

SSHv2

Andreas Aurand
Network Consultant NWCC, HP

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Agenda

- Übersicht
- SSH-Architektur
 - Transport-Protokoll
 - User-Authentication-Protokoll
 - Connection-Protokoll
- TCP Forwarding
- X11 Forwarding
- SSH und SOCKS

March 31, 2005 Andreas Aurand, HP Network Competence Center 2



SSH-Implementierungen

- **Tru64**
 - Kommerzielle SSH2-Implementation von SSH.COM
 - PublicKey-Authentifizierung unterstützt X.509-Zertifikate
- **OpenVMS**
 - Bestandteil von TCP/IP für OpenVMS
 - Gleiche Implementation wie unter Tru64
 - Keine PublicKey-Authentifizierung mittels Zertifikate möglich
 - Alle Befehle mit "_" anstatt mit "-"
 - Optionen in Großbuchstaben benötigen Gänsefüßchen
- **OpenSSH**
 - Open-Source-Implementation
 - Auf fast allen Plattformen verfügbar

March 31, 2005

Andreas Aurand, HP Network Competence Center

3



SSH-Kommandos unter OpenVMS

- [SYS\\$COMMON:\[SYSMGR\]TCPIP\\$DEFINE_COMMANDS.COM](#)
- `scp*2 ::= 'fedit("sys$system:tcpip$ssh_scp2.exe", "upcase")'`
- `sftp*2 ::= 'fedit("sys$system:tcpip$ssh_sftp2.exe", "upcase")'`
- `ssh*2 ::= 'fedit("sys$system:tcpip$ssh_ssh2.exe", "upcase")'`
- `ssh_add*2 ::= 'fedit("sys$system:tcpip$ssh_ssh-add2.exe", "upcase")'`
- `ssh_agent*2 ::= 'fedit("sys$system:tcpip$ssh_ssh-agent2.exe", "upcase")'`
- `ssh_keygen*2 ::= 'fedit("sys$system:tcpip$ssh_ssh-keygen2.exe", "upcase")'`
- Optionen in Großbuchstaben benötigen Gänsefüßchen
 - `ssh_keygen2 "-F" xxx.pub`

March 31, 2005

Andreas Aurand, HP Network Competence Center

4



SSH Konfigurationsdateien

- **SSH-Server**

- Tru64 `/etc/ssh2/sshd2_config`
- OpenVMS `TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]sshd2_config.;`
- OpenSSH `/usr/local/etc/sshd_config`

- **SSH-Client**

- Tru64
 - Global `/etc/ssh2/ssh2_config`
 - Benutzer `$HOME/.ssh2/ssh2_config`
- OpenVMS
 - Global `TCPIP$SSH_DEVICE:[TCPIP$SSH.SSH2]ssh2_config.;`
 - Benutzer `[".ssh2]ssh2_config.;`
- OpenSSH
 - Global `/usr/local/etc/ssh_config`
 - Benutzer `$HOME/.ssh/config`

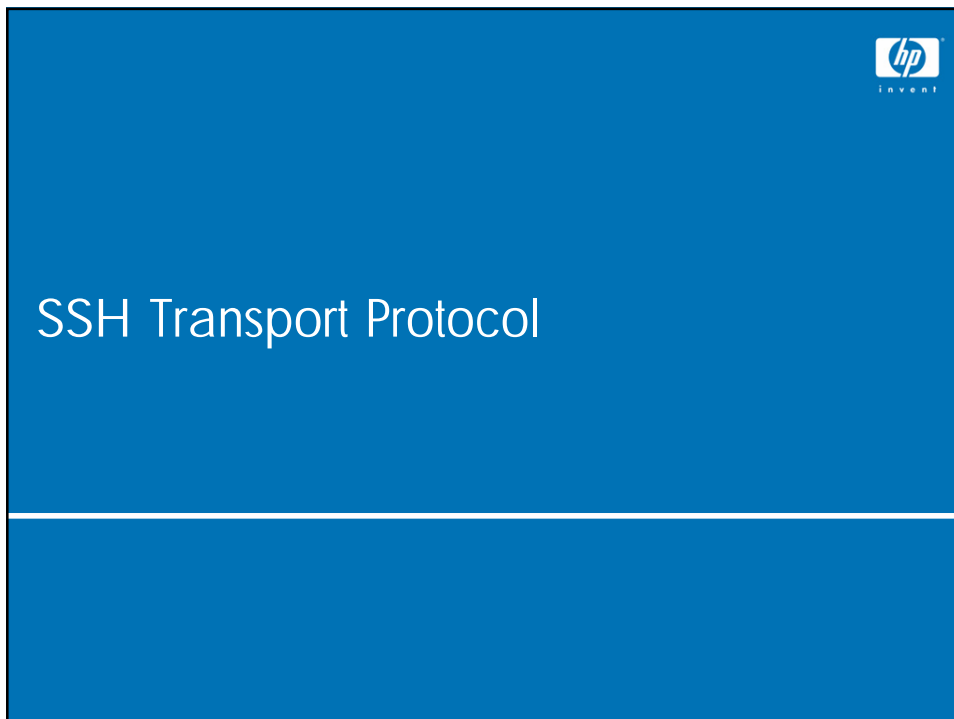
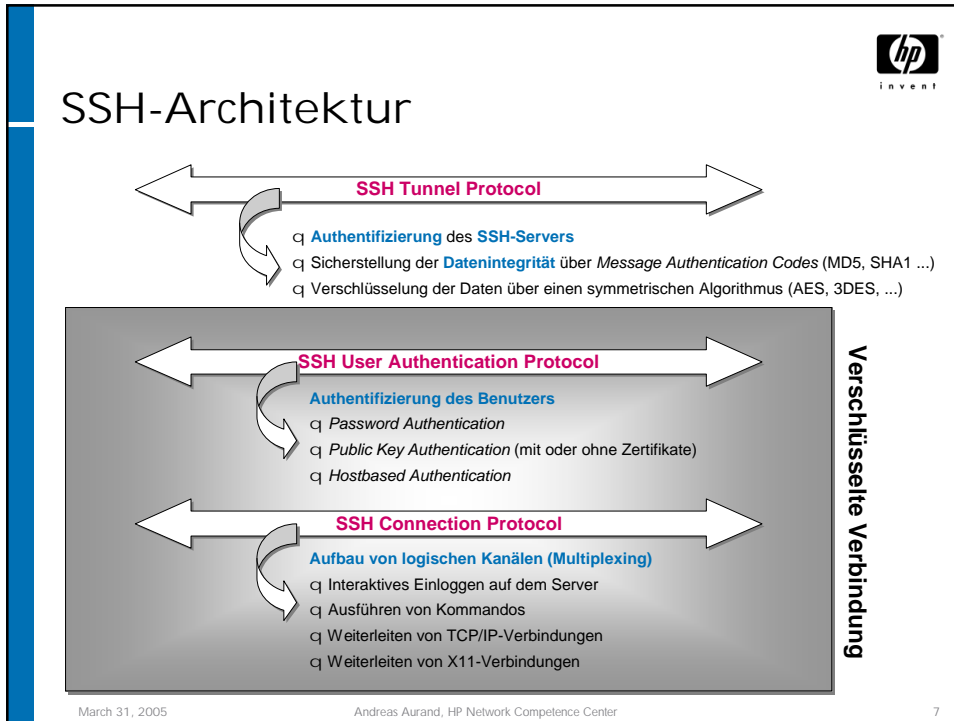
March 31, 2005


