FSI LEI 2025/2026

Exercícios Práticos #1

Segurança em correio eletrónico com GnuPG

1. Criar um par de chaves PGP (chave privada e pública)
2. Publicar a chave pública PGP em http://pgp.dei.uc.pt
3. Adicionar chaves públicas de outros utilizadores ao seu Keyring PGP
4. Validar a chave pública PGP de outros utilizadores no seu Keyring
5. Mudar o nível de confiança que atribui a outros utilizadores no seu Keyring
6. Utilizar o PGP para enviar e receber mensagens assinadas e encriptadas

Integração do PGP com clientes de email

Existem diversas soluções que permitem automatizar o uso de PGP no contexto da receção e envio de correio eletrónico, dependendo do cliente utilizado, refiram-se em particular os seguintes:

Enigmail (para Mozilla Thunderbird): https://www.enigmail.net/

GPGTools (para MacOS): https://gpgtools.org

Mailvelope (para sistemas de webmail): https://www.mailvelope.com

Objetivos

- Abordar conceitos introdutórios sobre o uso de criptografia assimétrica
- Utilizar o PGP (GnuPG) para adicionar segurança ao serviço de correio eletrónico

Materials de apoio

- GnuPG, The GNU Privacy Guard: http://www.gnupg.org
- Segurança Prática em Sistemas e Redes com Linux, Jorge Granjal, FCA 2017, Capítulo 2: "Segurança em Correio Eletrónico"