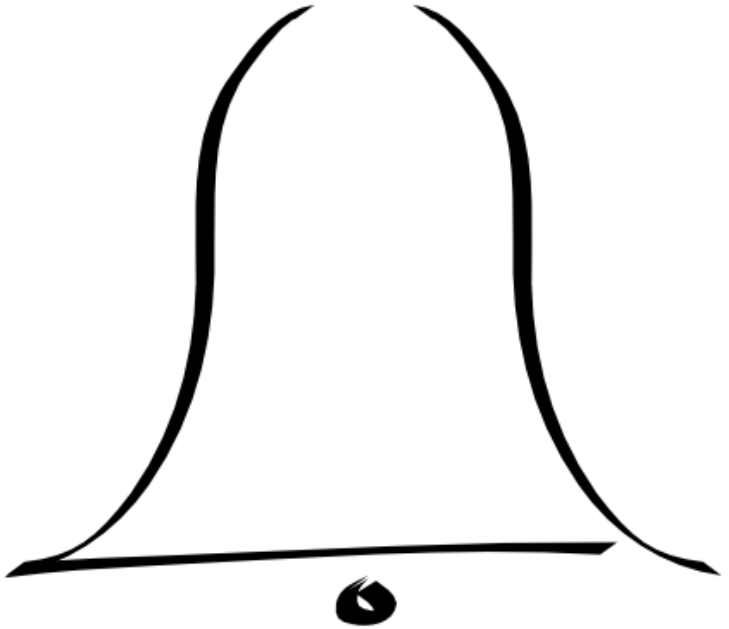
13/08, 8 anos do SoftwareLivreVS

SoftwareLivreVS



Grupo de Usuários de Software Livre do Vale do Rio dos Sinos

www.softwarelivre-vs.org

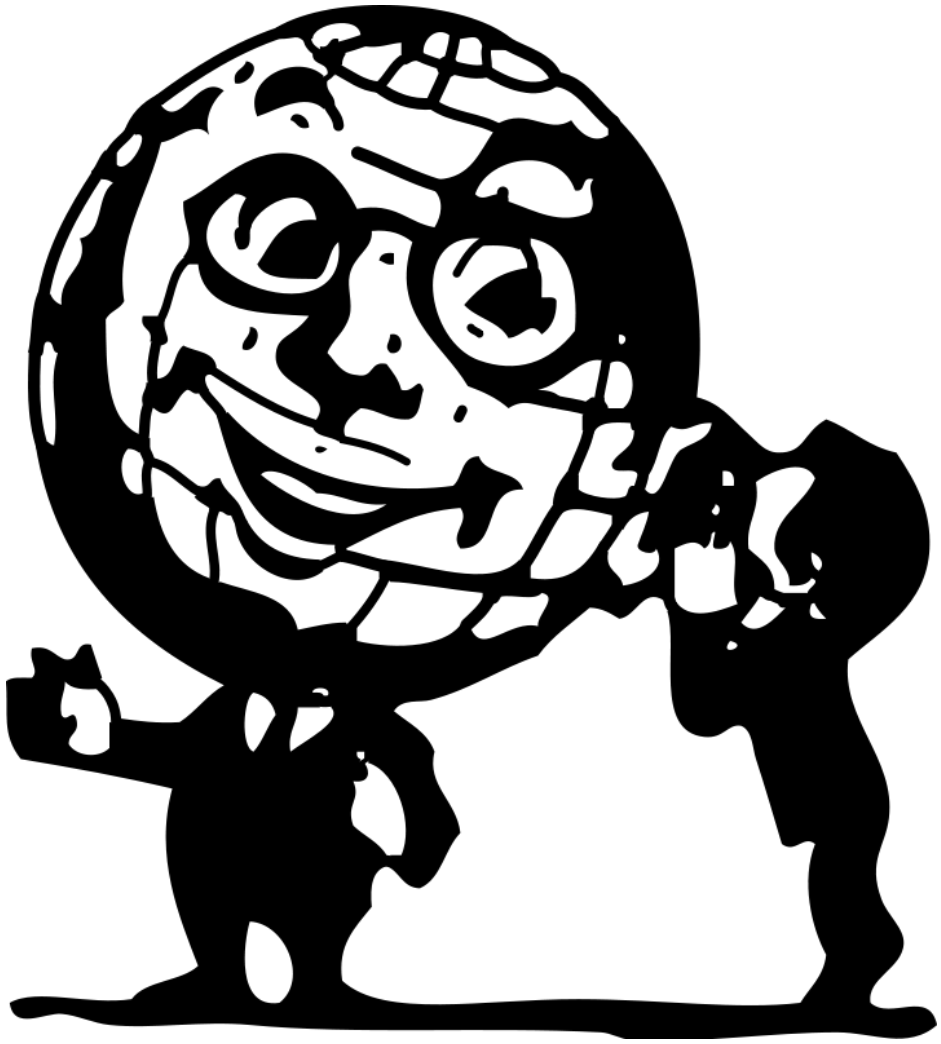
16/08, 20 anos do Debian

27/09, 30 anos do GNU

28/09, Dia da Liberdade de Software

Festa de Assinatura de Chaves OpenPGP

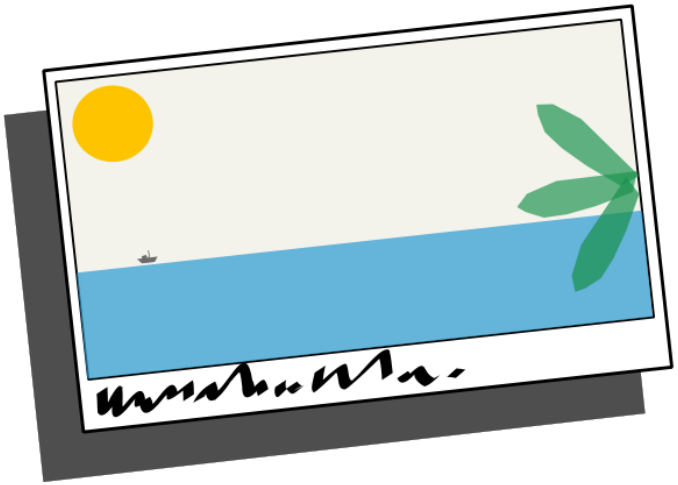
OpenPGP para iniciantes



Você sabe com quem está falando?