Andreas Aurand, HP Network Competence Center

5



SSH – eine Übersicht





Transport-Protokoll


- **Vertraulichkeit:** symmetrische Verschlüsselung
- **Integrität und Authentizität:** Message Authentication Code (MAC)

TCP Header (Port 22)	Packet Length 4 Octets	Padding Length 1 Octet	SSH Payload N1 (Packet Length - N2 - 1)	Random Padding N2 (Padding Length)	MAC (optional) MAC Length
-------------------------	---------------------------	---------------------------	---	--	------------------------------

Verschlüsselter Teil der SSH-Nachricht

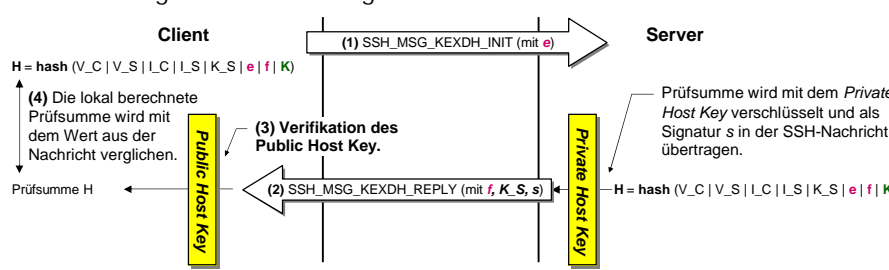
mac = MAC(key, sequence_number | unencrypted_packet)

March 31, 2005 Andreas Aurand, HP Network Competence Center 9



Transport-Protokoll

- **Authentifizierung des Servers** durch **PublicKey-Verfahren**
 - Server generiert Prüfsumme, verschlüsselt sie mit dem **Private Host Key** und hängt sie als Signatur an das SSH-Paket an.
 - Client entschlüsselt die Signatur mit dem **Public Host Key** des Servers und vergleicht sie mit lokal generierter Prüfsumme.




$H = \text{hash}(V_C | V_S | I_C | I_S | K_S | e | f | K)$

$H = \text{hash}(V_C | V_S | I_C | I_S | K_S | e | f | K)$

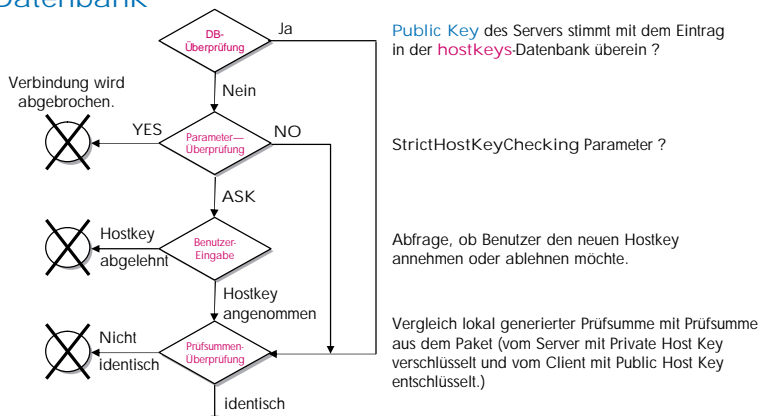
- Problem: Öffentlicher Schlüssel des Servers muss **vertrauenswürdig** sein
 - Eintrag des öffentlichen Schlüssels in **lokaler Datenbank** auf dem Client
 - Verwendung von **X.509-Zertifikaten** zur Verifikation des Schlüssels
 - Verifikation des Schlüssels durch **DNS SSHFP Resource Record**

March 31, 2005 Andreas Aurand, HP Network Competence Center 10




Transport-Protokoll

- Überprüfung des öffentlichen Schlüssels über Eintrag in lokaler Datenbank



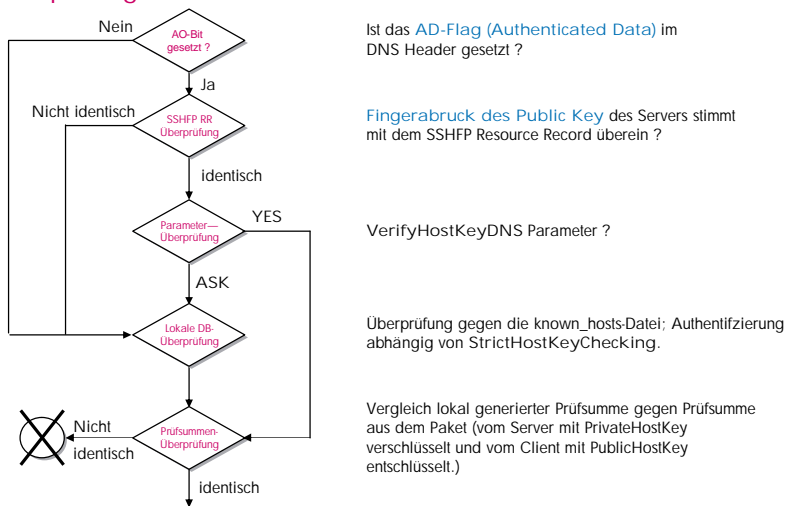
Diffie-Hellman-Schlüsselaustauschprotokoll

