Secure Email Communication with SEH Computertechnik GmbH using GPG/PGP

Background and Purpose

To protect sensitive information and to securely report security vulnerabilities, you can send encrypted emails to SEH Computertechnik GmbH. This article explains how to encrypt messages and communicate securely with us using PGP (Pretty Good Privacy) or GPG (GNU Privacy Guard).

Contact address for security-related information: security@seh.de

What is GPG/PGP and Why Do We Use It?

GPG and PGP are proven methods for encrypting and signing emails. They are based on the principle of asymmetric encryption:

- **Public Key:** Provided by SEH and used to encrypt your message.
- **Private Key:** Remains solely with SEH and is used to decrypt the message.

This process ensures that only authorized recipients at SEH can read your message. Additionally, you can digitally sign your message to verify its authenticity.

How to Communicate Securely with SEH

- **Download the Public Key**

  Download the public key of SEH Computertechnik GmbH from our website:
  https://www.seh-technology.com/services/security.html

- **Import the Key**

  Import the public key into your GPG/PGP application.

- **Compose and Encrypt Your Message**

  Compose your message to security@seh.de and encrypt it using the SEH key.

- **Send the Message**

  Send the encrypted message via email to the address above. Only authorized recipients at SEH can decrypt the message using the corresponding private key.

Installing and Using GPG/PGP

To send encrypted emails, you will need compatible GPG/PGP software:

- **Windows:** Gpg4win
- **macOS:** GPG Suite
- **Linux / other systems**: GnuPG is included in most distributions

1. Generating Your Own Keys

Generate your own key pair using the following command:

```
gpg --full-generate-key
```

2. **Import the SEH Public Key**

   ```
   gpg --import SEH_Computertechnik_Product_Security-E4B0B3CD_public.asc
   ```

3. **Encrypt and Sign Your Message**

   Encrypt and sign your message with the following command:

   ```
   gpg --encrypt --armor -r security@seh.de message.txt
   ```

   This creates an ASCII-armored file (`message.txt.asc`), which you can send as an email attachment.

   Important: Please include your public key when contacting us for the first time, so that we can reply to you in encrypted form as well.