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