March 31, 2005 Andreas Aurand, HP Network Competence Center 11



Transport-Protokoll

- Überprüfung des Schlüssels über DNS SSHFP Resource Record



Diffie-Hellman-Schlüsselaustauschprotokoll

March 31, 2005 Andreas Aurand, HP Network Competence Center 12



ServerHostKey generieren

- Tru64 und OpenVMS

- **ssh-keygen2 -b 2048 -t dsa -P /etc/ssh2/hostkey**

- -P : Privater Schlüssel wird ohne Passphrase abgespeichert
- -b : Größe des Schlüssels
- -t : Typ des Schlüsselpaares (rsa | dsa)

```
Generating 2048-bit dsa key pair
4 .oOo.oOo.oOo
Key generated.
2048-bit dsa, root@tru64.lab.net, Tue Oct 26 2004 12:16:13 +0200
Private key saved to /etc/ssh2/hostkey
Public key saved to /etc/ssh2/hostkey.pub
```

- Fingerprint des Schlüssels

- **ssh-keygen2 -F /etc/ssh2/hostkey.pub**

```
Fingerprint for key:
xuveh-memiz-cuzab-batev-zelim-kymek-hudef-gidec-nekes-kamuv-laxix
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

13



ServerHostKey generieren

- OpenSSH

- **linux:/usr/local/etc # ssh-keygen -b 2048 -t dsa**

- -b : Größe des Schlüssels
- -t : Typ des Schlüsselpaares (rsa, dsa oder rsa1 für SSHv1)

```
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa):
/usr/local/etc/ssh_host_dsa_key
Enter passphrase (empty for no passphrase):  Privater Schlüssel darf nicht über
Enter same passphrase again:  Passphrase geschützt werden
Your identification has been saved in /usr/local/etc/ssh_host_dsa_key.
Your public key has been saved in /usr/local/etc/ssh_host_dsa_key.pub.
```

- Fingerprint des Schlüssels

- **linux:/usr/local/etc # ssh-keygen -l -f ssh_host_dsa_key.pub**

```
2048 a3:2b:f8:ff:ac:e3:f7:14:d7:45:93:a4:13:03:0e:a1 ssh_host_dsa_key.pub
```


- **linux:/usr/local/etc # ssh-keygen -B -f ssh_host_dsa_key.pub**

```
2048 xohar-nulot-vekih-fufer-kineh-nasas-tuzyc-rigil-kyteg-cofot-gaxox ssh_host_dsa_key.pub
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

14



Vertrauenswürdige Instanz: lokale Client-Datenbank

- Öffentlicher HostKey des Servers auf Client eintragen
 - Tru64 und OpenVMS
 - Im Verzeichnis `$HOME/.ssh2/hostkeys`
 - Kein globales hostkeys-Verzeichnis

```


-rw----- 1 andreas users 1272 Oct 28 09:30 key_22_tru64.pub
-rw----- 1 andreas users 753 Oct 26 13:02 key_22_ovms1.pub
-rw----- 1 andreas users 1271 Nov 18 11:25 key_22_linux.pub

tru64> cat $HOME/.ssh2/hostkeys/key_22_ovms1.pub
---- BEGIN SSH2 PUBLIC KEY ----
Subject: andreas
Comment: "host key for ovms1, accepted by andreas Tue Oct 26 2004 13:02:04+0200"
AAAAB3NzaC1kc3MAAACBALV9YgFMS4eLMroyUdFI+IPrWERdHwgOC9mtuwO71DEaoHocx5
... ..
+w9/VA4A1laMXNyJ02M=
---- END SSH2 PUBLIC KEY ----

```

- OpenSSH
 - Alle Schlüssel werden in einer Datei abgelegt
 - Lokal für einen Benutzer: `$HOME/.ssh/known_hosts`
 - Global für alle Benutzer: `/usr/local/etc/ssh_known_hosts`

March 31, 2005 Andreas Aurand, HP Network Competence Center 15



Vertrauenswürdige Instanz: lokale Client-Datenbank

- Falls öffentlicher Schlüssel des Servers nicht vorliegt, kann der Client ihn automatisch eintragen
 - Parameter `StrictHostKeyChecking = yes | ask`

```

tru64> ssh2 linux
Host key not found from database.
Key fingerprint:
xohar-nulot-vekih-fufer-kineh-nasas-tuzyc-rigil-kyteg-cofot-gaxox
You can get a public key's fingerprint by running
% ssh-keygen -F publickey.pub
on the keyfile.
Are you sure you want to continue connecting (yes/no)? yes
Host key saved to /usr/local/users/andreas/.ssh2/hostkeys/key_22_linux.pub
host key for linux, accepted by andreas Thu Nov 18 2004 11:25:29 +0100

```


- Aus Sicherheitsgründen sollte man Fingerabdruck des Schlüssels verifizieren

```

linux# ssh-keygen -B -f /usr/local/etc/ssh_host_dsa_key.pub
2048 xohar-nulot-vekih-fufer-kineh-nasas-tuzyc-rigil-kyteg-cofot-gaxox ssh_host_dsa_key.pub

```

March 31, 2005 Andreas Aurand, HP Network Competence Center 16



Vertrauenswürdige Instanz: SSHFP Resource Record (nur OpenSSH)


- SSH Client überprüft den Fingerprint des empfangenen Schlüssels gegen einen DNS SSHFP RR
 - Fingerprint** des öffentlichen Schlüssels erzeugen


```
ssh-keygen -r linux.frs-lab.de -f /usr/local/etc/ssh_host_rsa_key.pub -g
linux.frs-lab.de IN TYPE44 \# 22 01 01 92ec4b2fc7ee225e58dc02e3a318bdc18e06a1d5

ssh-keygen -r linux.frs-lab.de -f /usr/local/etc/ssh_host_dsa_key.pub -g
linux.frs-lab.de IN TYPE44 \# 22 02 01 94b99fde18530fb66659b3cdbe1bd076b5410dd4
```
 - Fingerprint** in die Zonen-Datei des DNS-Servers eintragen


```
linux                A            192.168.28.197
                    TYPE44  \# 22 ( 010192EC4B2FC7EE225E58DC02E3A318BDC18E06A1D5 )
                    TYPE44  \# 22 ( 020194B99FDE18530FB66659B3CDBE1BD076B5410DD4 )
```
- Problem: DNS Response des Servers sollte über einen sicheren Weg empfangen werden (Schutz gegen MitM)
 - Empfohlen: DNS TSIG oder SIG(0) Authentifizierung bzw. IPsec

