Praktische Anleitung zu Konfiguration von IPSEC Verbindungen

mittels FreeS/WAN und PGPnet

–Screenshots–

Torsten Höfler

htor@informatik.tu-chemnitz.de
hoefler@delta.de

Inhaltsverzeichnis

1 Konfiguration eines PGPnet Clients (Windows) - Screenshots

1.1 PGPnet Version 6.5.8

1.1.1 Erzeugen der Schlüssel

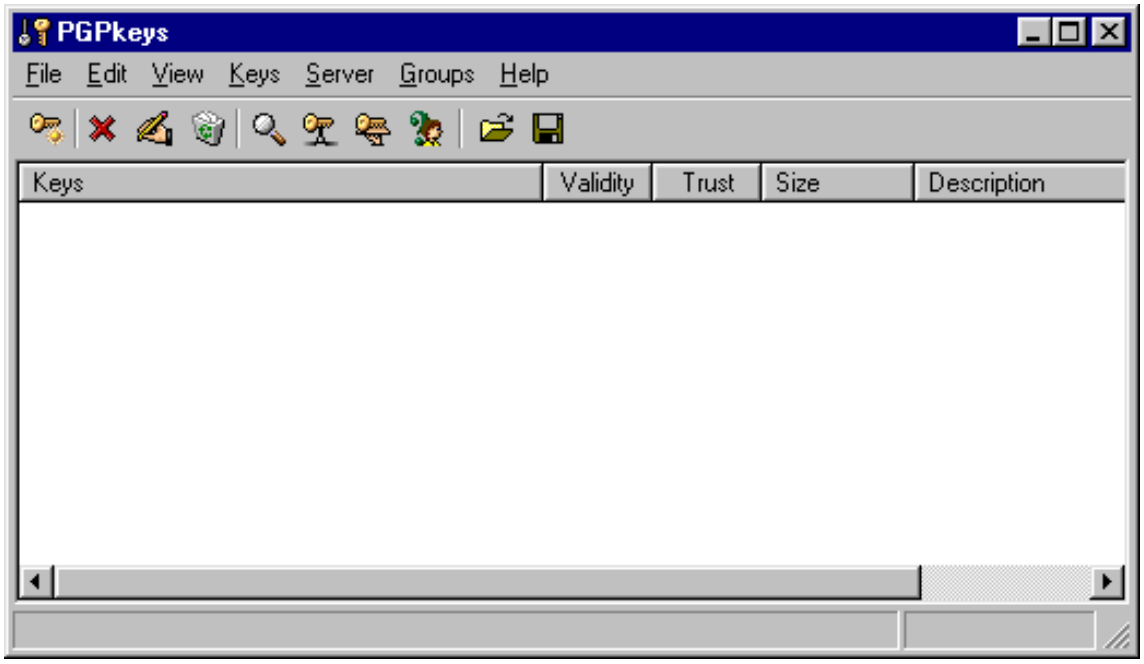

Abbildung 1: neuen Schlüssel erzeugen - 1

PGPkeys, nachdem alle vorhandenen Schlüssel gelöscht wurden.

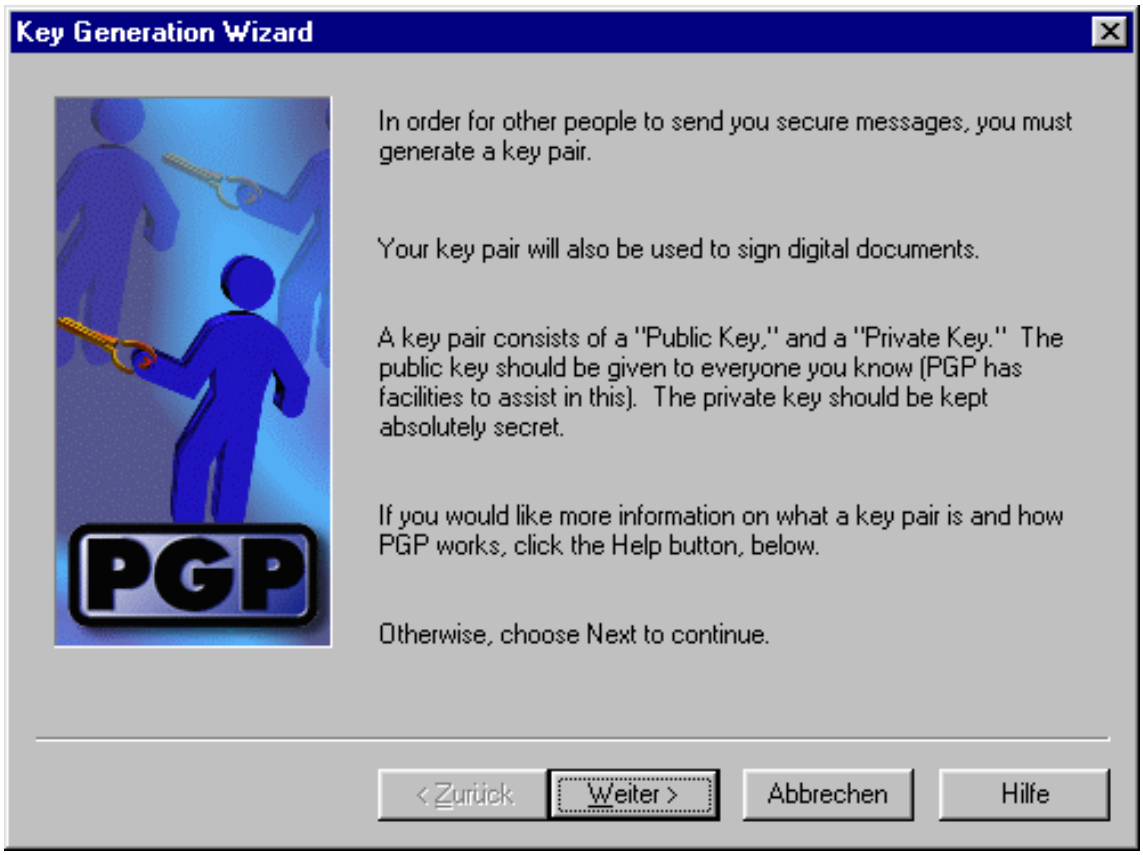

Abbildung 2: neuen Schlüssel erzeugen - 2

Erzeugen eines neuen Schlüssels - Startlogo

Abbildung 3: neuen Schlüssel erzeugen - 3

Eingabe der Identifikationsdaten für den neuen Schlüssel, anhand des hier vergebenen Namens wird später der FreeS/WAN Key extrahiert.

Abbildung 4: neuen Schlüssel erzeugen - 4

RSA Verschlüsselung wählen.

Abbildung 5: neuen Schlüssel erzeugen - 5

1024 Bit RSA

Abbildung 6: neuen Schlüssel erzeugen - 6

Gültigkeit des Schlüsselpaares (zu Testzwecken läuft es nie ab)

Abbildung 7: neuen Schlüssel erzeugen - 7

Persönliches Kennwort (Mantra).

Abbildung 8: neuen Schlüssel erzeugen - 8

Generierung des neuen Schlüssels abgeschlossen

Abbildung 9: neuen Schlüssel erzeugen - 9

Schlüssel nicht an Root-Server schicken, wenn keine eindeutige Identifikation möglich ist!

Abbildung 10: neuen Schlüssel erzeugen - 10

Schlüssel in keyring speichern

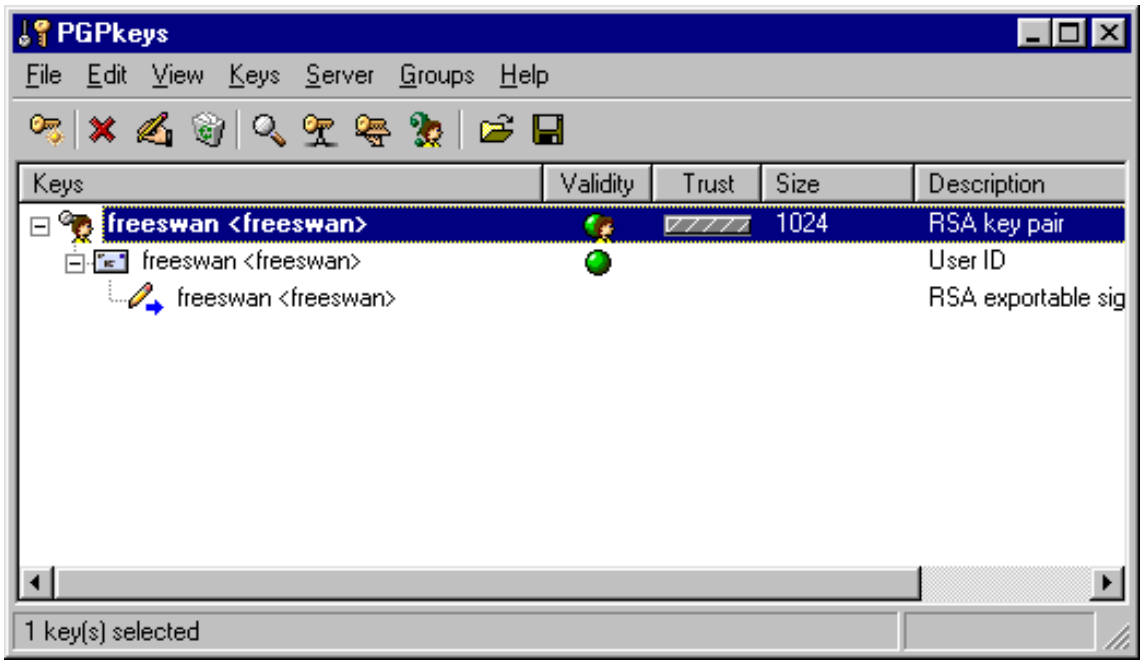

Abbildung 11: neuen Schlüssel erzeugen - 11

Ansicht des neu erzeugten Schlüssels in PGPkeys

Abbildung 12: neuen Schlüssel erzeugen - 12

Die Dateien pubring.pkr und secring.pkr im Keyring-Verzeichnis

1.1.2 Vorhandene Schlüssel in PGPnet importieren

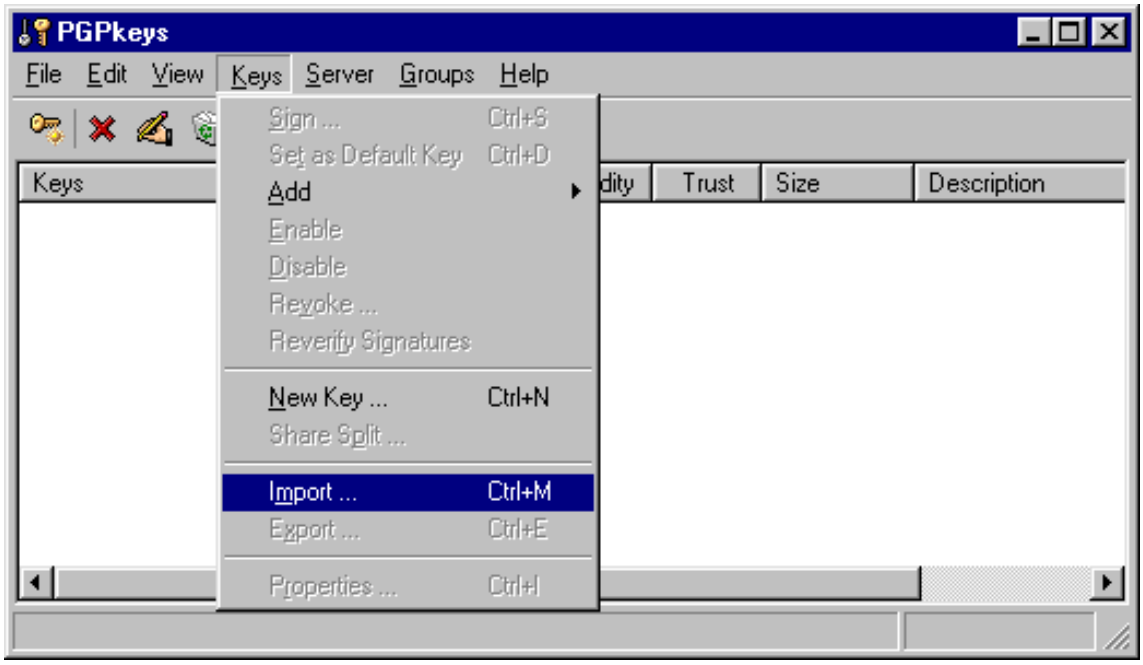

Abbildung 13: Schlüssel importieren - 1

Menüpunkt Schlüssel importieren.

