Subject: Core/SSH: ECDSA (256/384/521) and ED25519 algorithms support.
Posted by Oblivion on Wed, 12 May 2021 23:03:41 GMT
View Forum Message <> Reply to Message

Hi,

With the new development cycle, some improvements will follow (libssh2 team is pushing hard to publish v1.9.1). SSH package is now taking advantage of libssh2 v1.9, and the safer kex and PK signing methods.

Core/SSH: ECDSA 256/384/521 and ED 25519 based host keys are now recognized.
Core/SSH: Docs are updated to reflect the available elliptic curve KEX and PK methods.

Changes can be found in the Core/SSH of upp nightly builds or SVN/GIT.

IF you have any questions, suggestions, bug reports, etc. regarding the Core/SSH package, let me know.

Best regards,
Oblivion

Subject: Re: Core/SSH: ECDSA (256/384/521) and ED25519 algorithms support.
Posted by Didier on Tue, 18 May 2021 07:15:39 GMT
View Forum Message <> Reply to Message

Good job,

Keeping up with security protocols is a good thing !