March 31, 2005 Andreas Aurand, HP Network Competence Center 17



Konfiguration - SSH-Server

- Tru64 und OpenVMS (sshd2_config)
 - HostKeyFile** filename
 - Specifies the file containing the private host key. The default file `/etc/ssh2/hostkey`.
 - PublicHostKeyFile** filename
 - Specifies the name of the file containing the public host key. The default is the `/etc/ssh2/hostkey.pub` file.
- OpenSSH (sshd_config)
 - HostKey** filename
 - Specifies a file containing a private host key used by SSH. The defaults are
 - `/usr/local/etc/ssh_host_key` (SSHv1)
 - `/usr/local/etc/ssh_host_rsa_key` (SSHv2 mit RSA)
 - `/usr/local/etc/ssh_host_dsa_key` (SSHv2 mit DSA)
 - Zugehöriger öffentlicher Schlüssel hat immer die Endung `.pub`.

March 31, 2005 Andreas Aurand, HP Network Competence Center 18



Konfiguration - SSH-Client

- Tru64 und OpenVMS (ssh_config)
 - **StrictHostKeyChecking** yes/no/ask
 - Specifies whether the client automatically adds new host keys to the `$HOME/.ssh2/hostkeys` file.
- OpenSSH (ssh_config oder config)
 - **GlobalKnownHostsFile** filename
 - Specifies a file to use for the global host key database instead of `/usr/local/etc/ssh_known_hosts`
 - **UserKnownHostsFile** filename
 - Specifies a file to use for the user host key database instead of `$HOME/.ssh/known_hosts`
 - **StrictHostKeyChecking** yes/no/ask
 - If this flag is set to "yes", ssh will never automatically add host keys to the `$HOME/.ssh/known_hosts` file, and refuses to connect to hosts whose host key has changed. The host keys of known hosts will be verified automatically in all cases.


March 31, 2005

Andreas Aurand, HP Network Competence Center

19




SSH User Authentication Protocol



User Authentication Protocol

- Authentifizierung des Client-Benutzers auf dem Server
- Password-Authentifizierung
- PublicKey-Authentifizierung
 - über lokale Datenbank
 - über X.509-Zertifikat
 - über ActivCard
- HostBased-Authentifizierung
- weitere Methoden wie Kerberos, GSSAPI usw.

March 31, 2005 Andreas Aurand, HP Network Competence Center 21



Authentifizierungsmechanismus festlegen

- Tru64 und OpenVMS
 - AllowedAuthentications password
 - AllowedAuthentications publickey
 - AllowedAuthentications hostbased
 - RequiredAuthentications auth1,auth2,...

Mechanismen, die ein Benutzer durchlaufen muss.

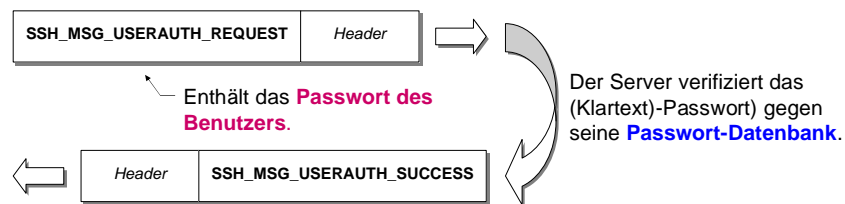
- OpenSSH
 - PasswordAuthentication yes/no
 - PubkeyAuthentication yes/no
 - HostbasedAuthentication yes/no

March 31, 2005 Andreas Aurand, HP Network Competence Center 22



Password-Authentifizierung

- Client sendet ein **Klartext-Passwort**, das auf dem Server verifiziert wird (z.B. gegen die Benutzerdatenbank)
 - Oft einzige Authentifizierungsmethode bei Routern, Switches usw.
- Da das Authentifizierungsprotokoll die verschlüsselte SSH-Transportverbindung benutzt, ist das Passwort nicht sichtbar.