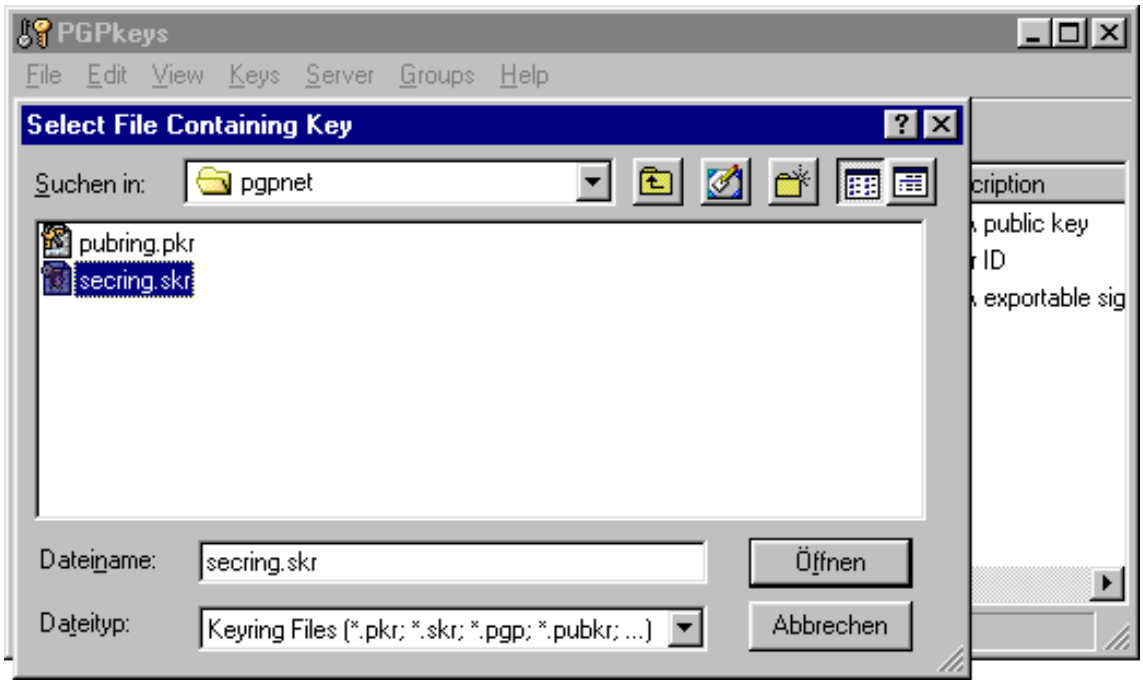

Abbildung 14: Schlüssel importieren - 2

Schlüssel wählen (Keyring Files)

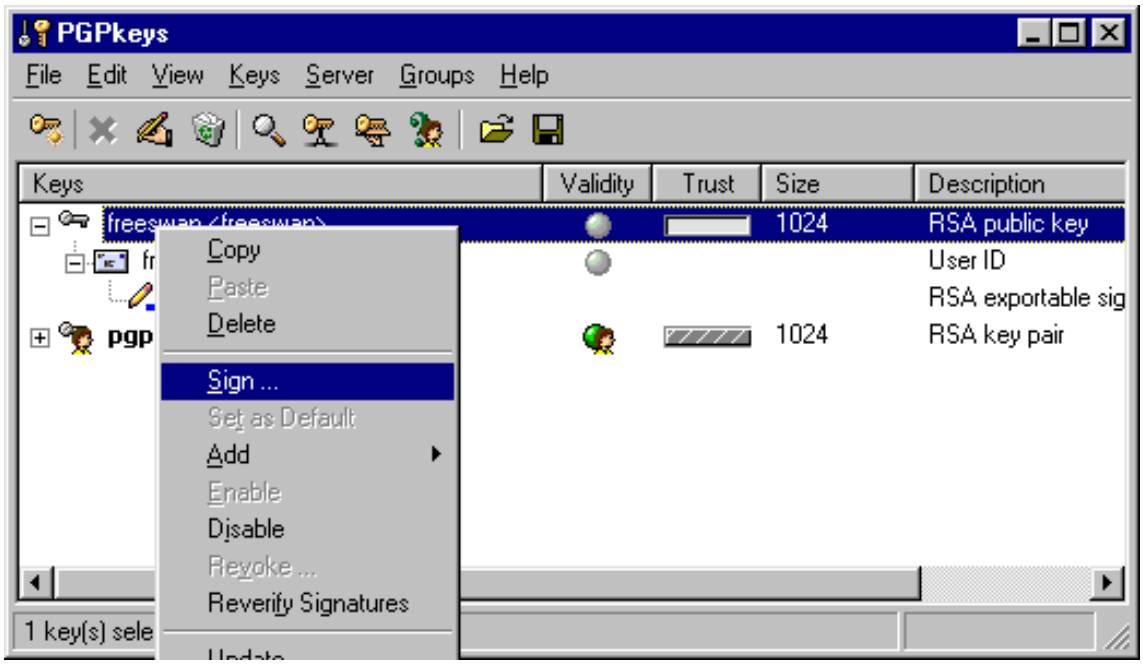

Abbildung 15: Schlüssel importieren - 3

Öffentlichen Schlüssel von freeswan signieren, und als „trusted“ definieren

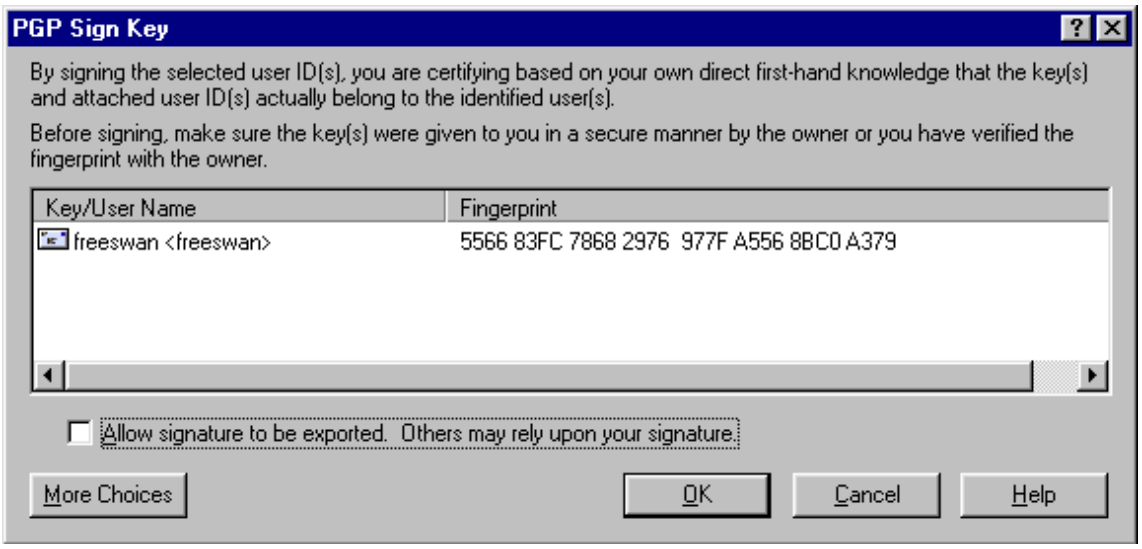

Abbildung 16: Schlüssel importieren - 4

Dialog zum signieren des Schlüssels

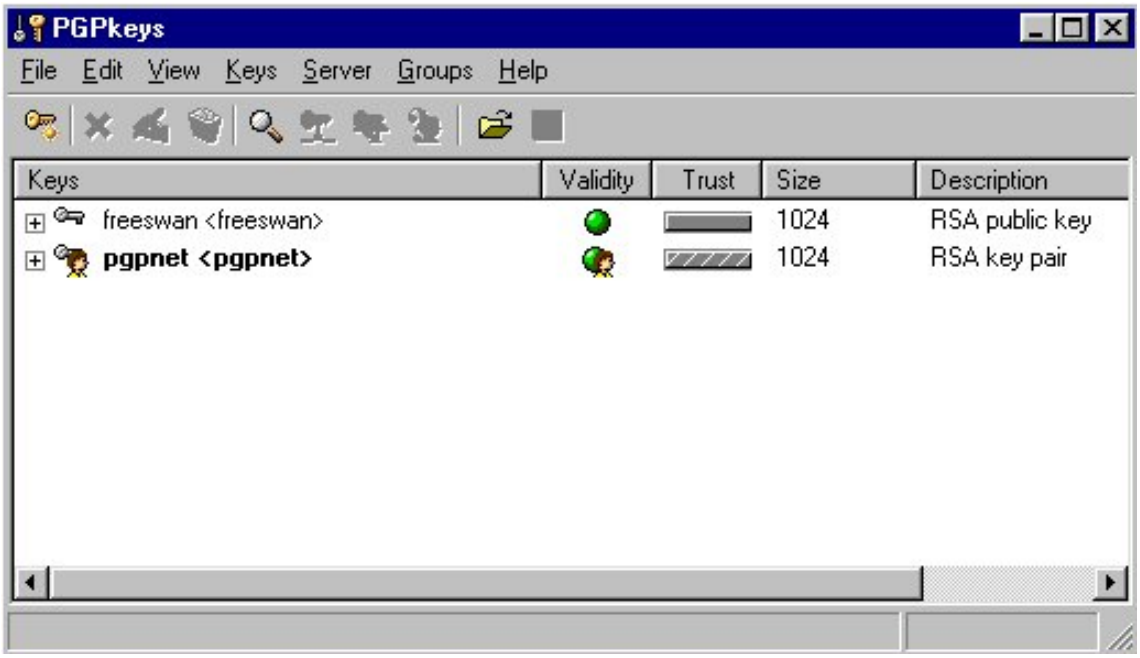

Abbildung 17: Schlüssel importieren - 5

Ansicht der komplett importierten Schlüssel

1.1.3 Konfigurieren von PGPnet

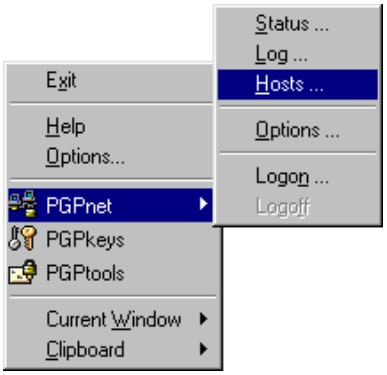

Abbildung 18: Optionen anpassen - 1

Konfiguration von PGPnet (Taskleistensymbol)

