

# SSH2 Public Key Problems for users other than root

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-02/0278.html>

---

*From:* Muso ([muso@mailandnews.com](mailto:muso@mailandnews.com))

*Date:* 02/22/03

From: [muso@mailandnews.com](mailto:muso@mailandnews.com) (Muso)

Date: 22 Feb 2003 05:17:51 -0800

Hi, I'm using OpenSSH3.1p1 on a RH Linux box and Putty 0.53 on W2K. I'm able to connect to the Linux box as user root with public key authentication.

I'm not able to login via PCA as an other user (No supported authentication methods available). I don't have a /etc/nologin file.

Putty logfile states:

```
Event Log: Writing new session log (SSH packets mode) to file:
putty.log
Event Log: Looking up host "214.171.34.6"
Event Log: Connecting to 214.171.34.6 port 22
Event Log: Server version: SSH-2.0-OpenSSH_3.1p1
Event Log: We believe remote version has SSH2 RSA padding bug
Event Log: We claim version: SSH-2.0-PuTTY-Release-0.53
Event Log: Using SSH protocol version 2
Event Log: Doing Diffie-Hellman group exchange
Event Log: Doing Diffie-Hellman key exchange
Event Log: Host key fingerprint is:
Event Log: ssh-rsa 1024
65:26:56:f5:eb:07:40:b8:89:9f:54:d9:29:ac:41:bb
Outgoing packet type 21 / 0x15 (SSH2_MSG_NEWKEYS)
Incoming packet type 21 / 0x15 (SSH2_MSG_NEWKEYS)
Event Log: Initialised AES-256 client->server encryption
Event Log: Initialised AES-256 server->client encryptionEvent Log:
Reading private key file "...pr-key-robby.PPK"
Event Log: Offered public key
Event Log: Server refused public key
Event Log: No supported authentications offered. Disconnecting
```

Does anyone has an idea where the problem could be? I really don't have any more ideas what to do now :-((.