March 31, 2005

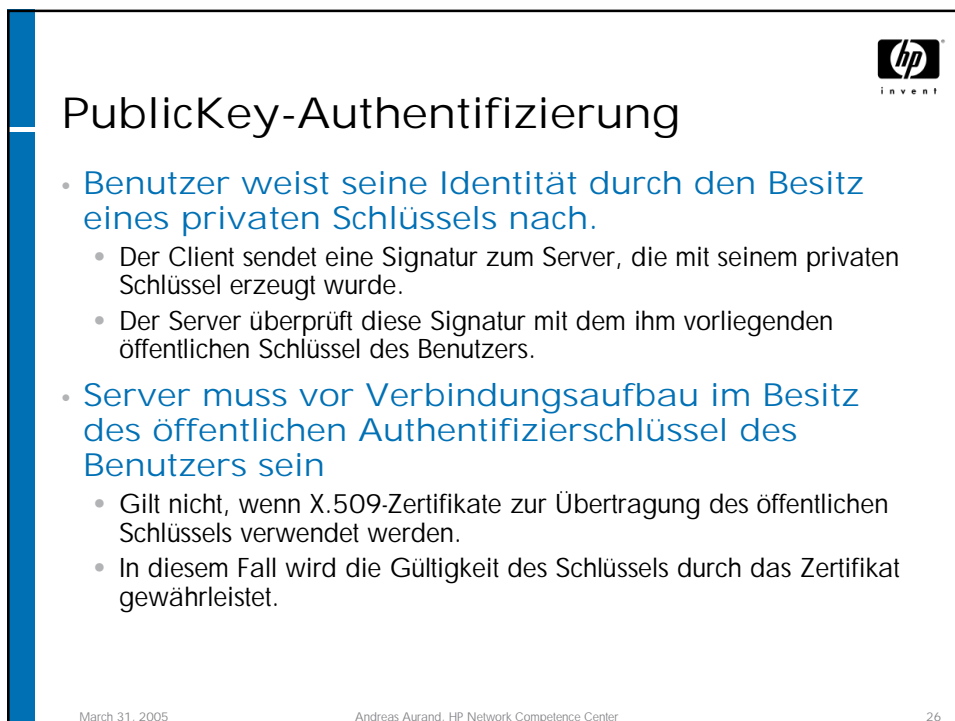
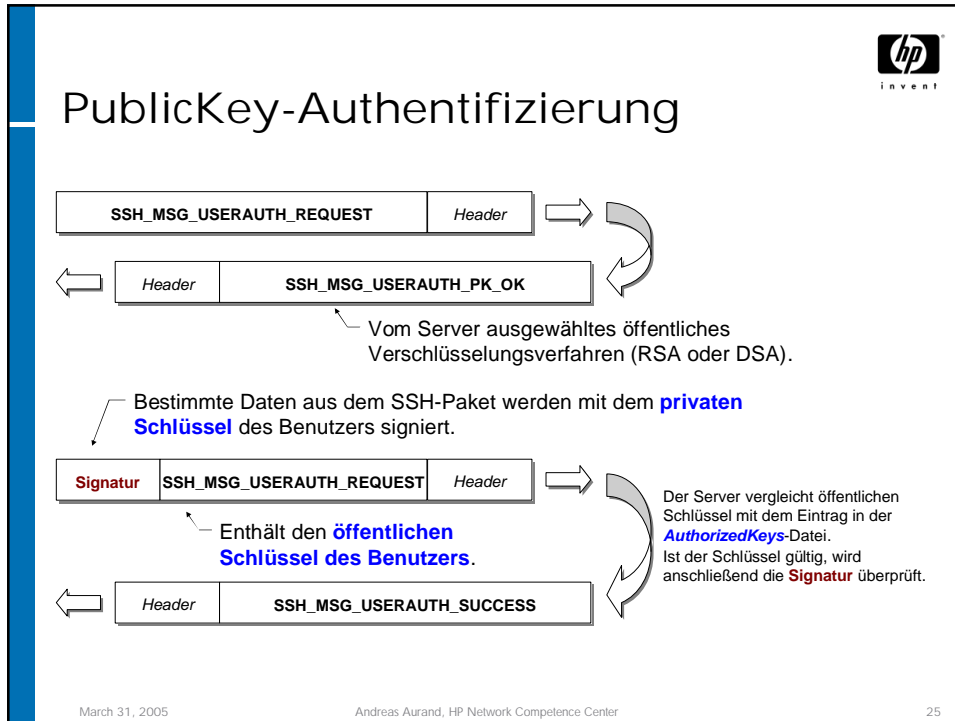
Andreas Aurand, HP Network Competence Center

23



SSH User Authentication Protocol

PublicKey-Authentifizierung





Konfiguration - SSH-Client

- Schlüsselpaar unter Tru64 und OpenVMS erzeugen

- **ssh-keygen2 -t dsa -b 2048**

```
Generating 2048-bit dsa key pair
 7 o.o0o.o0o.o0
Key generated.
2048-bit dsa, andreas@tru64.lab.net, Tue Oct 26 2004 11:19:36 +0200
Passphrase : ✓ Privater Schlüssel sollte über Passphrase geschützt werden
Again      :
Private key saved to /usr/local/users/andreas/.ssh2/id_dsa_2048_a
Public key saved to /usr/local/users/andreas/.ssh2/id_dsa_2048_a.pub
```

- Schlüsselpaar unter OpenSSH erzeugen

- **ssh-keygen -t dsa -b 2048**

```
Generating public/private dsa key pair.
Enter file in which to save the key (/home/andreas/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/andreas/.ssh/id_dsa.
Your public key has been saved in /home/andreas/.ssh/id_dsa.pub.
The key fingerprint is:
1a:38:35:f3:b7:db:30:15:66:7c:73:16:81:30:57:db andreas@linux
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

27



Konfiguration - SSH-Client

- Tru64- und OpenVMS

- Eintrag der zur Verfügung stehenden **privaten Schlüssel** des Benutzers als **IdKey** in die Datei **identification**
 - Datei wird über **IdentityFile**-Eintrag in ssh2_config festgelegt.
- Der zugehörige **öffentliche Schlüssel** hat die Endung **".pub"**

```
tru64> cat identification
IdKey id_dsa_2048_a
tru64> ls -l id*
-rw----- 1 andreas users      1412 Oct 26 11:19 id_dsa_2048_a
-rw-r--r-- 1 andreas users      1272 Oct 26 11:19 id_dsa_2048_a.pub
```

- OpenSSH

- Eintrag der zur Verfügung stehenden **privaten Schlüssel** des Benutzers **IdentityFile** in die Konfigurationsdatei

```
linux:/home/andreas/.ssh # cat config
...
IdentityFile ~/.ssh/identity # SSHv1
IdentityFile ~/.ssh/id_rsa # SSHv2 mit RSA als Algorithmus
IdentityFile ~/.ssh/id_dsa # SSHv2 mit DSA als Algorithmus
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

28



Konfiguration - SSH-Server

- Tru64 und OpenVMS
 - Eintrag der Dateinamen der öffentlichen Schlüssel der Benutzer in die `authorized2_keys`-Datei.
 - Dateiname wird über `AuthorizationFile`-Eintrag in `sshd2_config` festgelegt.

```
tru64> cat $HOME/.ssh2/authorization2_keys
Key    andreas_linux.pub
Key    aurand_ovms1.pub

tru64> ls -l *.pub
-rw-r--r--  1 andreas  users      1235 Oct 27 15:14 andreas_linux.pub
-rw-r--r--  1 andreas  users      1264 Oct 26 12:05 aurand_ovms1.pub
```
- OpenSSH
 - Eintrag der öffentlichen Schlüssel aller Benutzer in `authorized_keys`-Datei.
 - Dateiname wird über `AuthorizedKeysFile`-Eintrag in `sshd_config` festgelegt.