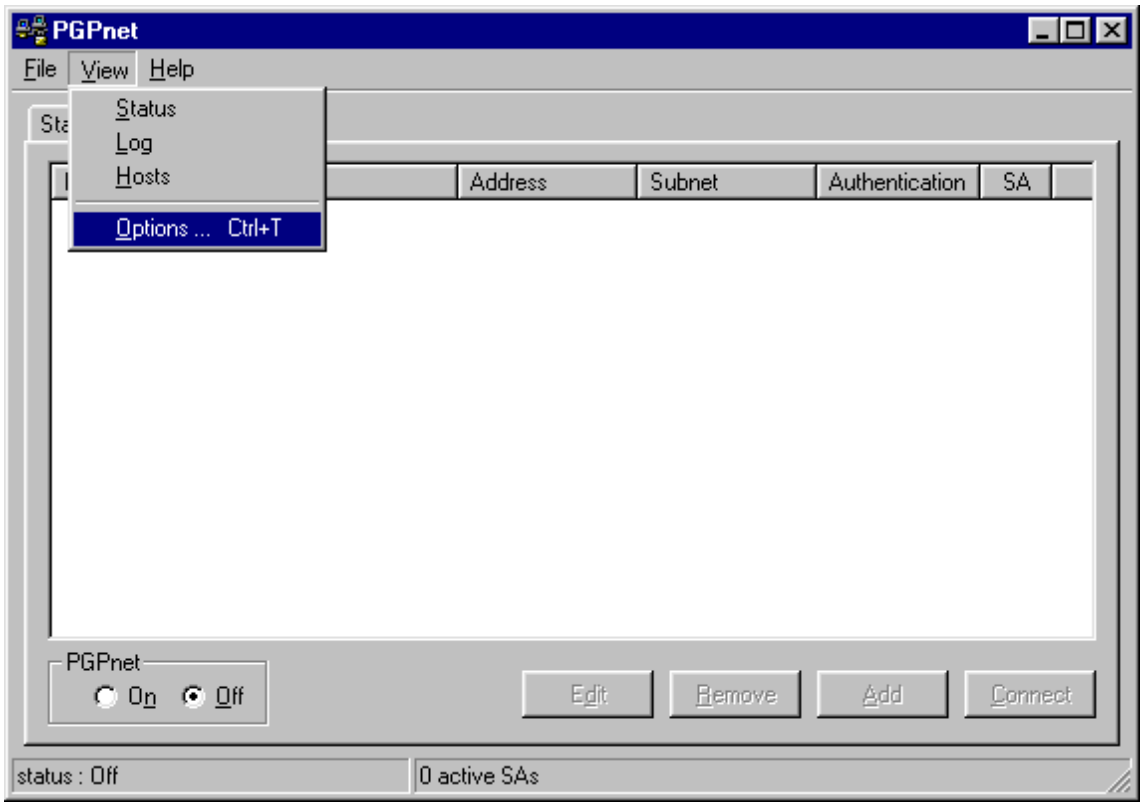

Abbildung 19: Optionen anpassen - 2

Menüpunkt Optionen

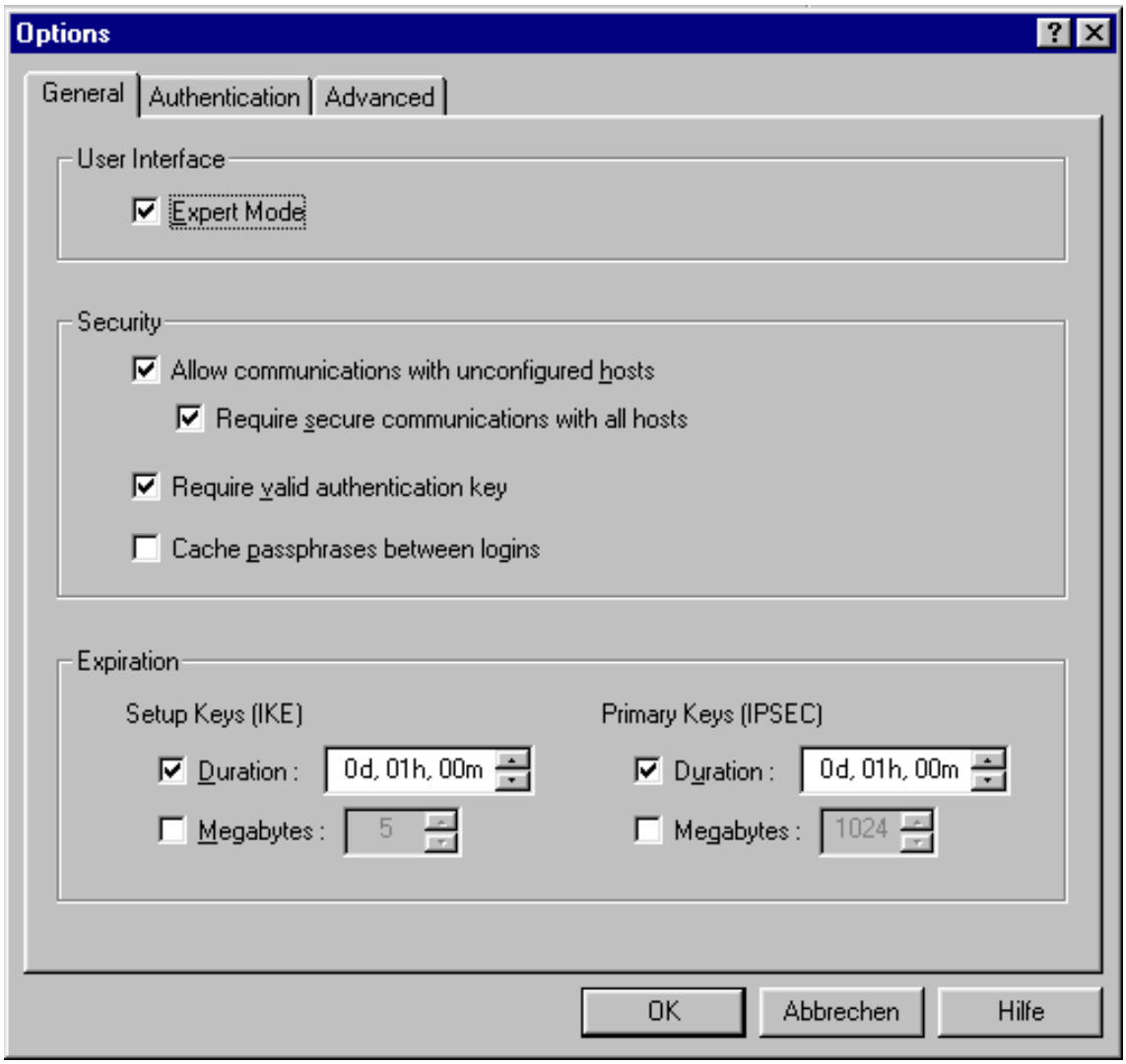

Abbildung 20: Optionen anpassen - 3

Menüpunkt „General“

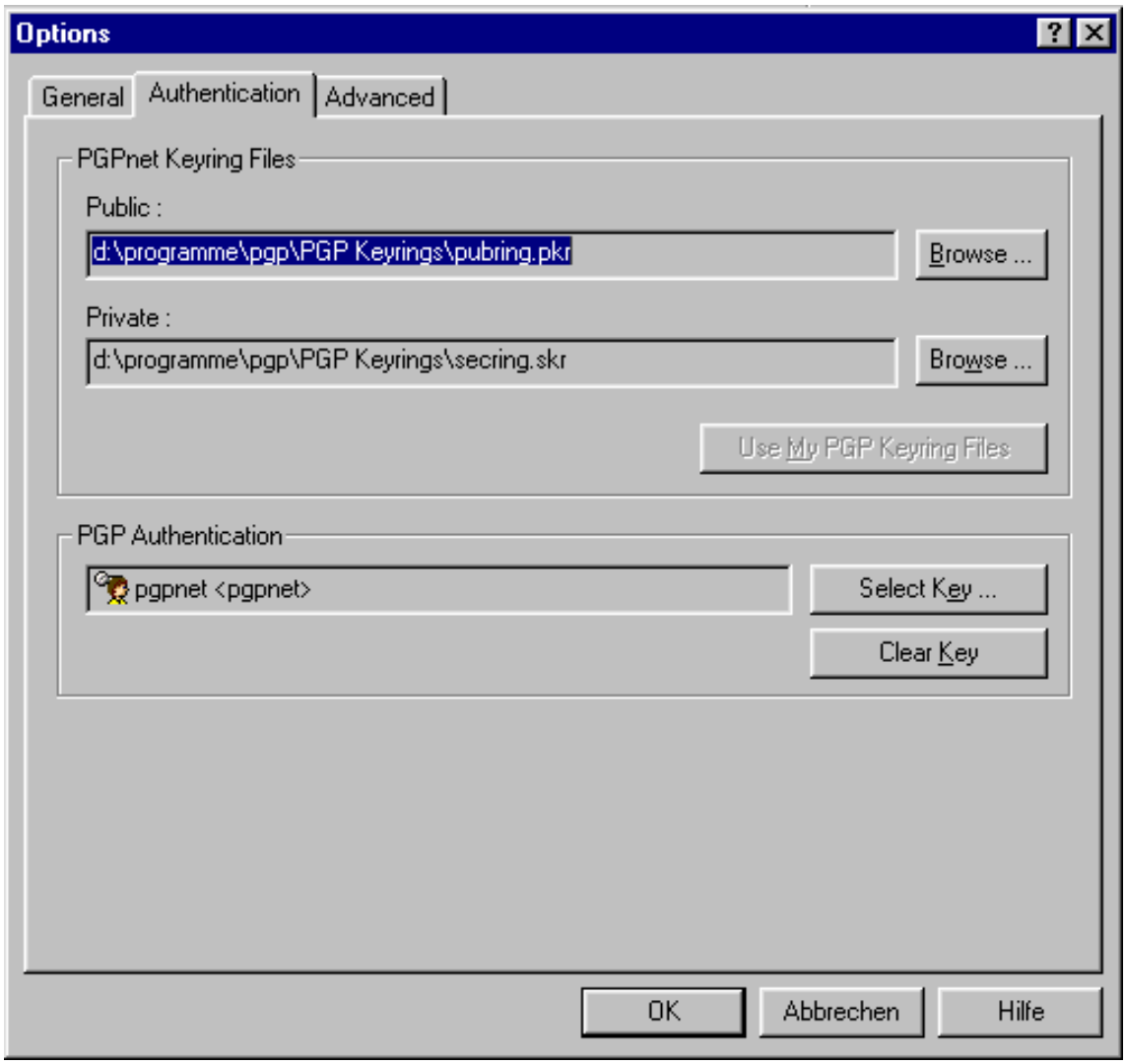

Abbildung 21: Optionen anpassen - 4

Menüpunkt „Authentication“

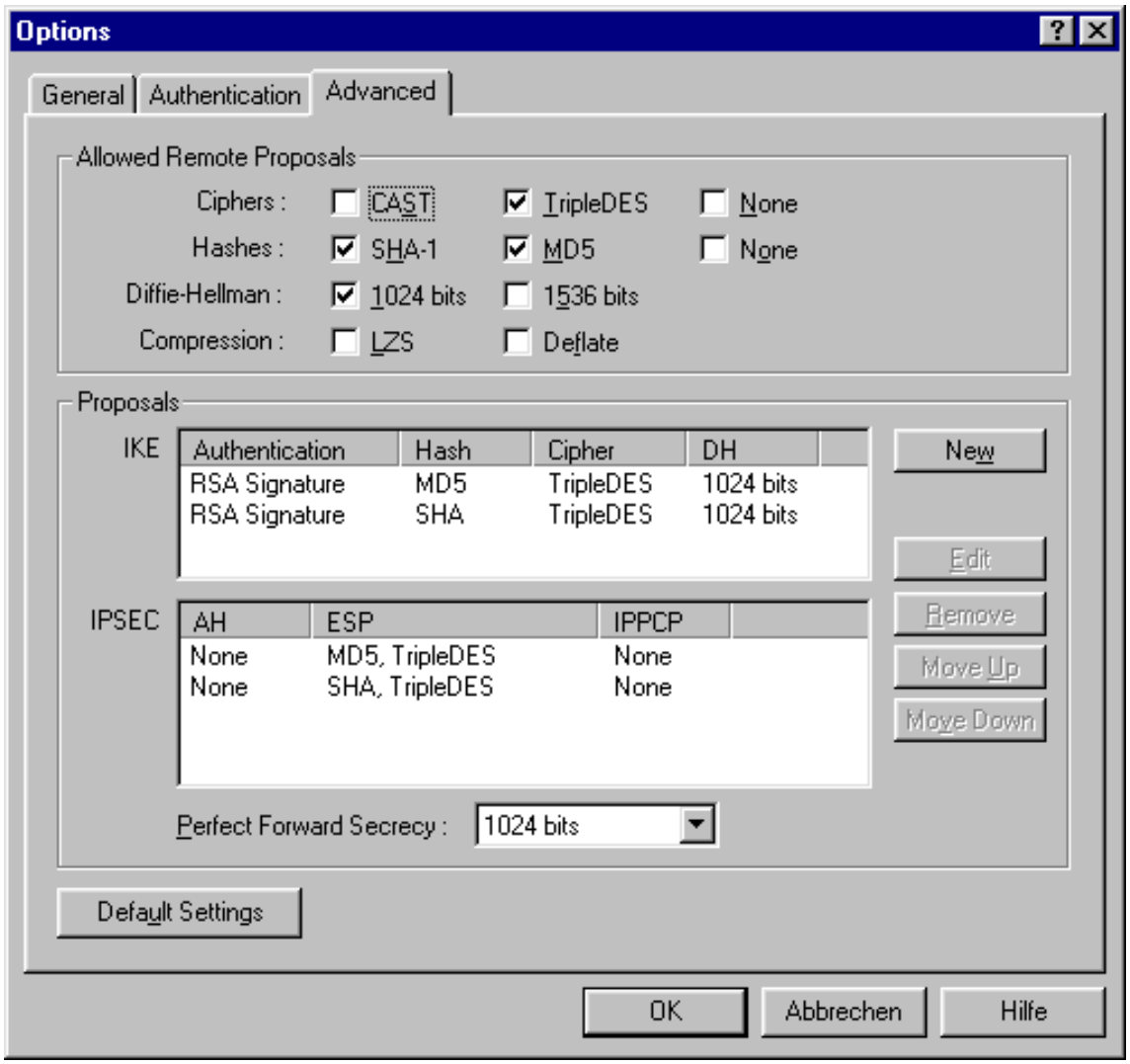

Abbildung 22: Optionen anpassen - 5

Menüpunkt „Advanced“

