

Verifizierung von Authentizität und Integrität von SEH-Software-Downloads

Hintergrund und Ziel

Dieser Artikel beschreibt, wie Sie sicherstellen, dass heruntergeladene SEH-Softwaredateien authentisch, vollständig und unverändert sind. Dazu kombinieren Sie zwei Prüfmethoden:

- **1. Authentizitätsprüfung:** Verifiziert, dass der veröffentlichte SHA-256-Hashwert tatsächlich von SEH stammt – durch Überprüfung der digitalen Signatur mit GPG/PGP.
- **2. Integritätsprüfung:** Überprüft, ob die heruntergeladene Datei vollständig und unverändert ist – durch Vergleich des berechneten Hashwerts mit dem verifizierten SEH-Hash.

Hinweis:

Führen Sie zuerst die Authentizitätsprüfung durch, um sicherzustellen, dass der verwendete Hashwert vertrauenswürdig ist. Danach folgt die Integritätsprüfung.

1. Authentizitätsprüfung des SHA-256-Hashes

Was ist GPG/PGP und warum nutzen wir es?

GPG (GNU Privacy Guard) bzw. PGP (Pretty Good Privacy) sind Standards zur digitalen Signatur und Verifikation von Dateien. Sie beruhen auf asymmetrischer Kryptografie:

- **Öffentlicher Schlüssel:** Wird von SEH bereitgestellt und dient zum Verifizieren, ob der Hashwert wirklich von SEH stammt.
- **Privater Schlüssel:** Bleibt ausschließlich bei SEH und dient zum Signieren der Hashdateien. (kryptografische Bindungen zwischen Hashwert und Signatur)

Dieses Verfahren stellt sicher, dass die SHA-256-Prüfsumme nicht manipuliert wurde und authentisch von SEH stammt – eine Voraussetzung für die sichere Integritätsprüfung der Softwaredatei.

GPG/PGP installieren

Für die Authentizitätsprüfung benötigen Sie eine GPG-kompatible Software:

- **Windows:** [Gpg4win](#)
- **macOS:** [MacGPG Suite](#)
- **Linux / andere Systeme:** [GnuPG](#)

Eigenes Schlüsselpaar erzeugen (optional)

Zur Nutzung von GPG empfiehlt sich ein eigenes Schlüsselpaar:

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

SEH-Schlüssel importieren

Laden Sie den öffentlichen SEH-Schlüssel herunter von:

<https://www.seh-technology.com/de/service/sicherheit.html>

Importieren Sie diesen in Ihre GPG-Anwendung:

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

SHA-256-Prüfsummen-Dateien herunterladen

Laden Sie folgende Dateien entweder aus dem ZIP-Archiv der Software (Ordner Checksum) oder von der SEH-Webseite:

- sha256.txt – Prüfsummendatei
- sha256.pgp – Digitale Signatur der Prüfsummendatei

Signatur der Prüfsummendatei prüfen

Führen Sie den folgenden Befehl aus:

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

Erwartete Ausgabe:

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

2. Integritätsprüfung der Softwaredatei

Nach erfolgreicher Signaturprüfung dient der verifizierte Hashwert aus `sha256.txt` als Referenz. Vergleichen Sie den berechneten SHA-256-Hash Ihrer heruntergeladenen Datei mit dem zuvor verifizierten Referenzwert von SEH.

Um den SHA-256-Hash der betreffenden Datei zu überprüfen, muss eine Prüfsumme der heruntergeladenen Datei erstellt und mit dem von SEH bereitgestellten SHA-256-Hash verglichen werden. Dies kann mit einem externen Tool oder direkt mit den Bordmitteln des jeweiligen Betriebssystems geschehen.

Der SHA-256-Hash der betreffenden Datei kann unter **macOS/Linux** mit den Tools `shasum` und unter **Microsoft Windows** mit den Tools `certutil` oder `Get-FileHash` berechnet werden. Im Folgenden Beispiel wird die Benutzung der Tools anhand der Software `d-sys-uds-20.1.32.bin` für den `utnserver Pro` gezeigt.

Von SEH angegebener SHA-256-Hash für die Datei `d-sys-uds-20.1.32.bin`:

```
3dcbd6cbbc7cc414889049223fe943101da76829497d6fbb7fb453c69e59b7b8
```

Windows Eingabeaufforderung

Der allgemeine Funktionsaufruf in der Windows Eingabeaufforderung lautet:

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

Beispiel:

Berechnen des Hashwertes der Datei „d-sys-uds-20.1.32.bin“:

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

Windows PowerShell

Der allgemeine Funktionsaufruf in der Windows PowerShell lautet:

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

Beispiel:

Berechnen des Hashwertes der Datei „*d-sys-uds-20.1.32.bin*“:

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

macOS/Linux

Der allgemeine Funktionsaufruf im Terminal lautet:

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

Beispiel:

Berechnen des Hashwertes der Datei „*d-sys-uds-20.1.32.bin*“:

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

Mit Hilfe der Option `-c` kann der Hashwert berechnet, mit dem SEH-Hashwert verglichen und das Ergebnis angezeigt werden:

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

Fazit

Wenn Sie sowohl die **Authentizitätsprüfung** (Signaturprüfung des SHA-256-Hashs) als auch die **Integritätsprüfung** (Vergleich des Datei-Hashs) erfolgreich durchführen, können Sie sicher sein, dass:

- die Datei **authentisch von SEH** stammt
- die Datei **nicht verändert oder beschädigt** wurde

Mit diesem Verfahren ist sichergestellt, dass SEH Software-Downloads sowohl hinsichtlich ihrer Herkunft als auch ihrer Inhalte vollständig verifiziert werden können.