gpg-agent Weiterleitung per ssh

Während ssh agent Forwarding schon lange funktioniert und es ermöglicht, auch auf einem entfernten Rechner auf die ssh-Keys des lokalen ssh-agents (auch via gnupg) zugreifen zu können um sich auf diese Weise vom Remote-Host auf weiteren Remote-Hosts anmelden zu können, funktioniert das für gpg-Informationen noch nicht so lange.

Ziel ist es, auch auf einer per ssh angemeldeten Maschine die lokalen geheimen Schlüssel von gnupg nutzen zu können - oder auch Zugriff auf die gnupg-Karte zu haben.

Das funktioniert via Agent Forwarding und ist im Prinzip unkompliziert und lässt sich wie in der Anleitung https://wiki.gnupg.org/AgentForwarding konfigurieren.

Allerdings klappt das zumindest bei Debian 9/10 nicht out of the Box. Schuld ist systemd, durch den auf dem entfernten Rechner die Sockets bereits existieren - und daher nicht per Forwarding zur Verfügung gestellt werden können. Fehlermeldung:

```
Warning: remote port forwarding failed for listen path
/run/user/1000/gnupg/S.gpg-agent
```

Eigentlich soll ein Eintrag

```
StreamLocalBindUnlink yes
```

in der sshd_config auf dem Remote Host dafür sorgen, dass ggf. vorhandene Sockets überschrieben werden. Aber entweder verhindert das ein Bug - oder es gibt eine Race-Condition. (Genau habe ich das noch nicht heraus gefunden).

Ein Workaround ist ein Überschreiben des systemd-Files im lokalen User-Verzeichnis. Wir benennen hier den automatisch angeleten Socket einfach um:

.config/systemd/user/gpg-agent.socket

```
[Unit]
Description=GnuPG cryptographic agent and passphrase cache
Documentation=man:gpg-agent(1)

[Socket]
ListenStream=%t/gnupg/S.gpg-agent.disabled
FileDescriptorName=std
SocketMode=0600
DirectoryMode=0700

[Install]
WantedBy=sockets.target
```

Ein Eintrag in der lokalen `.ssh/config` wie z.B.

```
host RemoteForwardedGnupg
    HostName somehost.example.org
    User user
    RemoteForward /run/user/1000/gnupg/S.gpg-agent
/run/user/1000/gnupg/S.gpg-agent.extra
```

(Achtung: lokale und remote User-Ids müssen entsprechend gesetzt werden. Der erste Eintrag ist der Remote-Socket, der zweite der Lokale).