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