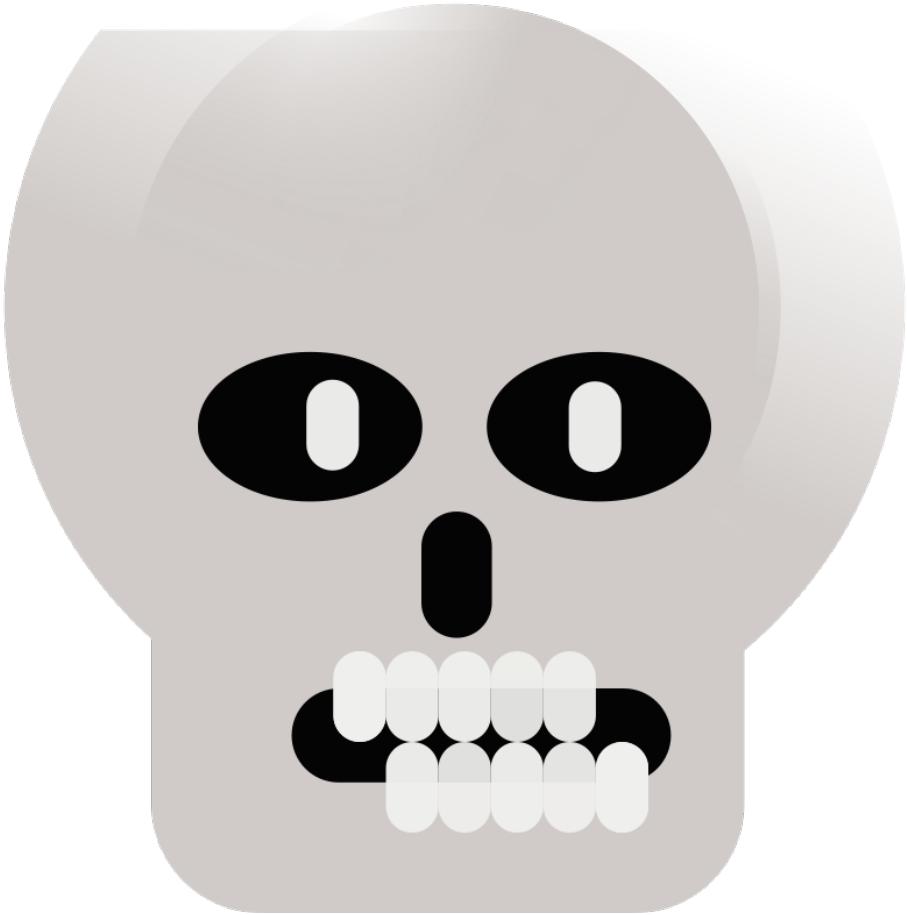
Privacidade no e-mail com OpenPGP para iniciantes

O problema



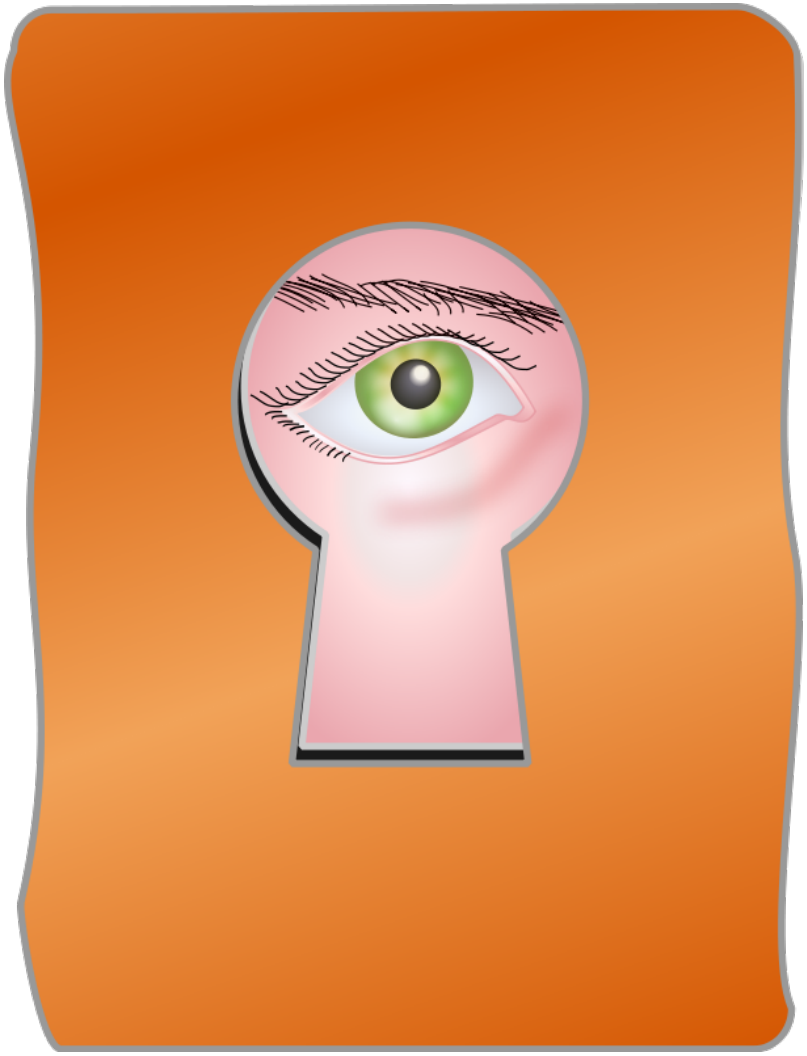
- E-mails não são seguros:
  - Texto plano
  - Sem controle de integridade
  - Podem ser:
    - Interceptados
    - Lidos
    - Modificados

