

comp.security.ssh: The authenticity of host 'intranet (x.x.x.x)' can't be established."

## The authenticity of host 'intranet (x.x.x.x)' can't be established."

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-04/0258.html>

---

*From:* Gregory ([gdepaix@cassiopee.fr](mailto:gdepaix@cassiopee.fr))

*Date:* 04/24/03

From: "Gregory" <[gdepaix@cassiopee.fr](mailto:gdepaix@cassiopee.fr)>

Date: Thu, 24 Apr 2003 16:06:11 +0200

Hi,

I am a newbie with ssh, but I tried to do exactly what is explained in installation files or support files and I'm still stuck.

I've got 2 Win2k boxes.

192.168.0.6 is a ssh server and 192.168.1.124 is a ssh client.

Every times I'm trying to connect the server, I've got this message :

```
"C:\>ssh grdep@192.168.0.6
```

The authenticity of host 'intranet (192.168.0.6)' can't be established."

Private/Public Keys are manually made for user "grdep" and 192.168.0.6 and 192.168.1.124.

In the homedir of user "grdep" are the files "authorized\_keys2" with information about 192.168.0.6 and 192.168.1.124, and "known\_hosts" with the same information + host names and IP addresses separated by a comma.

I think this is correct, but it still doesn't work.

I don't know what to do else,

So, if you can help me, i will really appreciate.

\*\*\*\*\*

Here the debug output of sshd:

```
F:\Program Files\OpenSSH\usr\sbin>sshd -d -d -d  
debug1: sshd version OpenSSH_3.5p1  
debug3: Not a RSA1 key file /etc/ssh_host_rsa_key.
```

The authenticity of host 'intranet (x.x.x.x)' can't be established."

comp.security.ssh: The authenticity of host 'intranet (x.x.x.x)' can't be established."

```
debug1: read PEM private key done: type RSA
debug1: private host key: #0 type 1 RSA
debug3: Not a RSA1 key file /etc/ssh_host_dsa_key.
debug1: read PEM private key done: type DSA
debug1: private host key: #1 type 2 DSA
debug1: Bind to port 22 on 0.0.0.0.
Server listening on 0.0.0.0 port 22.
debug1: Server will not fork when running in debugging mode.
Connection from 192.168.1.124 port 35095
debug1: Client protocol version 2.0; client software version OpenSSH_3.5p1
debug1: match: OpenSSH_3.5p1 pat OpenSSH*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_3.5p1
debug1: list_hostkey_types: ssh-rsa,ssh-dss
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,r
ijndael-cbc@lysator.liu.se
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,r
ijndael-cbc@lysator.liu.se
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hm
ac-md5-96
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hm
ac-md5-96
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: kex_parse_kexinit:
diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1
debug2: kex_parse_kexinit: ssh-rsa,ssh-dss
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,r
ijndael-cbc@lysator.liu.se
debug2: kex_parse_kexinit:
aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,arcfour,aes192-cbc,aes256-cbc,r
ijndael-cbc@lysator.liu.se
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hm
ac-md5-96
debug2: kex_parse_kexinit:
hmac-md5,hmac-sha1,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hm
```

The authenticity of host 'intranet (x.x.x.x)' can't be established."

comp.security.ssh: The authenticity of host 'intranet (x.x.x.x)' can't be established."

```
ac-md5-96
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit: none,zlib
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit:
debug2: kex_parse_kexinit: first_kex_follows 0
debug2: kex_parse_kexinit: reserved 0
debug2: mac_init: found hmac-md5
debug1: kex: client->server aes128-cbc hmac-md5 none
debug2: mac_init: found hmac-md5
debug1: kex: server->client aes128-cbc hmac-md5 none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST received
debug1: SSH2_MSG_KEX_DH_GEX_GROUP sent
debug1: dh_gen_key: priv key bits set: 133/256
debug1: bits set: 1607/3191
debug1: expecting SSH2_MSG_KEX_DH_GEX_INIT
debug1: bits set: 1645/3191
debug1: SSH2_MSG_KEX_DH_GEX_REPLY sent
debug1: kex_derive_keys
debug1: newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: waiting for SSH2_MSG_NEWKEYS
```