1.1.4 Hinzufügen einer neuen Verbindung

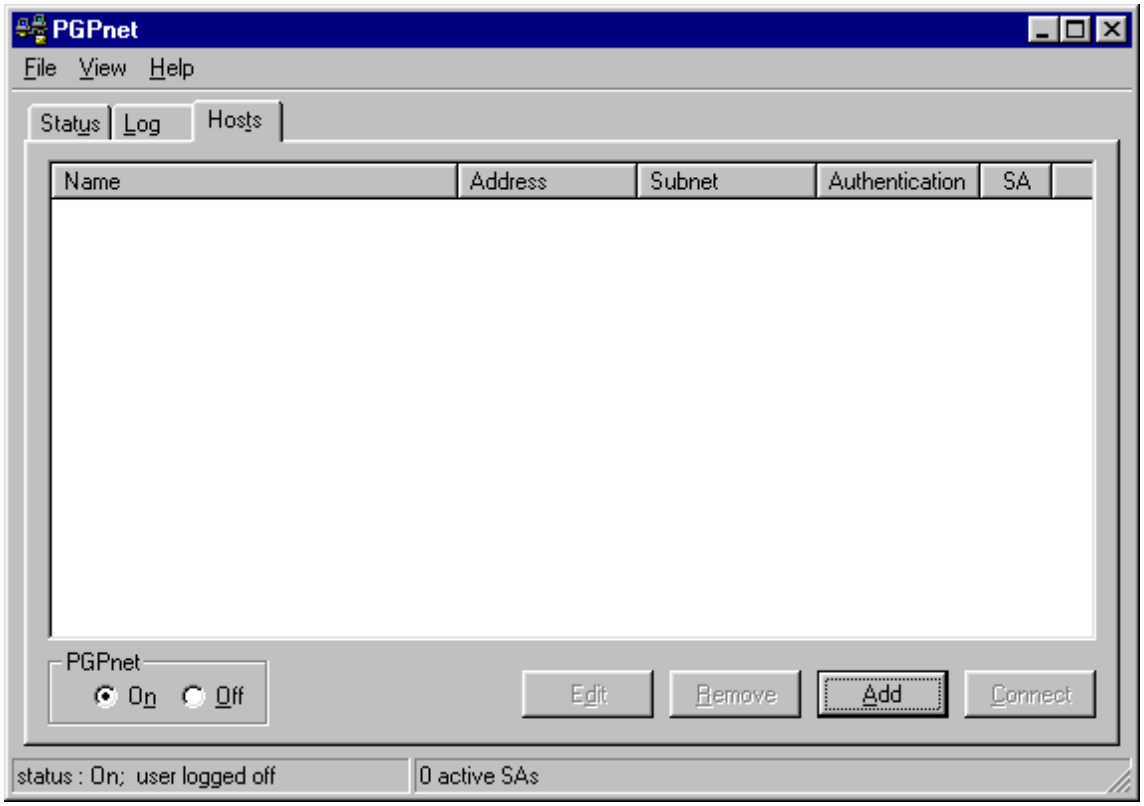

Abbildung 23: Neue Verbindung anlegen - 1

Hinzufügen eines neuen IPSEC-Servers

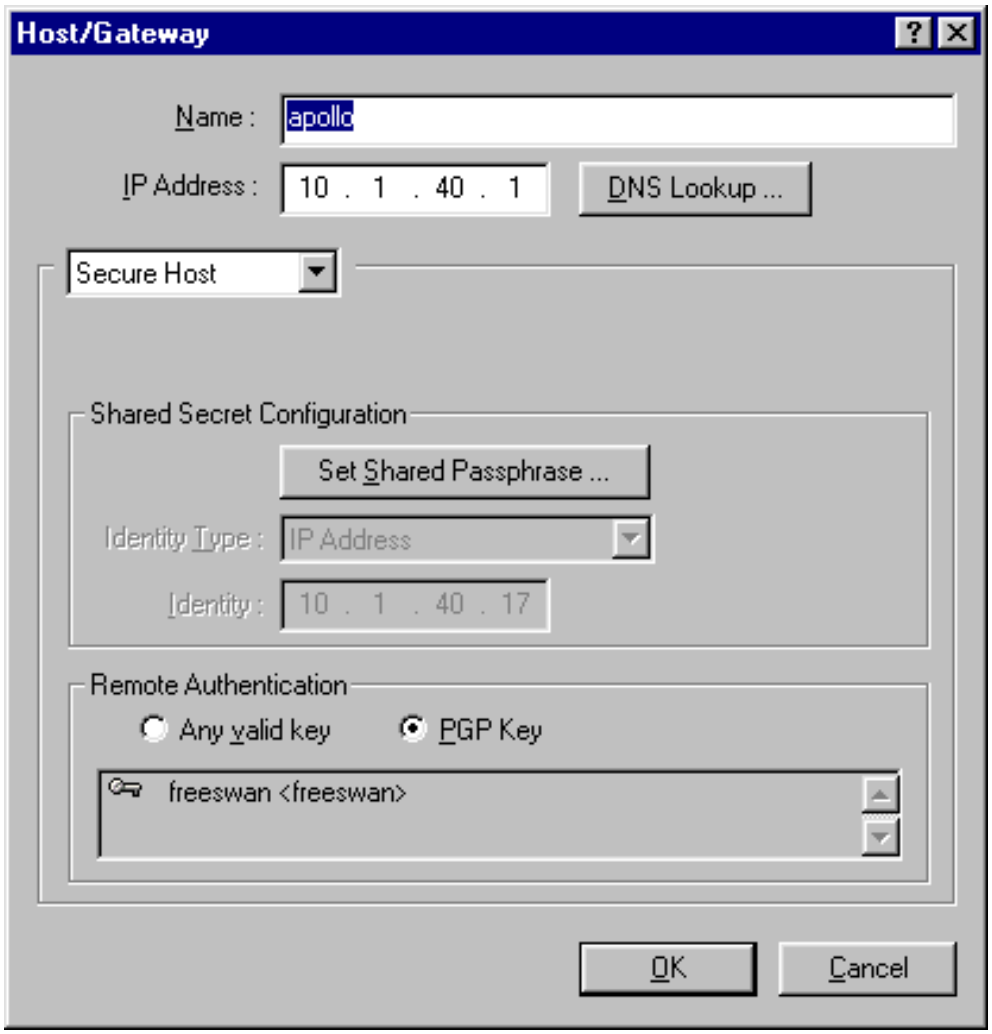

Abbildung 24: Neue Verbindung anlegen - 2

Generelle Einstellungen

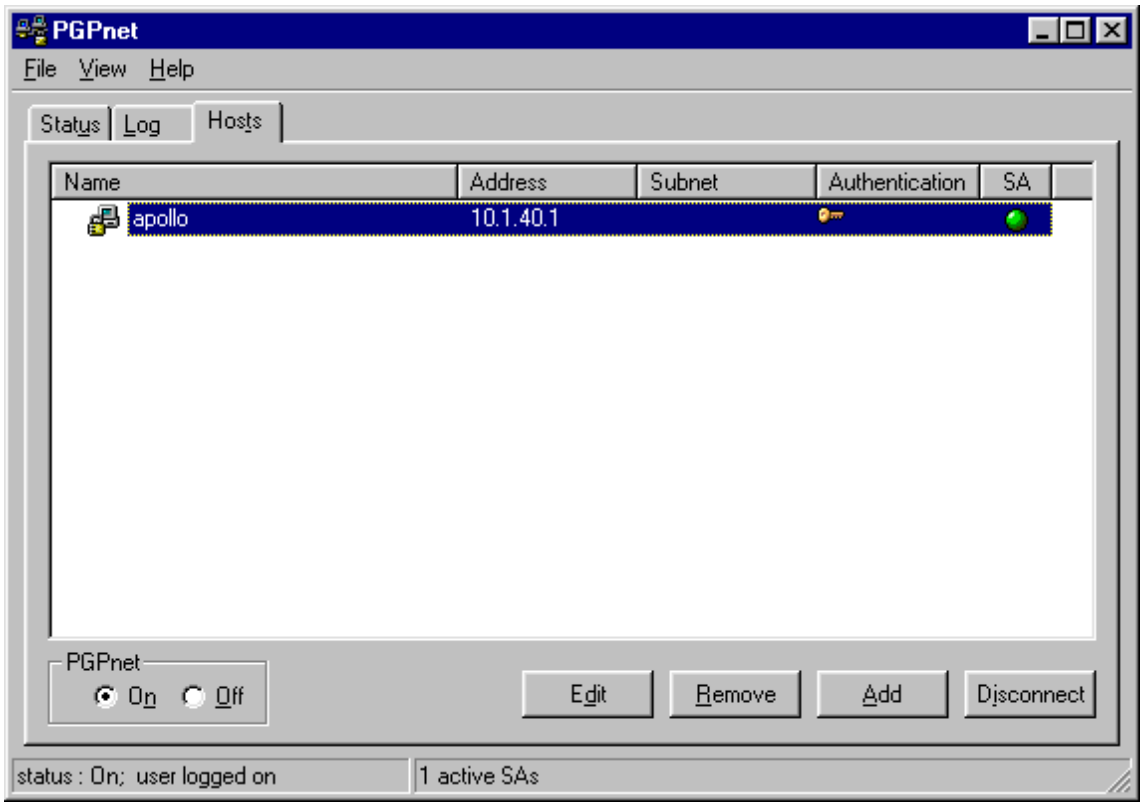

Abbildung 25: Neue Verbindung anlegen - 3

Verbindung aktivieren (Connect)