O problema



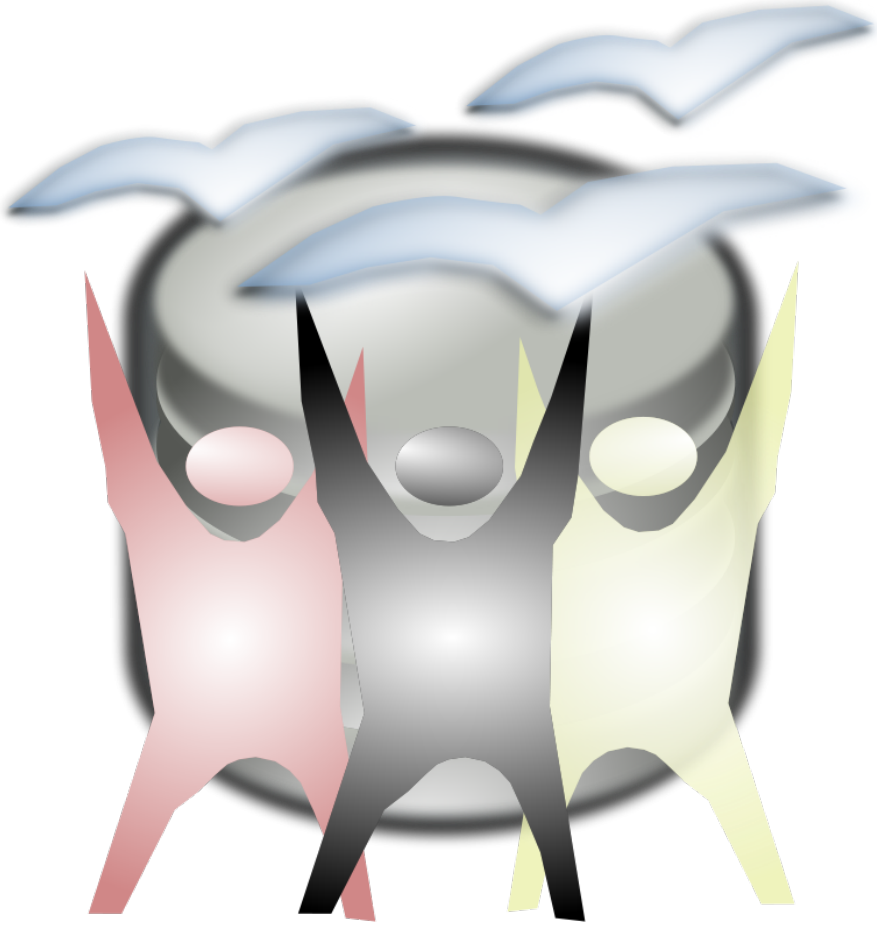
- É impossível ter certeza de:
  - Quem enviou o e-mail
  - Que somente será lido por pessoas autorizadas
  - Que não foi modificado

Por que se importar?



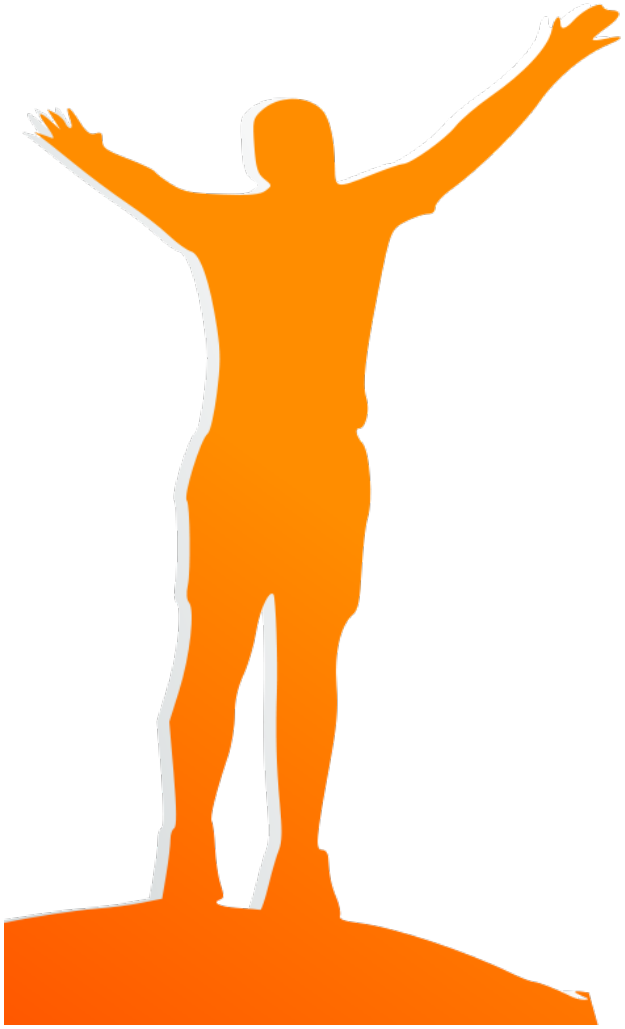
- É pessoal.
- É privado.
- É da sua conta, e de mais ninguém.
- Não há nada de errado em assegurar a sua privacidade.