March 31, 2005

Andreas Aurand, HP Network Competence Center

29



Schlüsselformat konvertieren

- OpenSSH verwendet anderes Format für die öffentlichen Schlüssel als die kommerziellen SSH-Implementationen
- SECSH- oder SSH2-Format in OpenSSH-Format umwandeln
 - Für Einträge in `known_hosts`- oder `authorized_keys`-Datei
 - `ssh-keygen -e -f filename`
- OpenSSH-Format in SECSH- oder SSH2-Format umwandeln
 - Für Übernahme der öffentlichen Schlüssel in `hostkeys`- und `authorization2_keys`- Verzeichnis
 - `ssh-keygen -i -f filename`

March 31, 2005

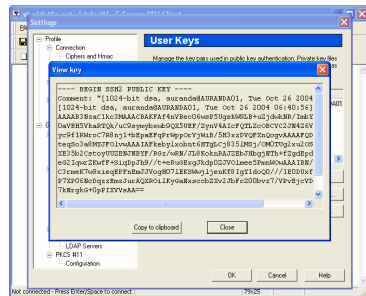
Andreas Aurand, HP Network Competence Center

30



Schlüsselformat konvertieren

- SSH2-Client (F-Secure Client unter Windows XP)



- OpenSSH-Server

```
# ssh-keygen -i -f dsa_pc.pub
```

```
ssh-dss AAAAB3NzaC1kc3MAAACBAKFAF4nVBec06wsP5UgskW9LB+uZjdwkNR/ImbYNT5JcuCigKC0aVBH5VkaRTQ...
```

```
# ssh-keygen -i -f dsa_pc.pub >> ~andreas/.ssh/authorized_keys
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

31



SSH-Agent

- **ssh-agent2 \$shell** bzw. **ssh-agent \$shell**
 - Erzeugt Subprozess und ermöglicht das **Speichern der privaten Benutzerschlüssel in Memory**
- **ssh-add2** bzw. **ssh-add**
 - Fügt privaten Schlüssel zum ssh-agent2 hinzu
 - Beim Verbindungsaufbau wird **Passphrase** nicht mehr abgefragt
 - Vereinfacht vor allem SSH-Skripte

March 31, 2005

Andreas Aurand, HP Network Competence Center

32



SSH-Agent - OpenVMS

- SSH_AGENT starten (kreiert Subprozess)

```
$ @SYS$MANAGER:TCPIP$DEFINE_COMMANDS.COM
```

```
$ ssh_agent2
```

```
%DCL-S-SPAWNED, process AURAND_73 spawned
```

```
$ ssh_add2
```

```
Adding identity: /user$root/aurand/ssh2/id_dsa_2048_a.pub
Need passphrase for "/user$root/aurand/ssh2/id_dsa_2048_a"
(2048-bit dsa, aurand@ovms1, Tue Oct 26 2004 09:14:10).
```

```
Enter passphrase:
```

```
$ ssh_add2 -l
```

```
Listing identities.
```

```
The authorization agent has one key:
```

```
id_dsa_2048_a: 2048-bit dsa, aurand@ovms1, Tue Oct 26 2004 09:14:10
```

- Beim Aufruf von SSH wird keine Passphrase mehr abgefragt

```
$ ssh2 andreas@unix1
```

```
Authentication successful.
```

```
andreas@unix1 >
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

33



SSH-Agent - Tru64 / OpenSSH

- Eintrag im Initialization File der Shell

```
eval `ssh-agent2 -s`  
ssh-add2
```

```
eval `ssh-agent -s`  
ssh-add
```

```
-c Generate C-shell commands on stdout  
-s Generate Bourne shell commands on stdout
```

- Beim Einloggen wird Passphrase des privaten Schlüssels abgefragt

```
...  
Agent pid 15701  
Adding identity: /usr/local/users/andreas/.ssh2/id_dsa_2048_a.pub  
Need passphrase for /usr/local/users/andreas/.ssh2/id_dsa_2048_a  
(2048-bit dsa, andreas@unix1, Tue Oct 26 2004 11:19:36+0200).
```

```
Enter passphrase:
```

```
unix1 > ssh-add2 -l
```

```
Listing identities.
```