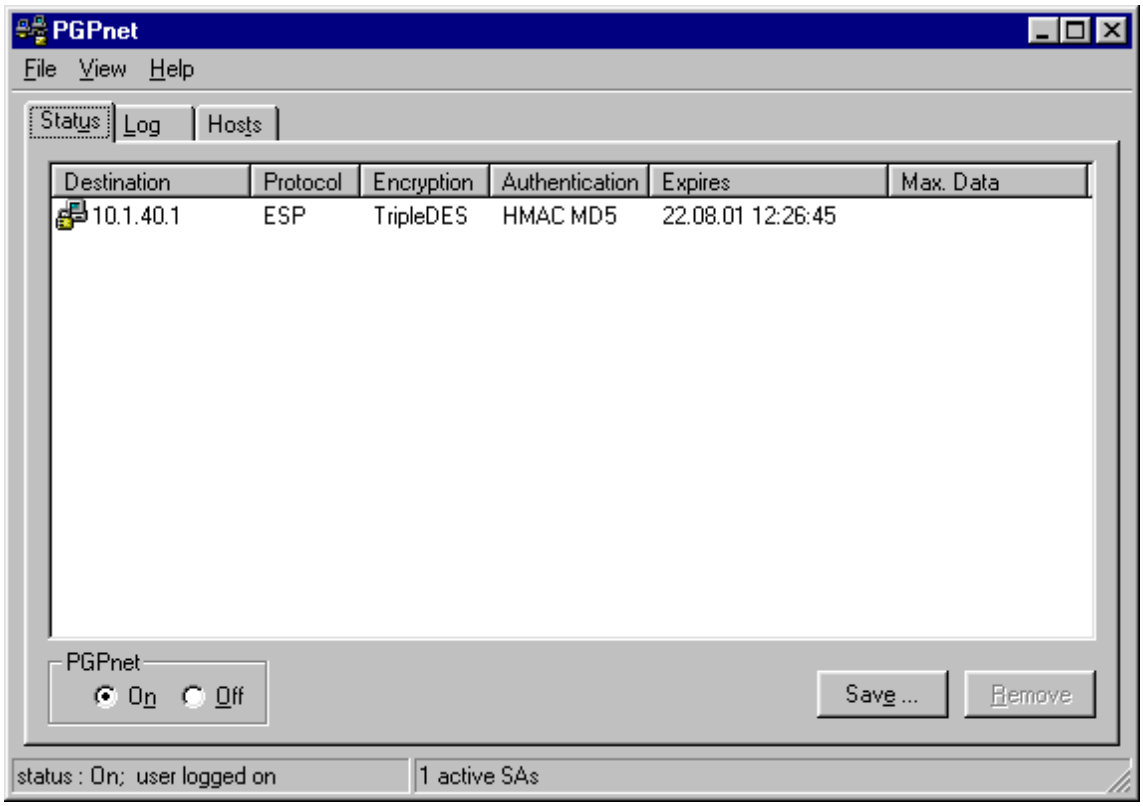

Abbildung 26: Neue Verbindung anlegen - 4

Verbindung hergestellt

1.2 PGPnet Version 7.0.3

1.2.1 Vorhandene Schlüssel in PGPnet importieren

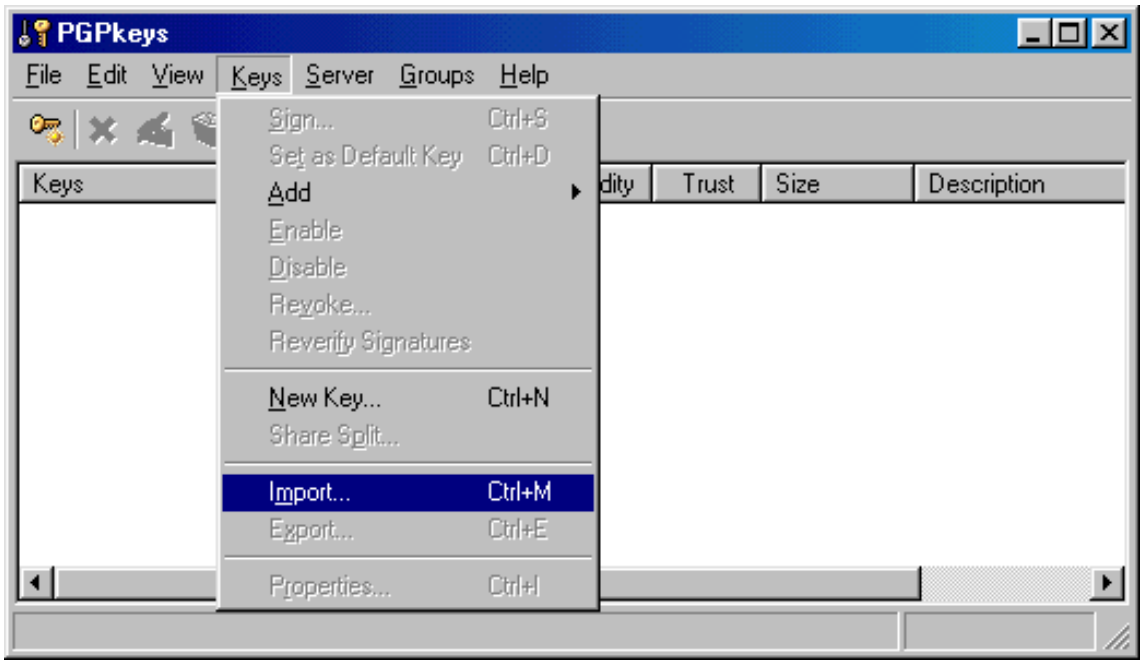

Abbildung 27: Schlüssel importieren - 1

Schlüssel importieren

Abbildung 28: Schlüssel importieren - 2

Keyring File auswählen

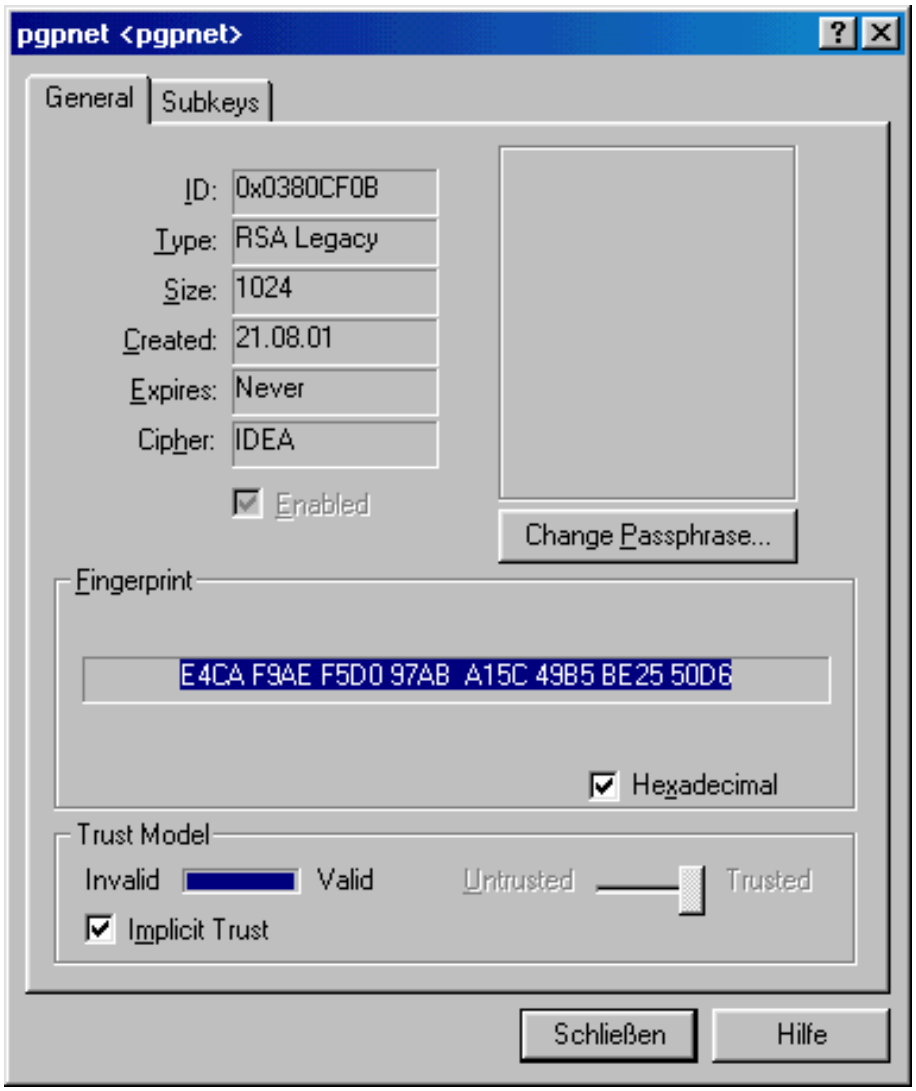

Abbildung 29: Schlüssel importieren - 3

Optionen (Key Properties) - (incl. Hexadezimalem Fingerprint)