Declaração dos Direitos Humanos



Artigo XII - ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

Constituição Brasileira

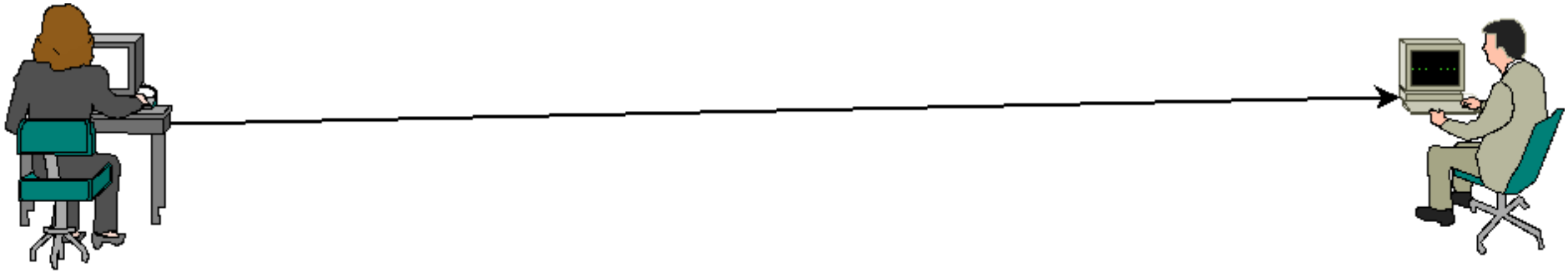


Art. 5º, XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

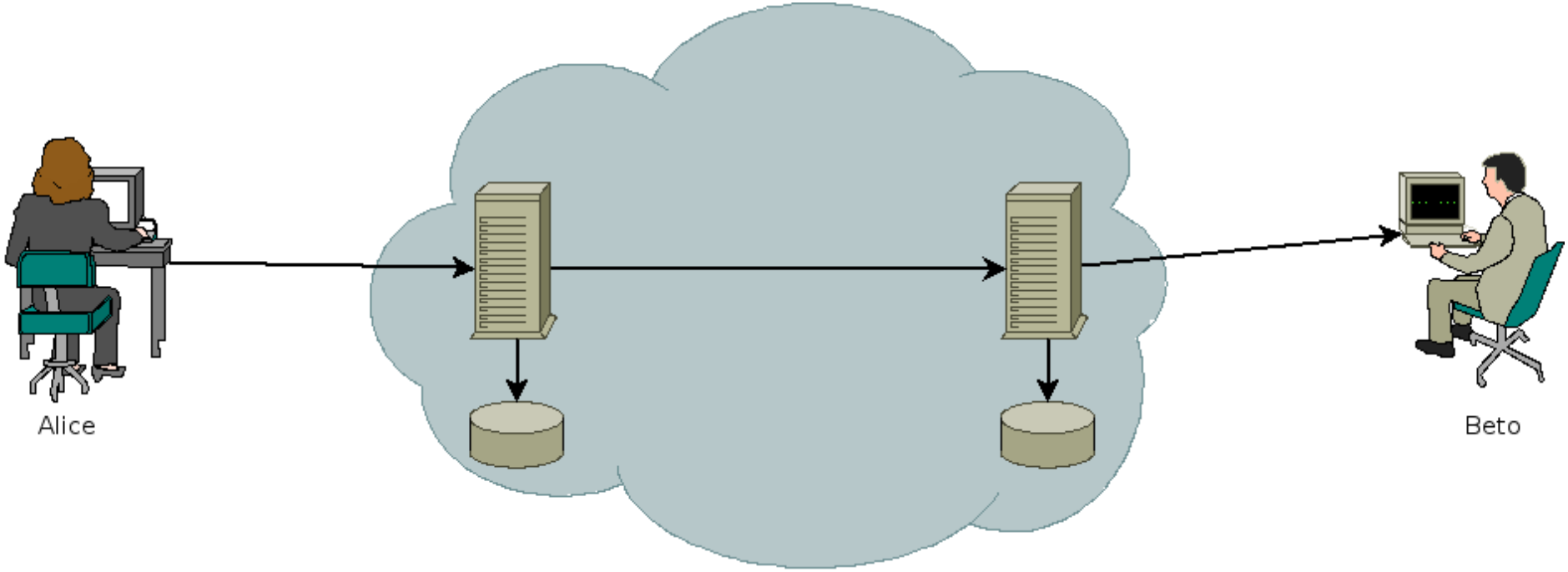
Defenda a sua privacidade!

- Privacidade é um direito seu!
- Faça você mesmo, não espere pelos outros!

