Verifying Authenticity and Integrity of SEH Software Downloads

Background and Objective

This article explains how to ensure that downloaded SEH software files are authentic, complete, and unmodified. Two verification methods are combined:

1. **Authenticity check**: Verifies that the published SHA-256 hash value actually originates from SEH — by verifying the digital signature using GPG/PGP.
2. **Integrity check**: Verifies that the downloaded file is complete and unmodified — by comparing the calculated hash value with the verified SEH hash.

Note:
Perform the authenticity check first to ensure that the hash value used is trustworthy, followed by the integrity check.

1. Authenticity Check of SHA-256 Hash

What is GPG/PGP and why do we use it?

GPG (GNU Privacy Guard) or PGP (Pretty Good Privacy) are standards for digitally signing and verifying files. They are based on asymmetric cryptography:

- **Public key**: Provided by SEH, used to verify the authenticity of the hash value.
- **Private key**: Remains solely with SEH and is used to sign the hash files (cryptographic binding between the hash value and the signature).

This procedure ensures that the SHA-256 checksum is authentic and has not been tampered with, providing a foundation for the secure integrity verification of the software file.

Installing GPG/PGP

To perform the authenticity check, you need a GPG-compatible software:

- **Windows:** Gpg4win
- **macOS:** MacGPG Suite
- **Linux / andere Systeme:** GnuPG

Create Your Own Key Pair

Using GPG, it is recommended to create your own key pair:

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

Importing the SEH Public Key

Download the SEH public key from:

https://www.seh-technology.com/services/security.html

Import the key into your GPG application:

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

Downloading SHA-256 Checksum Files

Download the following files either from the ZIP archive of the software (Checksum folder) or from the SEH website:

- sha256.txt – Checksum file
- sha256.pgp – Digital signature of the checksum file

Verifying the Signature of the Checksum File

Execute the following command:

```
gpg --verify sha256.pgp sha256.txt
```

Expected output:

```
gpg: Good signature from "SEH Security <security@seh-technology.com>"
```

2. Integrity Check of the Software File

After successful signature verification, use the verified hash value from sha256.txt as a reference. Compare the calculated SHA-256 hash of your downloaded file with the verified reference value from SEH.

To check the SHA-256 hash of the file in question, generate a checksum of the downloaded file and compare it with the SHA-256 hash provided by SEH. This can be done using an external tool or built-in OS functions.

The SHA-256 hash of the corresponding file can be calculated on macOS/Linux using the `shasum` tool, and on Microsoft Windows using either the `certutil` or `Get-FileHash` tools.
The following example demonstrates the use of these tools with the software file *d-sys-uds-20.1.32.bin* for the utnserver Pro.

The SHA-256 hash can be calculated as follows:

SEH-provided SHA-256 Hash for the file d-sys-uds-20.1.32.bin:

```
3dcbd6cbbc7cc414889049223fe943101da76829497d6fbb7fb453c69e59b7b8
```

Windows Command Prompt

General command format:

```
CertUtil -hashfile [FILENAME] SHA256
```

Example:

```
C:\> certutil -hashfile d-sys-uds-20.1.32.bin SHA256
```

Windows PowerShell

General command format:

```
Get-FileHash [FILENAME] -Algorithm SHA256
```

Example:

```
C:\> Get-FileHash .\d-sys-uds-20.1.32.bin -Algorithm SHA256
```

macOS / Linux

General command format:

```
shasum -a 256 [FILENAME]
```

Example:

```
shasum -a 256 d-sys-uds-20.1.32.bin
```

You can also automatically verify the calculated hash against the SEH hash using the `-c` option:

```
echo '3dcbd6cbbc7cc414889049223fe943101da76829497d6fbb7fb453c69e59b7b8
*d-sys-uds-20.1.32.bin' | shasum -c
```

Conclusion

If both the **authenticity check** (signature verification of the SHA-256 hash) and **the integrity check** (file hash comparison) succeed, you can be assured that:

- The file genuinely **originates from SEH**
- The file has **not been altered or corrupted**

This method ensures complete verification of SEH software downloads regarding their origin and content.