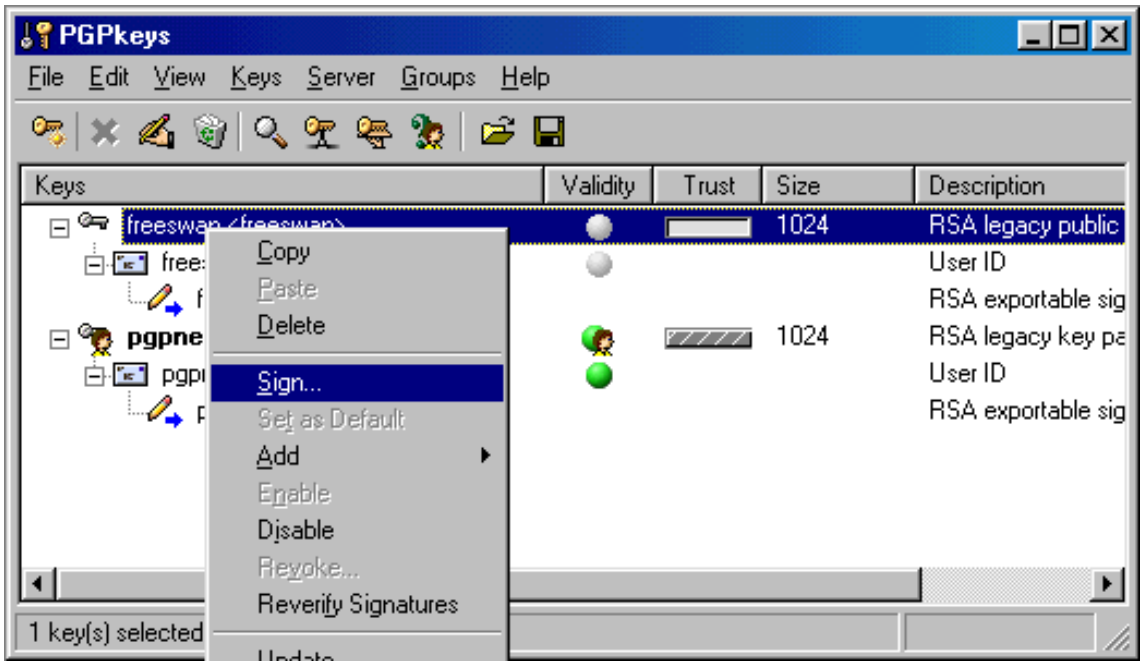

Abbildung 30: Schlüssel importieren - 4

FreeS/WAN Public Key signieren

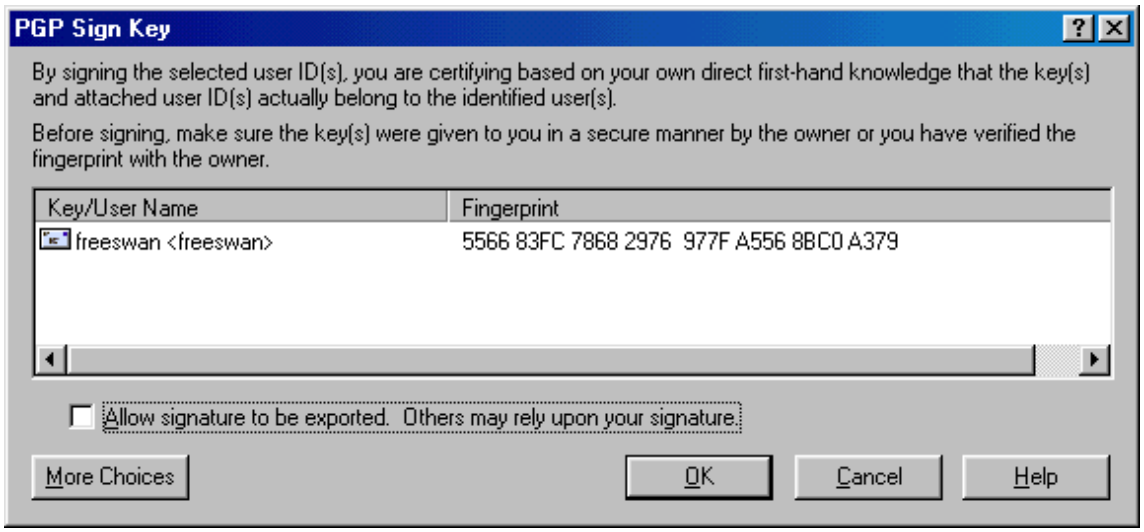

Abbildung 31: Schlüssel importieren - 5

Bestätigung der Unterzeichnung

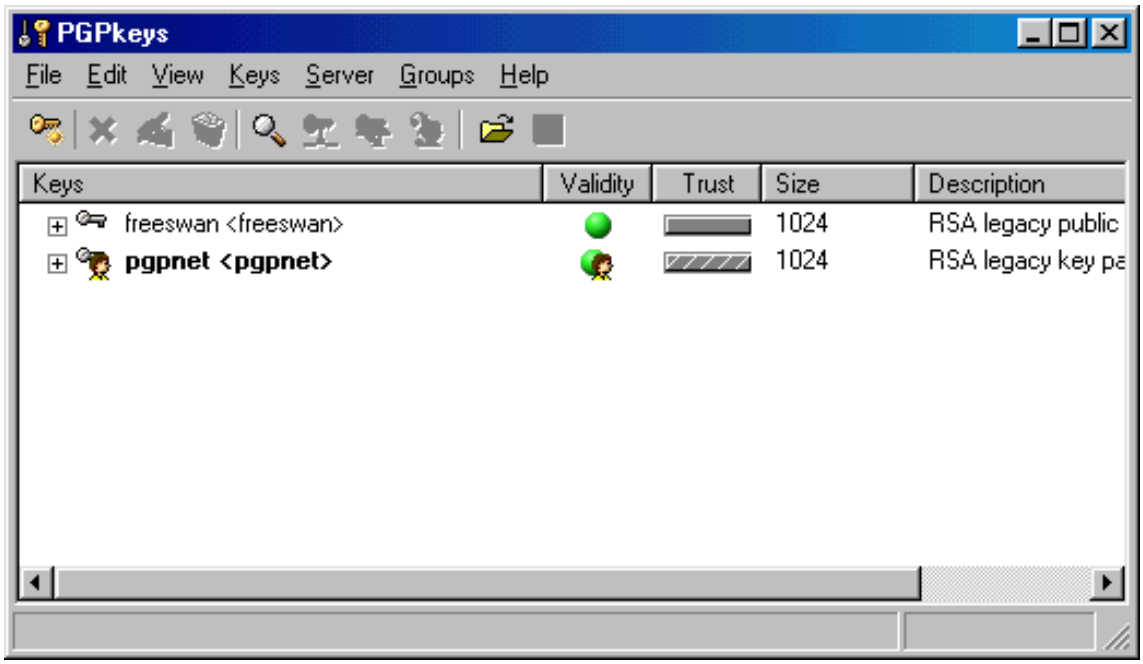

Abbildung 32: Schlüssel importieren - 6

Konfigurierte Schlüssel

1.2.2 Konfigurieren von PGPnet

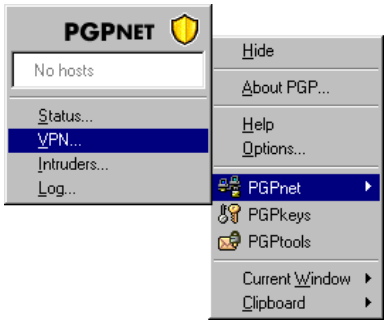

Abbildung 33: Optionen anpassen - 1

VPN wählen (Tray-Icon)