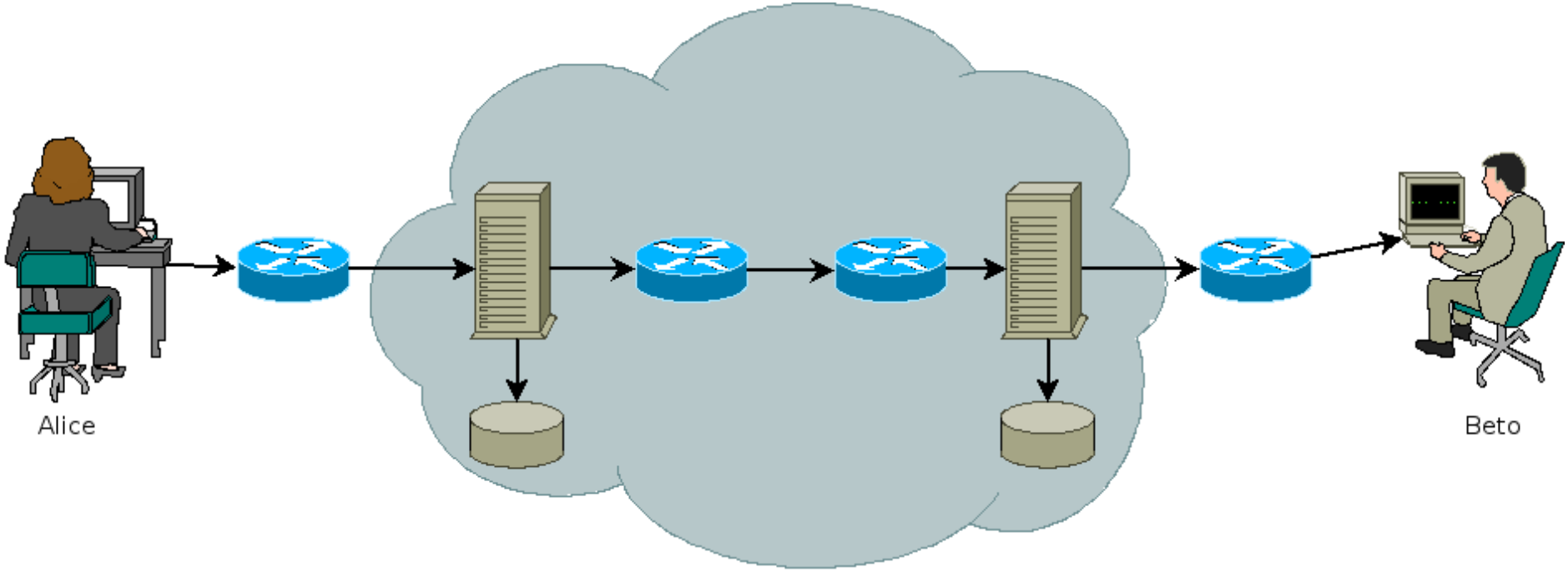
O caminho do e-mail



O caminho do e-mail



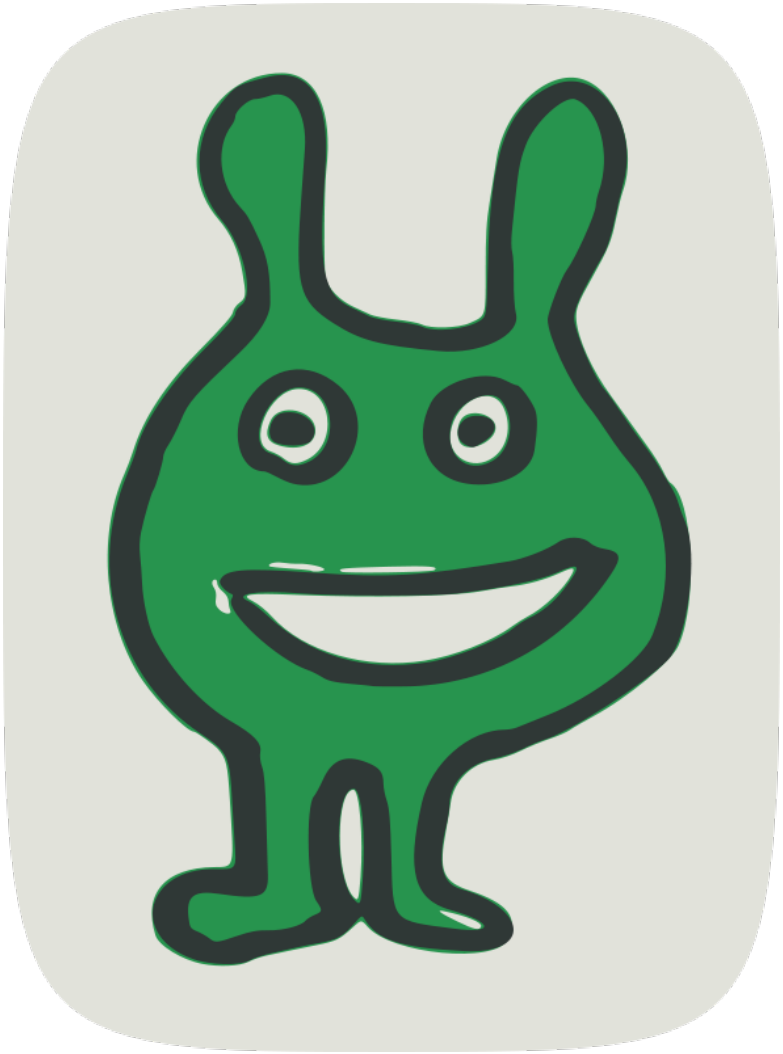
O caminho do e-mail



A solução proposta

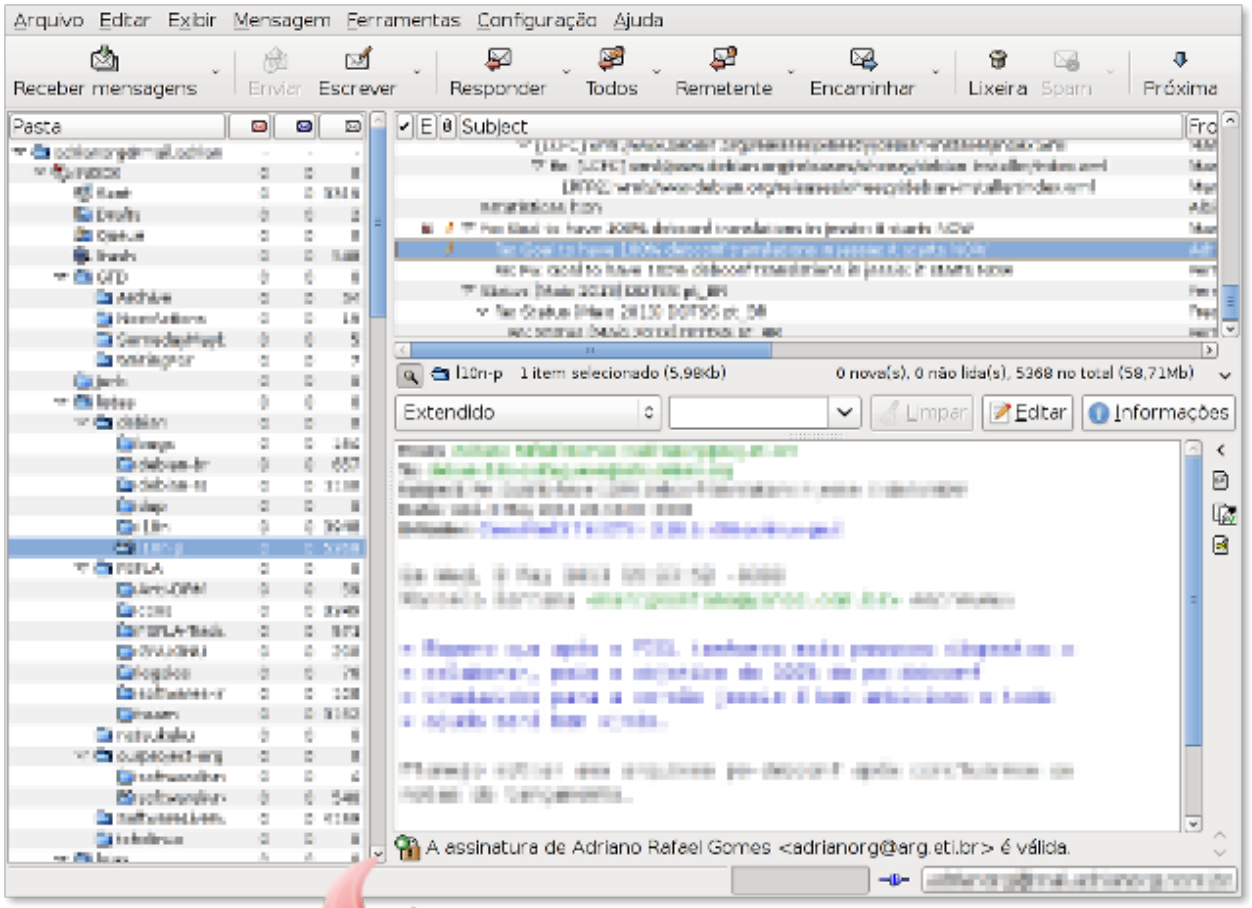
- Usar criptografia e assinatura digital
  - Confidencialidade
