Provedor de serviço criptográfico: GnuPG

Lucas João Martins

GnuPG é uma alternativa de software livre ao aplicativo PGP de criptografia. Trata-se de uma completa implementação do padrão OpenPGP definido pela RFC4880. O GnuPG permite cifrar/assinar dados e comunicação, e, apresenta um sistema de gerenciamento de chaves versátil com acesso em qualquer tipo de diretório de chave pública. Trata-se de uma ferramenta de linha de comando com fácil integração em outras aplicações. Há várias aplicações de frontend e bibliotecas que utilizam o GnuPG como backend. Por fim, ele também suporta S/MIME e ssh.

O sofware faz parte do projeto GNU e recebe um grande financiamento do governo alemão. Seu criador foi o desenvolvedor alemão Werner Koch, com uma primeira release em 07 de setembro de 1999 (18 anos atrás). GnuPG é licenciado pela GNU GPLv3, além de ter mais de 80% do seu código escrito em C. Vale citar também que ele está disponível para diversos sistemas operacionais, como Microsoft Windows, macOS, Linux e Android.

A aplicação defende e faz propaganda para que as pessoas se preocupem com a sua privacidade. Aliás, recentemente foi uma das ferramentas utilizadas por Snowden para desmascarar os segredos da NSA. Para finalizar, essas são as principais características, note que algumas já foram citadas, do GnuPG:

- implementação completa do OpenPGP;
- implementação completa do CMS/X.509 (S/MIME);
- implementação de um ssh-agent;
- executa em diversos sistemas operacionais;
- alternativa completa ao PGP escrita do zero;
- não utiliza algoritmos patenteados;
- funciona melhor que o PGP através de features de segurança consideradas o estado da arte;
- decifra e verifica mensagens do PGP 5, 6 e 7;
- suporta RSA, ECDH, ECDSA, EdDSA, Elgamal, DSA, AES, Camellia, 3DES, Twofish, SHA2 e muitos outros algoritmos;
- suporta diversas linguagens;
- possui um sistema de ajuda online;
- suporte integrado para HKP (sks-keyservers.net).