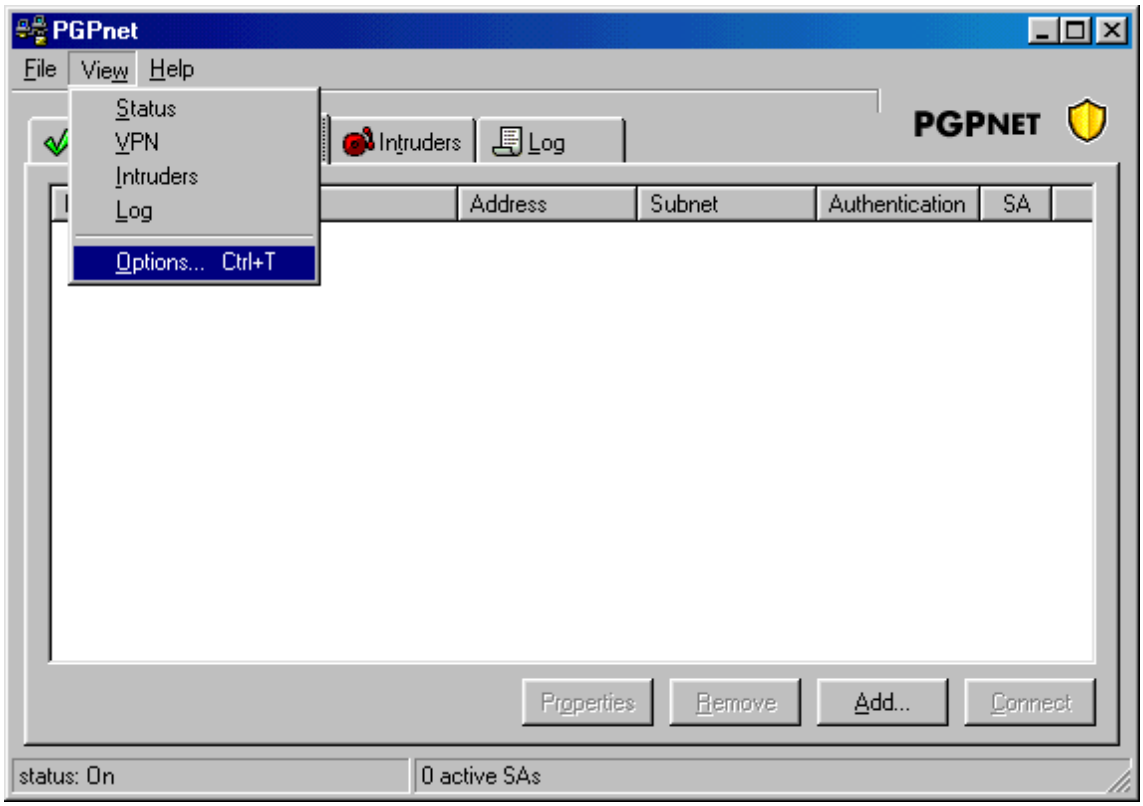

Abbildung 34: Optionen anpassen - 2

Optionen

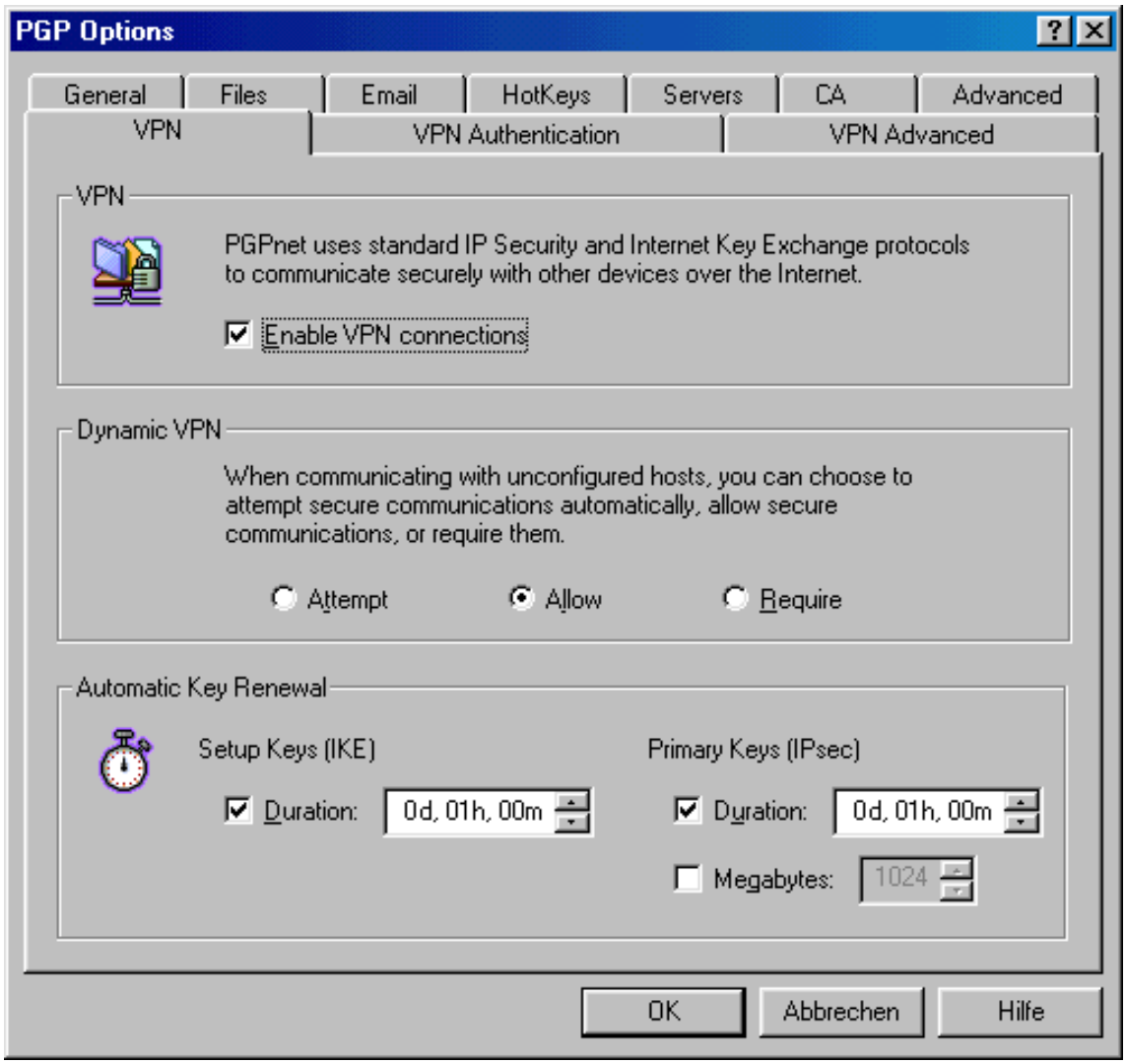

Abbildung 35: Optionen anpassen - 3

Optionen - „VPN“

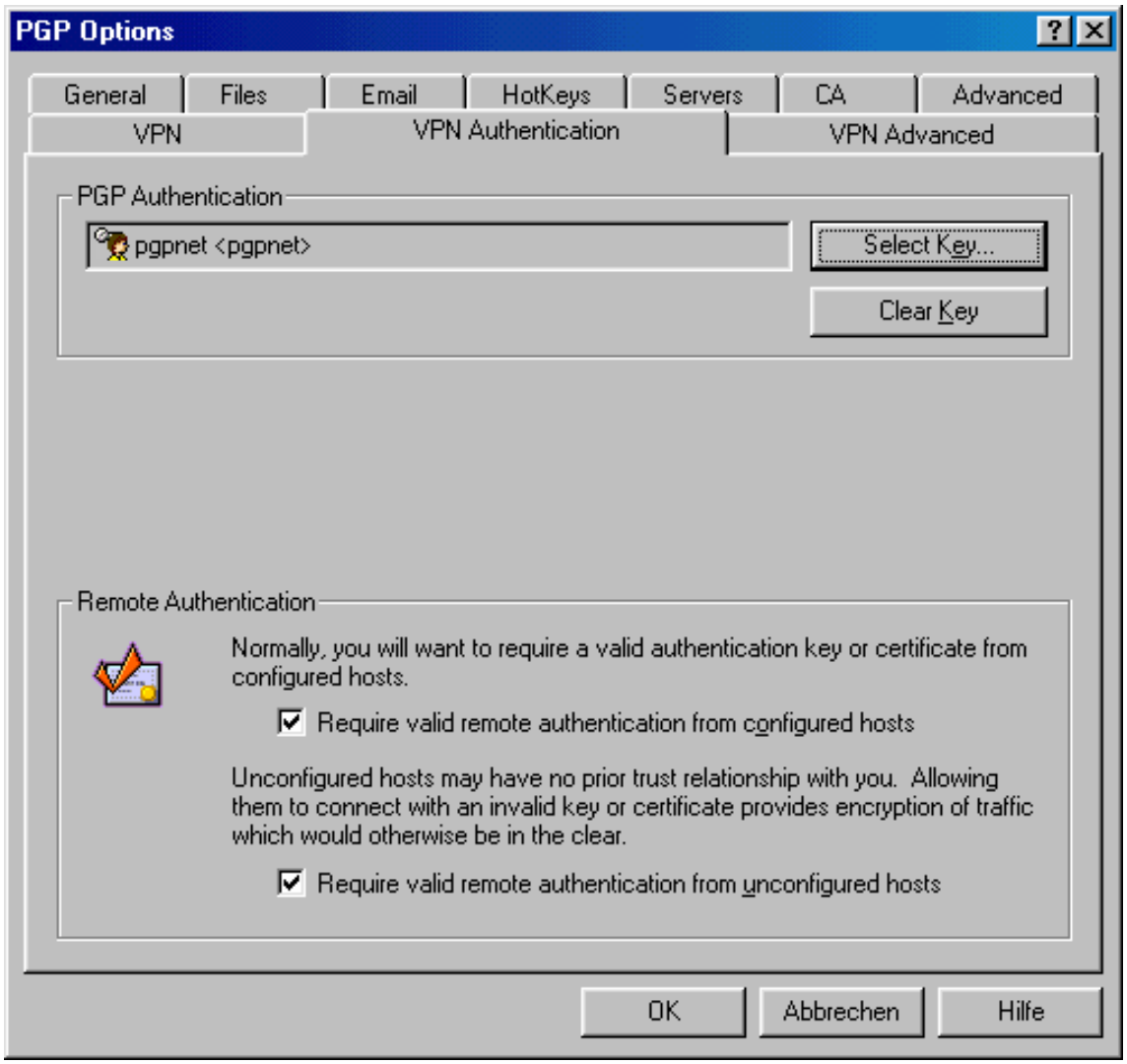

Abbildung 36: Optionen anpassen - 4

Optionen - „VPN Authentication“

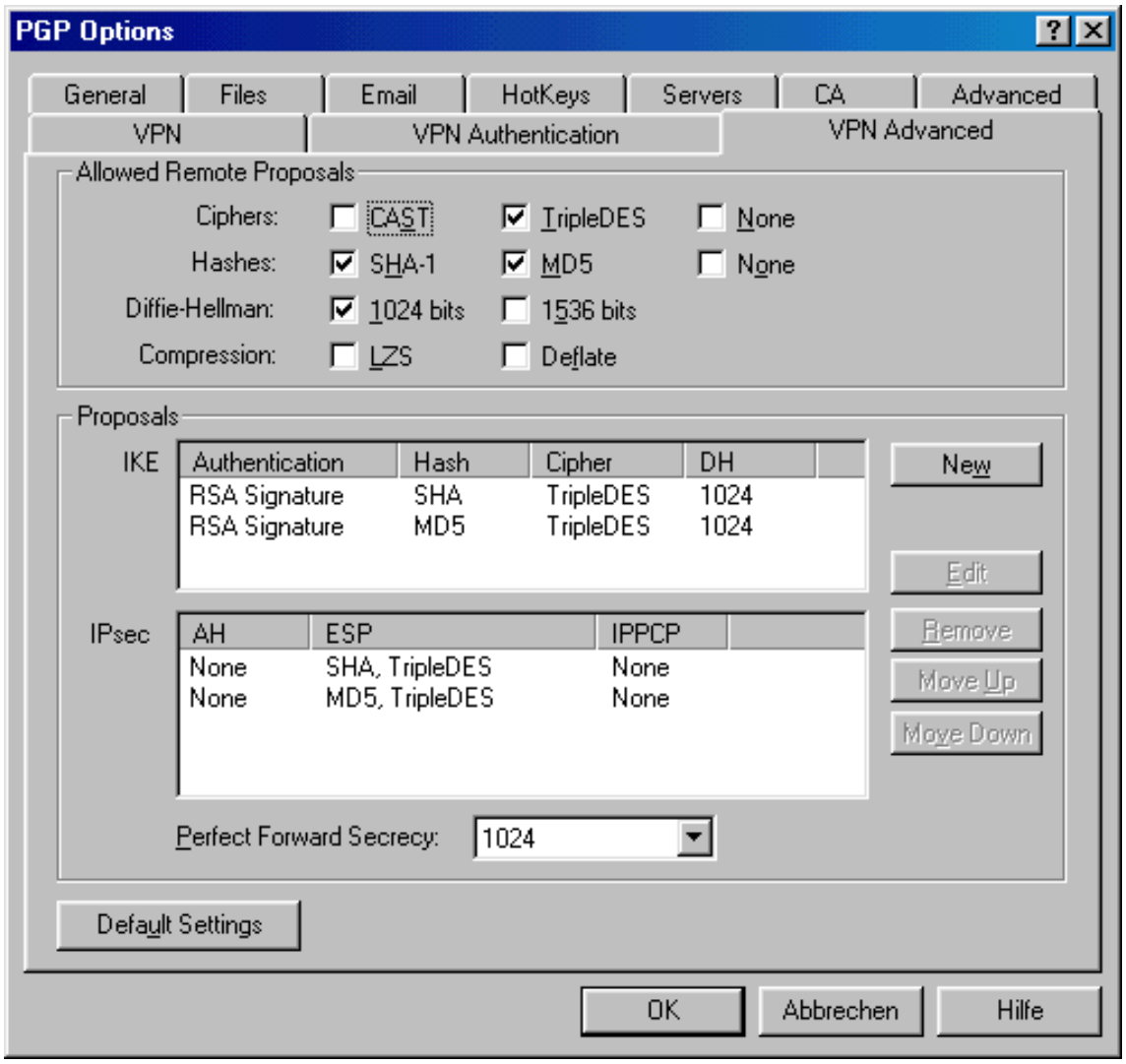

Abbildung 37: Optionen anpassen - 5

Optionen - „VPN Advanced“

1.2.3 Hinzufügen einer neuen Verbindung