  - Autenticidade
  - Integridade
  - Não-repúdio

A solução proposta



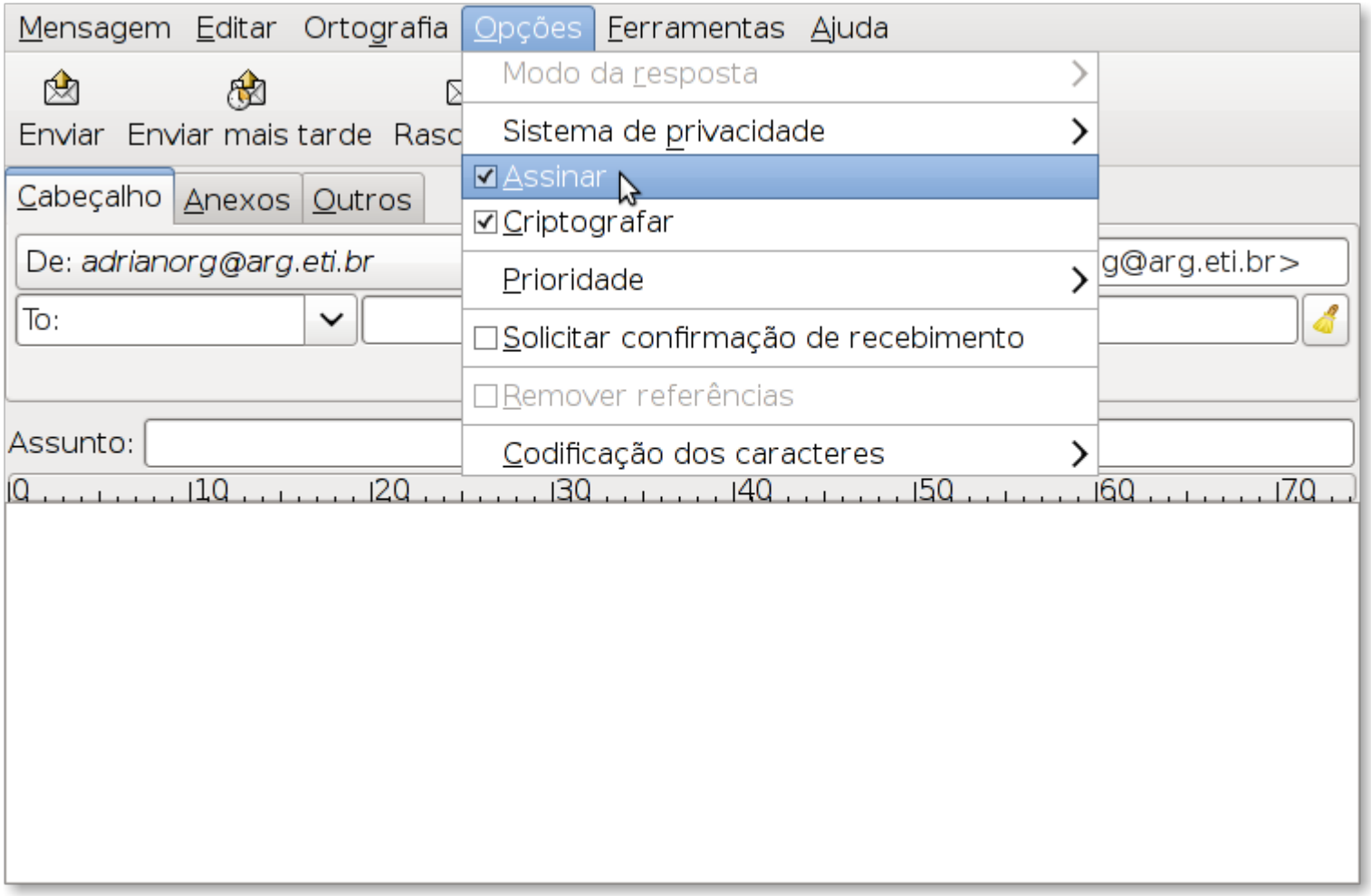
- Torna possível ter certeza absoluta de:
  - Quem enviou o e-mail
  - Que somente será lido por pessoas autorizadas
  - Que não foi modificado

