###### SSH Public Key Authentication

***Objective:***

Authenticate to the device with a public key instead of a password.

***Procedure:***

* Generate the public private key pair on the client (note that this will depend on the client in use. Example below is a Linux client):

*ssh-keygen -t rsa -b 2048 -N "" -f key\_pair*

* Install the Public key on the device:

ssh-user-pubkey-install user diag url <http://1.1.1.1/pub.key>

* Configure SSH server (example below):

system ssh-server config encryption-algorithm aes256-cbc system ssh-server config mac-algorithm hmac-sha2-256

system ssh-server config kex-algorithm diffie-hellman-group14-sha256 system ssh-server config pka-algorithm ssh-rsa

* Enable public key authentication:

system ssh-server config public-key-authentication enabled

* Verify public key is installed and associated with correct user:

CN5166-0004-R203> show system ssh-server user-pubkey user-name diag

+ SSH USER PUBLIC KEYS +

| Name | Value |

+ + +

| User | diag |

| Fingerprint(MD5) | 56:15:0a:04:15:0c:09:b8:60:f5:1f:c4:f2:44:09:72 |

| Fingerprint(SHA-1) | cJYRbUOM0C3MmF3FhMbVRhgn2AU |

+ + +

* Verify Encryption algorithm is correct :

CN5166-0004-R203> show system ssh-server config

+ SSH SERVER CONFIG +

| Name | Value |

+ + +

| Encryption Algorithm | aes256-cbc |

| Kex Algorithm | diffie-hellman-group14-sha256 |

| MAC Algorithm | hmac-sha2-256 |

| Public Key Algorithm | ssh-rsa |

| Public Key Authentication | enabled |

| Rekey Limit | 500M |

| Rekey Time | None |

+ + +

* Authenticate to the device with client and key

Test Case Results:

Passed: Yes No Verified by Date/Time Comments