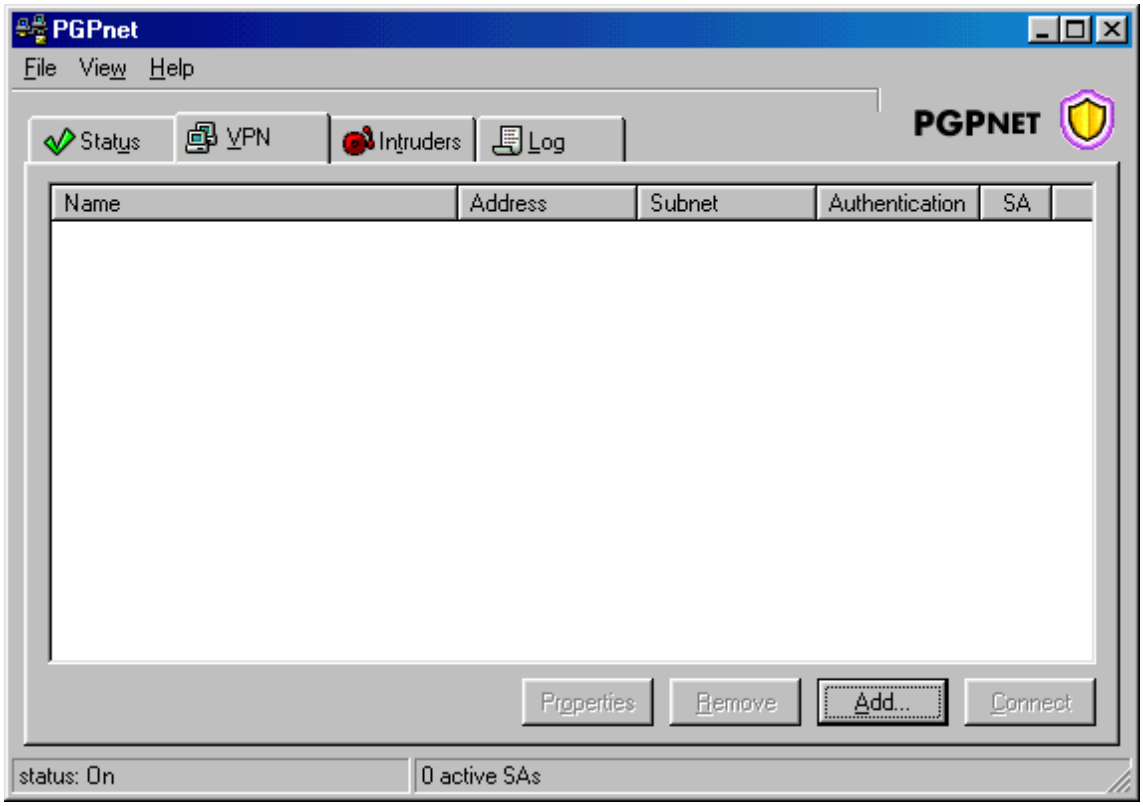

Abbildung 38: Neue Verbindung anlegen - 1

PGPnet Grundfenster

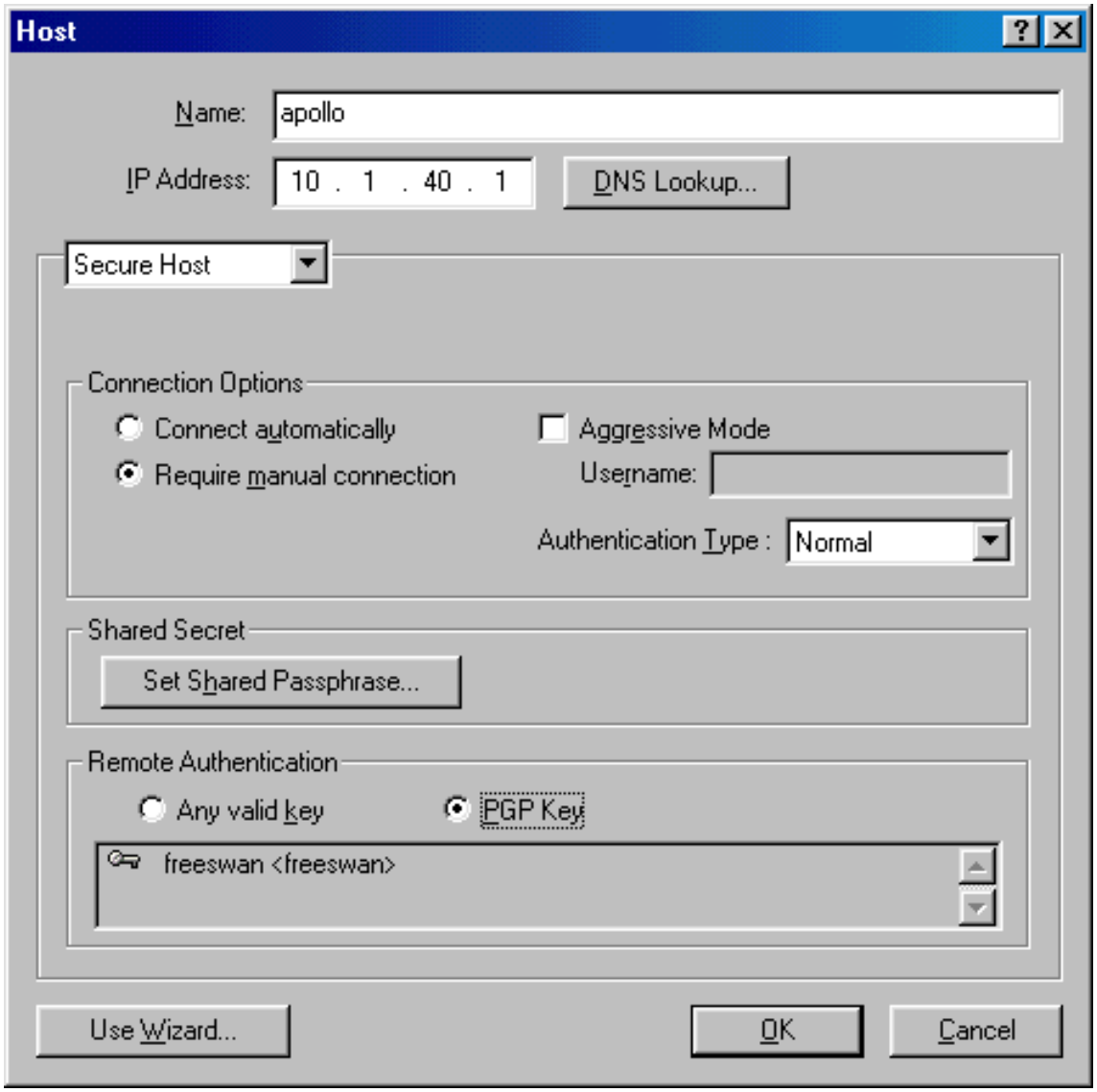

Abbildung 39: Neue Verbindung anlegen - 2

Neue Verbindung anlegen (Expert Mode)

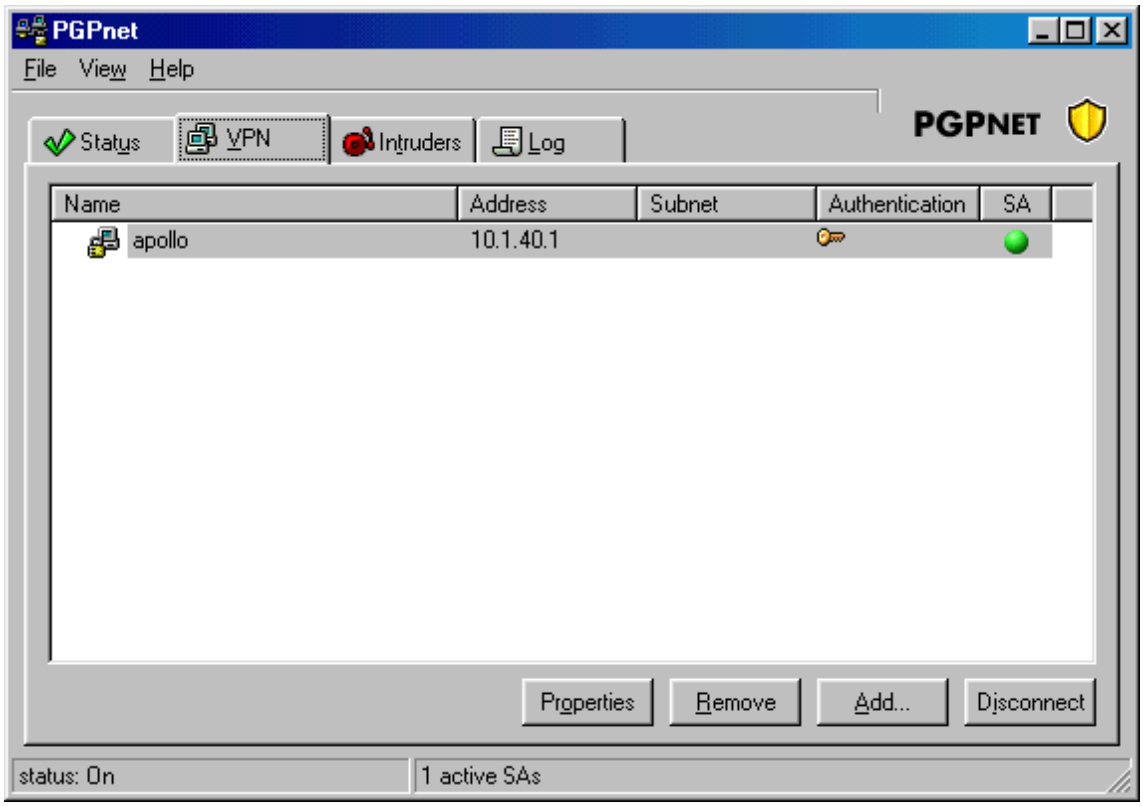

Abbildung 40: Neue Verbindung anlegen - 3

Verbindung herstellen (Connect)

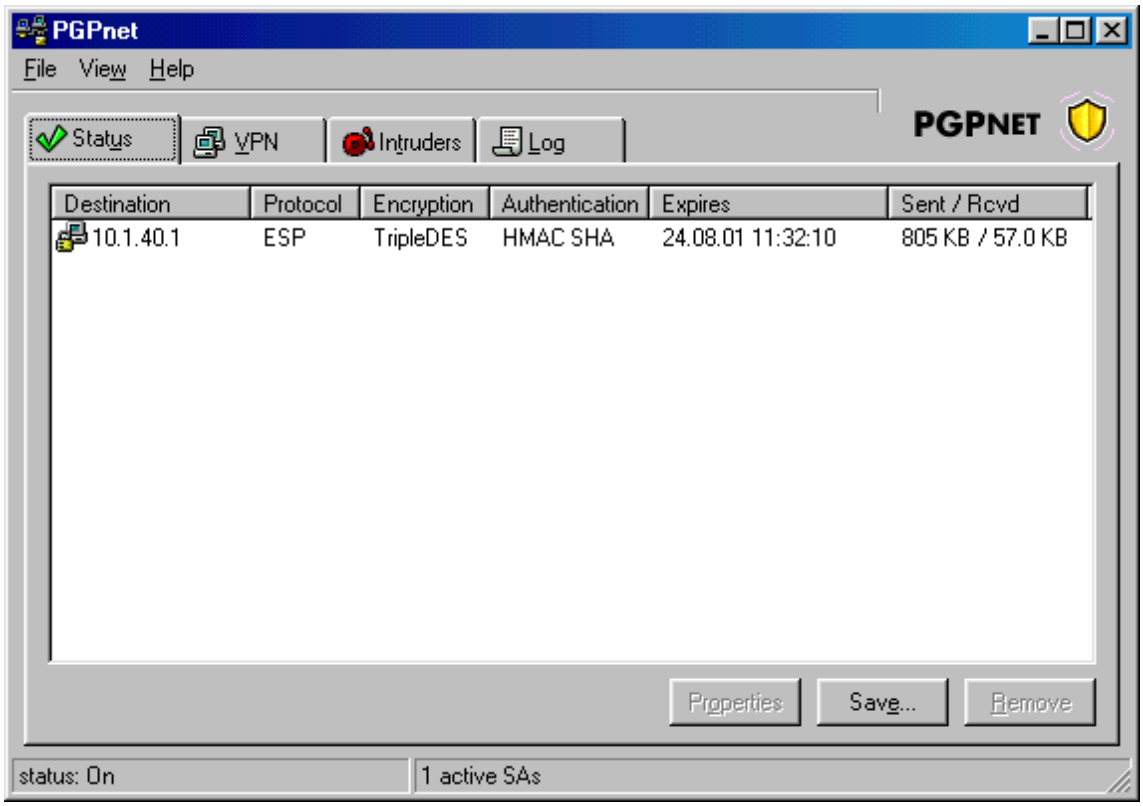

Abbildung 41: Neue Verbindung anlegen - 4

Verbindung hergestellt (Status)