipurpose Internet Mail Extensions

- Defined by the Internet Engineering Task Force(IETF)
- You will need software for encrypting emails

Useful Links

- [GnuPG](#)
- [Mozilla Thunderbird](#)
- [Enigmail](#)
- [A key-server](#)
- [Another key-server](#)

The background features a dark blue gradient. On the left side, there are several horizontal, slightly blurred light trails in shades of cyan and blue, suggesting motion or data flow. A bright orange and yellow lens flare is positioned on the left, overlapping the light trails. A trail of small, glowing blue dots curves from the top left towards the center, resembling a particle path or a data stream.

Questions?