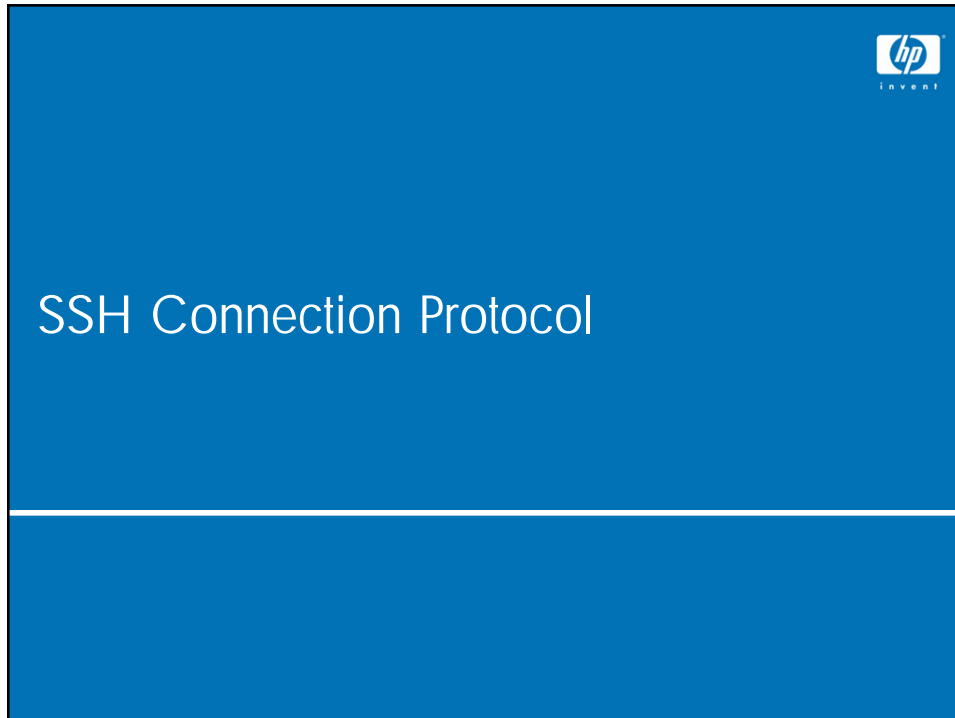
```
The authorization agent has one key:
```

```
id_dsa_2048_a: 2048-bit dsa, andreas@unix1, Tue Oct 26 2004 11:19:36 +0200
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

34



SSH Connection Protocol

- Baut die eigentlichen **Applikationsverbindungen (Channels)** zwischen Client und Server auf
 - Werden alle über die verschlüsselte und authentifizierte SSH-Tunnelverbindung gebündelt
- Folgende Applikationen sind unterstützt
 - Interaktive Verbindungen (Remote Shell)
 - Remote Command Execution
 - Weiterleiten von TCP-Verbindungen
 - Weiterleiten von X.11-Verbindungen
 - Starten eines Subsystems (z.B. SFTP)

March 31, 2005 Andreas Aurand, HP Network Competence Center 36



SSH Connection Protocol

- **Remote Shell**
 - Tru64 und OpenVMS
 - `ssh2 [-l username] nodename`
 - OpenSSH
 - `ssh [-l username] nodename`

- **Remote Command Execution**
 - Tru64 und OpenVMS
 - `ssh2 [-l username] nodename command`
 - OpenSSH
 - `ssh [-l username] nodename command`

March 31, 2005

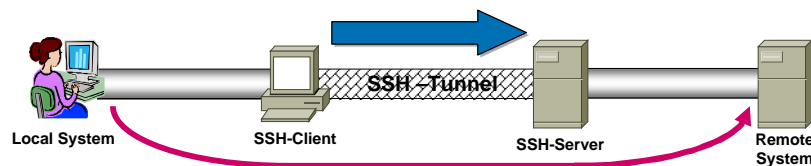
Andreas Aurand, HP Network Competence Center

37

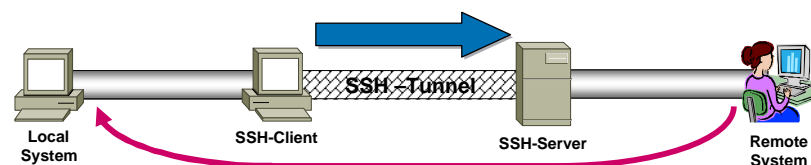


TCP Forwarding

- Local Forward




- Remote Forward



March 31, 2005


Andreas Aurand, HP Network Competence Center

38




TCP Local Forwarding


- Aufbau des SSH-Tunnels ohne Einloggen (Listen Port auf SSH-Client)



tru64
SSH-Client



(9609) SSH-Tunnel (22)




linux
SSH-Server


```

tru64 > ssh2 -f -S -o "GatewayPorts yes" -Ltcp/8011:web.frs-lab.de:80 linux.hp.com
Authentication successful.
tru64 > netstat -an | grep 22
tcp        0      0 192.168.28.198.9609    192.168.28.196.22    ESTABLISHED
tru64 > netstat -an | grep 8011
tcp        0      0 *.8011                *.*                  LISTEN
    
```


- Local Forward Port benutzen (http://tru64:8011/)




Benutzer auf PC




tru64 (SSH-Client)




linux (SSH-Server)




web.frs-lab.de



(1397) TCP (8011)



(9609) SSH-Tunnel (22)




(32859) TCP (80)

```


tru64 > netstat -an | grep 8011
tcp        0      0 10.137.28.189.8011    10.137.76.11.1373    ESTABLISHED
linux # netstat -an | grep 80
tcp        0      0 192.168.28.196:32859  192.168.28.197:80    ESTABLISHED
    
```

March 31, 2005 Andreas Aurand, HP Network Competence Center 39




TCP Remote Forwarding


- Aufbau des SSH-Tunnels ohne Einloggen (Listen Port auf SSH-Server)



tru64
SSH-Client



(9712) SSH-Tunnel (22)




linux
SSH-Server


```

tru64 > ssh2 -f -S -Rtcp/33023:rsys.frs-lab.de:23 linux.hp.com
Authentication successful.
tru64 > netstat -an | grep 22
tcp        0      0 192.168.28.198.9712    192.168.28.196.22    ESTABLISHED
tru64 > netstat -an | grep 33023
tcp        0      0 :::33023              :::*                  LISTEN
    
```


- Remote Forward Port benutzen (telnet linux 33023)




rsys.frs-lab.de




tru64 (SSH-Client)




linux (SSH-Server)




Benutzer auf PC



(23) TCP (9716)



(9609) SSH-Tunnel (22)




(33023) TCP (3587)

```

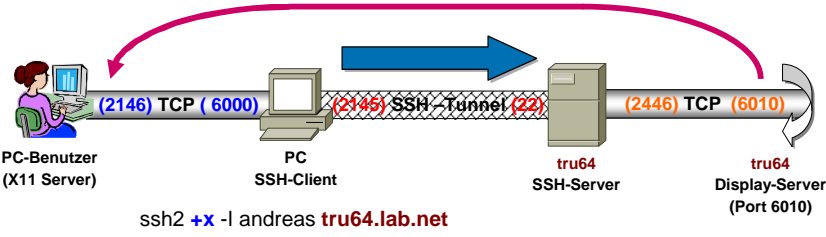
tru64 > netstat -an | grep 23
tcp        0      0 10.137.28.198.9716    10.137.28.211.23     ESTABLISHED
linux > netstat -an | grep 33023
tcp        0      0 192.168.28.199:3587   192.168.28.199:3587 ESTABLISHED
    
