

---

Subject: HowTO use Core/SSH with PRIV/PUB Keys ?

Posted by [omari](#) on Fri, 26 Jul 2024 15:53:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi,

I want to connect to server that accept only private key authentication.

I can connect using command line :

```
ssh -i ./id_rsa user@ServerIP
```

but with Core/SSH, i have tryed without success.

```
SshSession session;
```

```
String priv = "C:\\Users\\user\\.ssh\\id_rsa";
```

```
String pub = "C:\\Users\\user\\.ssh\\id_rsa.pub";
```

```
session.HostBasedAuth().Keys(priv, pub, "", true ).Connect("ssh://user@ServerIP");
```

```
session.GetErrorDesc() return "Invalid signature for supplied public key, or bad username/public  
key combination"
```

```
session.PublicKeyAuth().Keys(priv, pub, "", true ).Connect("ssh://user@ServerIP");
```

```
session.GetErrorDesc() return "Username/PublicKey combination invalid"
```

---

---

Subject: Re: HowTO use Core/SSH with PRIV/PUB Keys ?

Posted by [Oblivion](#) on Sat, 27 Jul 2024 06:58:54 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi omari,

Quote:Hi,

I want to connect to server that accept only private key authentication.

I can connect using command line :

```
ssh -i ./id_rsa user@ServerIP
```

but with Core/SSH, i have tryed without success.

```
SshSession session;
```

```
String priv = "C:\\Users\\user\\.ssh\\id_rsa";  
String pub = "C:\\Users\\user\\.ssh\\id_rsa.pub";
```

```
session.HostBasedAuth().Keys(priv, pub, "", true ).Connect("ssh://user@ServerIP");
```

session.GetErrorDesc() return "Invalid signature for supplied public key, or bad username/public key combination"

```
session.PublicKeyAuth().Keys(priv, pub, "", true ).Connect("ssh://user@ServerIP");
```

session.GetErrorDesc() return "Username/PublicKey combination invalid"

libssh2 can compute public key from private key, but it wasn't enabled in Upp::SSH package (till now). I have pushed the patches to my fork of the latest upp.

If you could check and confirm that it works, I'll make a pull request and patch the code in Upp main branch.

(All you need to do is pass an empty or null String as public key.)

Best regards,  
Oblivion

---

---

Subject: Re: HowTO use Core/SSH with PRIV/PUB Keys ?

Posted by [omari](#) on Sat, 27 Jul 2024 23:38:28 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi Oblivion.

I have tested your change, but it does not work. it show the same error message.

I think this is a limitation of our libssh2 version 1.10.

support for RSA is enhanced in 1.11 version.

<https://github.com/libssh2/libssh2/releases>

then i wait for libssh2 upgrade to 1.11 version.

for now, i can use LocalProcess and ssh.exe as external process.

Thanks Oblivion.

---

---

Subject: Re: HowTO use Core/SSH with PRIV/PUB Keys ?

Posted by [omari](#) on Mon, 29 Jul 2024 06:22:56 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hi,

i have successfully connected using ed25519 private key.

`ssh-keygen -t ed25519 -f mykey_ed25519`

this confirm that the problem concern only RSA.

after further search i found that:

- libssh2 <= 1.10 use RSA\_SHA1 as signing algorithm.
- RSA\_SHA1 is unsecure and depracted then default to rejected by ssh servers.
- this is fixed in 1.11 version (i hope):

Adds RSA-SHA2 key upgrading to OpenSSL, WinCNG, mbedTLS, OS400 backends

---

---

Subject: Re: HowTO use Core/SSH with PRIV/PUB Keys ?

Posted by [Oblivion](#) on Mon, 29 Jul 2024 09:52:39 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

Hello Omari

Quote:after further search i found that:

- libssh2 <= 1.10 use RSA\_SHA1 as signing algorithm.
- RSA\_SHA1 is unsecure and depracted then default to rejected by ssh servers.
- this is fixed in 1.11 version (i hope):

Nice to know that it worked for you!

FYI, libssh2 1.11.0 introduced some bugs (a few of them are serious) and regressions (They did a massive cleanup and they are still cleaning up the older and unsafe code, so it was somewhat expected.).

I am going to update the underlying libssh2 library in SSH package to v1.11, once the 1.11.1 becomes official (It is around the corner).

Thank you for your patience.

Best regards,  
Oblivion

---