Cliente de e-mail



A assinatura de Adriano Rafael Gomes <adrianorg@arg.eti.br> é válida.

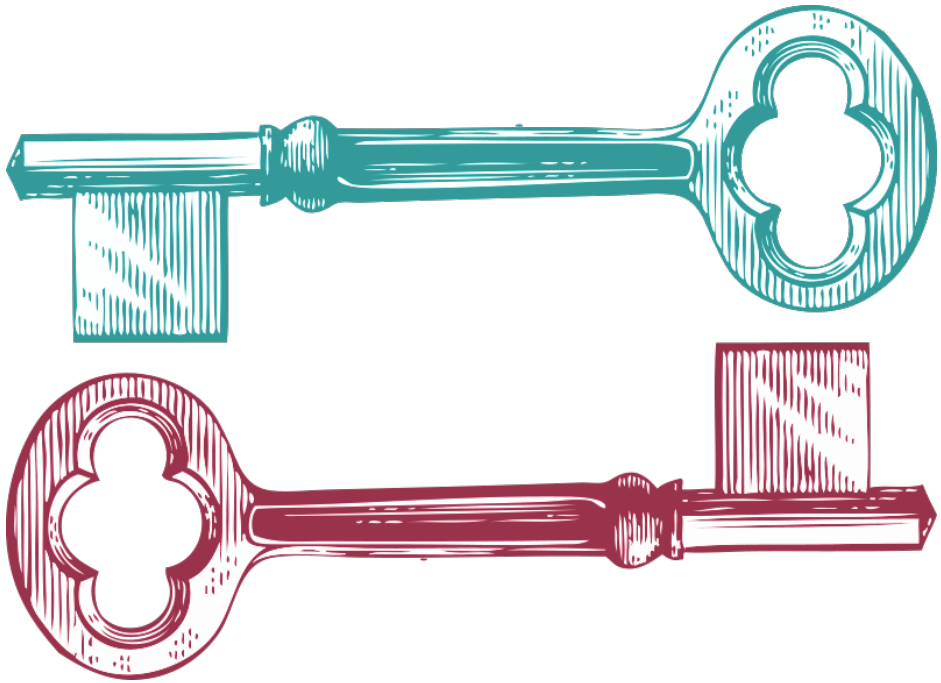
Cliente de e-mail



OpenPGP

- Padrão aberto e livre – RFC 4880
- Descentralizado
- Implementação livre: GnuPG

Funcionamento



- Chaves criptográficas, em pares:
  - Pública
  - Privada
- Funções:
  - Criptografar e descriptografar
  - Assinar e conferir assinaturas

Chave privada

- Deve ser mantida em segredo
- Descriptografar e-mails enviados para mim
- Assinar e-mails que eu enviar

Chave pública

- Deve ser divulgada
- Criptografar e-mails para outras pessoas
- Verificar assinaturas de outras pessoas