```

March 31, 2005 Andreas Aurand, HP Network Competence Center 40



X11 Forwarding

- Unix-Server
 - C:\> ssh2 +x -l andreas tru64.lab.net




ssh2 +x -l andreas tru64.lab.net

- OpenVMS-Server
 - C:\> ssh2 -l aurand -R tcp/6000:localhost:6010 ovms1.lab.net
 - \$ set display/create/transport=tcpip/node=localhost/server=10

TCP Port 6010

March 31, 2005 Andreas Aurand, HP Network Competence Center 41




TCP und X.11 Forwarding

- OpenVMS und Tru64 (sshd2_config)
 - GatewayPorts yes / no (in Client-Konfig. ssh2_config)
 - AllowTcpForwarding yes / no
 - AllowX11Forwarding yes / no
 - AllowTcpForwardingForGroups / DenyTcpForwardingForGroups
 - AllowTcpForwardingForUsers / DenyTcpForwardingForUsers
 - ForwardACL
- OpenSSH (sshd_config)
 - AllowTcpForwarding yes / no
 - GatewayPorts yes / no
 - X11Forwarding yes / no
 - X11UseLocalhost yes / no

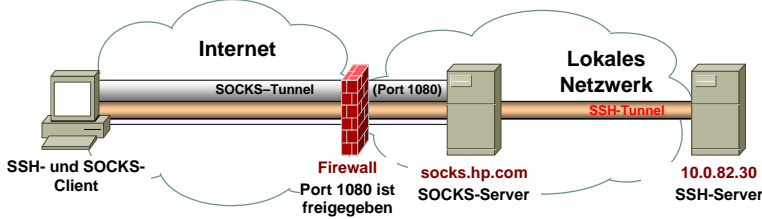
Bei "no" kann man nur vom SSH-Server bzw. Client Verbindungen zu dem Forwarding Port aufbauen.

March 31, 2005 Andreas Aurand, HP Network Competence Center 42



SSH über Socks-Tunnel (OpenVMS/Tru64)


- SSH-Verbindung wird über SOCKS-Tunnel weitergeleitet
 - Kein Eintrag für SSH-Port auf der Firewall notwendig



- Auf SOCKS-Server wird konfiguriert, welche Clients welche Netzwerke ansprechen dürfen
- Auf SSH-Client wird für den SOCKS-Server ein Logical (OpenVMS) bzw. eine Umgebungsvariable (Tru64) definiert

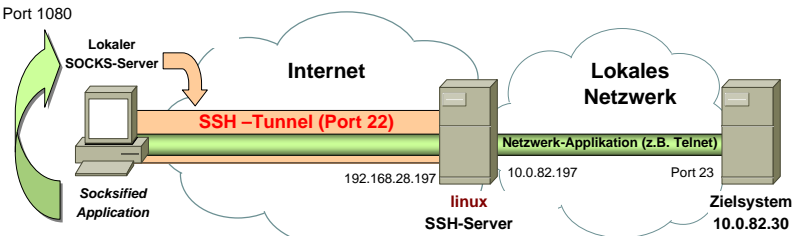
```
$ define SSH_SOCKS_SERVER "socks://andreas@socks.hp.com:1080/10.0.0.0/8"
$ ssh2 -o "UseSocks5 yes" andreas@10.0.82.30
```

March 31, 2005 Andreas Aurand, HP Network Competence Center 43



Dynamic Forwarding (OpenSSH)

- SSH-Client arbeitet als SOCKS-Server
 - Terminiert die Socks-Verbindung lokal, baut dann dynamisch einen TCP-Forward-Tunnel für die eigentliche Applikation auf
 - Leitet den Datenstrom über SSH zum Server weiter. Stellt dann die Verbindung zum eigentlichen Zielsystem her.
 - Server muss keine OpenSSH-Implementation verwenden
- Art von SSH VPN
 - Nur für socksifizierte Applikationen möglich



March 31, 2005 Andreas Aurand, ... 44



Dynamic Forwarding (OpenSSH)

- Konfiguration des lokalen SOCKS-Servers (auf SSH-Client)

```
client > cat /etc/socks.conf
route {
    from: 0.0.0.0/0  to: 10.0.82.0/24  via: 127.0.0.1  port = 1080
    proxyprotocol: socks_v5
    method: none #username
}
```

- Aufbau einer Verbindung über den lokalen SOCKS-Server

```
client > ssh -v -v -v -N -f -D 1080 linux
client > socksify telnet 10.0.82.30
Trying 10.0.82.30...
... ..
debug2: channel 2: socks5 post auth
debug2: channel 2: dynamic request: socks5 host 10.0.82.30 port 23 command 1
debug2: channel 2: open confirm rwindow 131072 rmax 32768
Connected to 10.0.82.30 (10.0.82.30).
Escape character is '^'.
```

March 31, 2005

Andreas Aurand, HP Network Competence Center

45




SFTP Subsystem

- Tru64 und OpenVMS: **Subsystem-<subsystem name>**
 - The argument is a command that will be executed when the subsystem is requested. The sftp command uses a subsystem of the sshd2 daemon to transfer files securely.
 - subsystem-sftp sftp-server2
 - subsystem-sftp SYS\$SYSTEM:TCPIP\$SSH_SFTP-SERVER2.EXE
- OpenSSH: **Subsystem**
 - Configures an external subsystem. Arguments should be a subsystem name and a command to execute upon subsystem request..
 - Subsystem sftp /usr/local/libexec/sftp-server

March 31, 2005

Andreas Aurand, HP Network Competence Center

46




SFTP und SCP

- **SFTP:** entspricht dem normalen FTP-Kommando


```
tru64> sftp andreas@linux
Passphrase for key "/usr/local/users/andreas/.ssh2/id_dsa_2048_a" ...
sftp> ls
.
.qt
.kde
.ssh
.xim
...
```
- **SCP:** entspricht dem normalen RCP-Kommando


```
tru64> scp2 andreas@linux:traceroute.txt xyz.txt
Passphrase for key "/usr/local/users/andreas/.ssh2/id_dsa_2048_a" ...:
traceroute.txt          | 87kB | 86.8 kB/s | TOC: 00:00:01 | 100%
```

March 31, 2005 Andreas Aurand, HP Network Competence Center 47



Links

- OpenSSH
 - <http://www.openssh.org/>
 - OpenSSH-Server unter Windows
 - <http://sshwndows.sourceforge.net>
 - UNIX-Emulator unter Windows
 - Einsatz von UNIX-Tools unter Windows (z.B. openssh)
 - <http://www.cygwin.com/>
- OpenVMS
 - <http://h71000.www7.hp.com/openvms/security.html#ssh>
- Tru64
 - <http://h30097.www3.hp.com/unix/ssh/>

March 31, 2005 Andreas Aurand, HP Network Competence Center 48

Fragen

