Seminar Impact Considerations

Casper Kristiansson

February 13, 2024

1 Identity verification using GPG

1.1 What is it

GPG is a free and open-source library where it is used to encrypt and sign data. The goal is to ensure privacy and authenticity. The tools enable users to encrypt messages and files and create digital signatures.

1.2 What it is used for

In the context of identity verification, GPG is used to prove the ownership of an email address or digital identity securely. By signing a message or a document with their private key a user can prove their identity. It can be proven using the public key which can decrypt and verify the signature. This process is often used for secure email communication and code signing.

1.3 How it works

First, a user generates a pair of keys, a private key and a public key. For a user to verify its identity the user signs a message or a document with their private key. The sender's public key can then decrypt the signature to verify that the signature is valid.