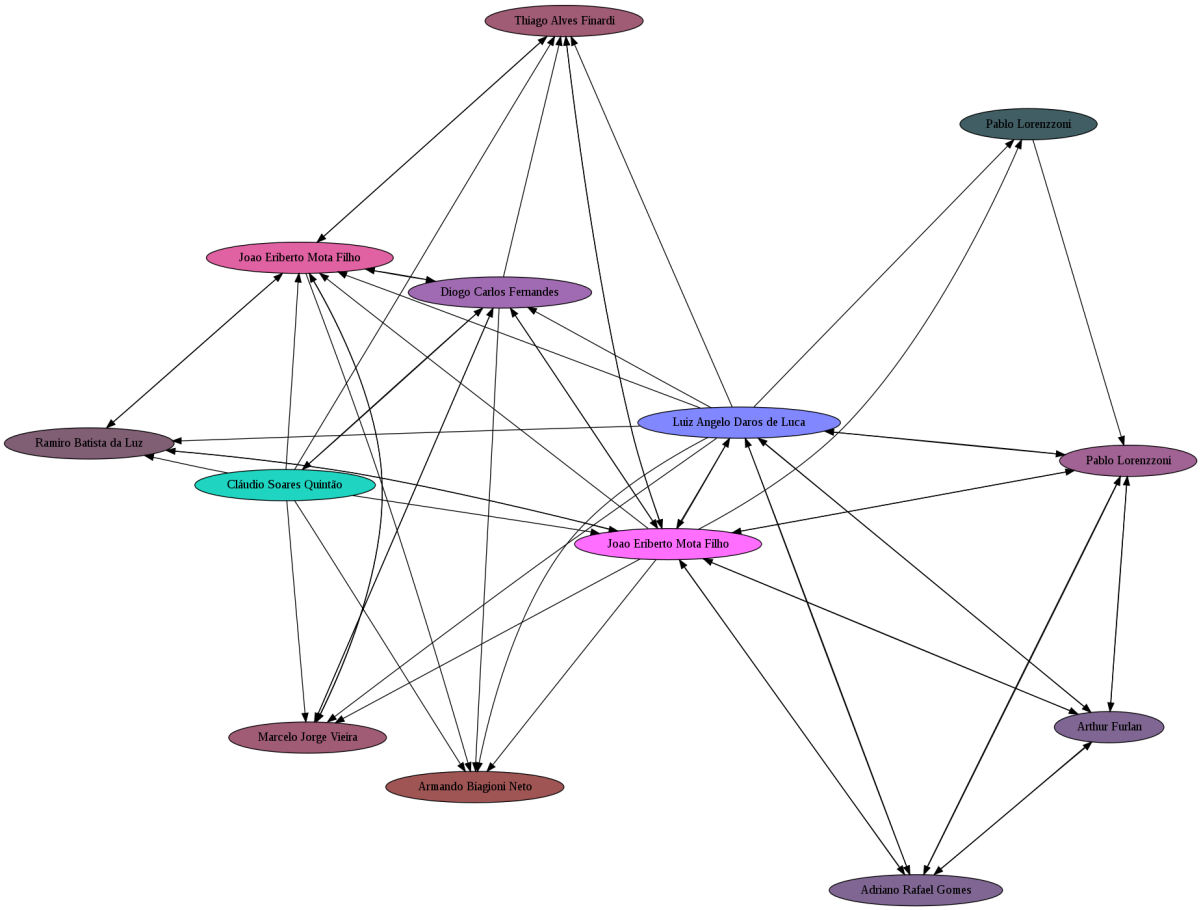
Servidores de chaves

- Para divulgar as chaves públicas
- Replicam as chaves uns para os outros

Assinatura de chaves

- Atesta que uma chave realmente pertence ao respectivo dono

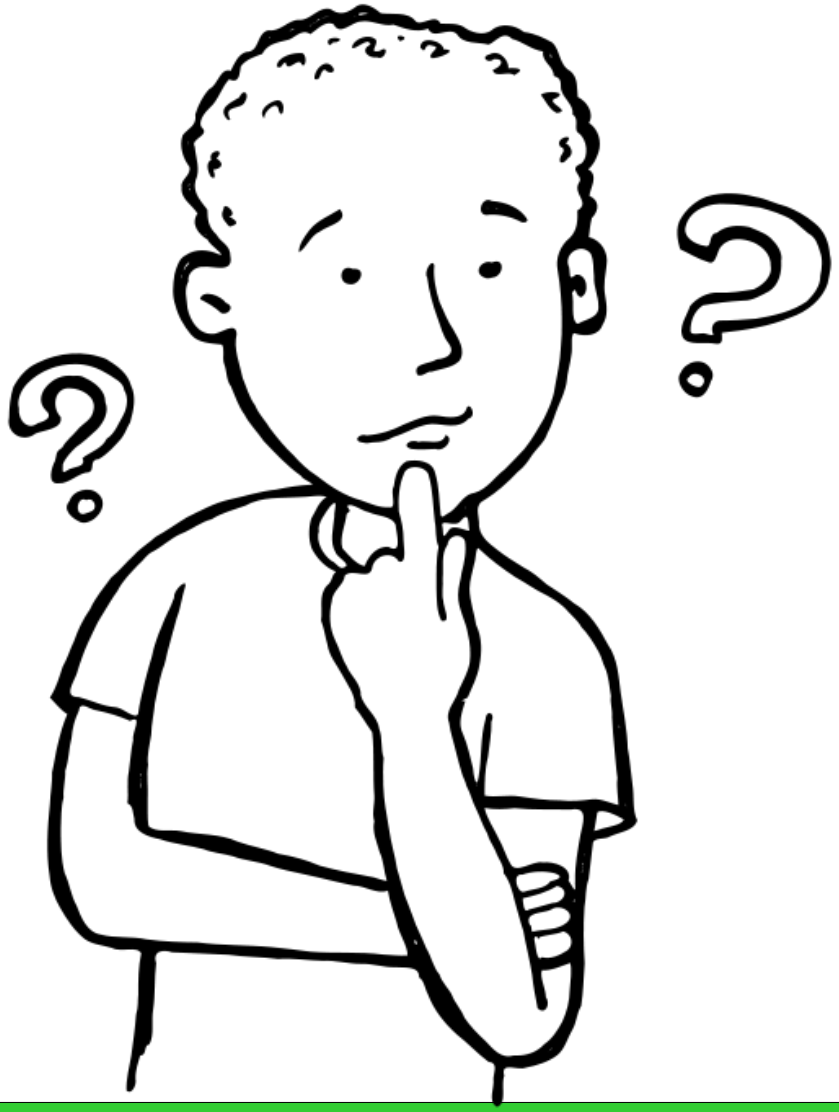
Rede de confiança



Festa de assinatura de chaves

https://secure.wikimedia.org/wikipedia/en/wiki/File:FOSDEM_2008_Key_signing_party.jpg

Perguntas



Sobre

- Contato:
  adrianorg@arg.eti.br
  http://arg.eti.br/
- Licença:
  http://creativecommons.org/licenses/by-sa/3.0/
- Imagens:
  https://openclipart.org/
- Bitcoins para o autor:
  1PbE7swb9XtZpqsoueB3s1FSj6sTcxHmou

Bônus

RESPONSIBLE BEHAVIOR – Never bring tequila to a key-signing party.

http://xkcd.com/364/

Log

- 25/09/2010: Dia da Liberdade de Software, NH
- 10/08/2013: TcheLinux VS, FTEC, NH
- 28/09/2013: Dia da Liberdade de Software, NH