Securing SSH with FIDO2 Security Key

Version 1.1

06/2023

Table of contents

1. Local system configuration

1. Systems must use OpenSSH version 8.3 or higher to configure and operate the SSH with FIDO2 Security Keys. To check the running version, enter

   `ssh -V`
2. The FIDO2 Security Keys must have a PIN set. To set a PIN for the FIDO2 Security Keys, follow ***these***[linkki ohjeisiin] instructions.

1. Open the Terminal and insert FIDO2 Security Key into the system.

2. Enter the following command to generate a key.

   `ssh-keygen -t ecdsa-sk -O resident -O application=ssh:`*`YourTextHere`* `-O verify-required`
   - *YourTextHere* can be replaced by anything that helps you identify where this key is being used, such as a server name.

3. Enter the PIN, touch the key, and press enter to save the keys with default file names. Passphrases are not needed since this configuration requires verification of the key.

4. The private keys are stored to `~/.ssh`. There are found two keys, the reference to the private key and the public key.

5. Add the public key to the remote system with the following command:

   `ssh-copy-id -i ~/.ssh/id_ecdsa_sk.pub user@host`

6. Logon to the remote server using `ssh user@host`. Now the login requires the configured Security Key

2. Remote system configuration

1. Configure /etc/ssh/sshd_config
    - change or add the following lines to the configuration file:

```
PubkeyAuthentication yes
PasswordAuthentication no
PubkeyAuthOptions verify-required
```

2. Check `/etc/ssh/sshd_config.d`
    - if there is a configuration file present f. e. *`50-cloud-init.conf`*, modify the contents to correspond to the above settings.

3. Restart the SSH functions of the remote system by:

    ```
    sudo systemctl restart sshd
    ```

    or

    ```
    sudo service ssh restart
    ```

4. The remote system should now allow login only with the FIDO2 Security Key

3. Using a previously configured Security Key in a new local system

1. Insert the previously configured Security Key into a local system and navigate to `~/.ssh`

2. Download the keypair from the Security Key to the `~/.ssh` folder using
   `ssh-keygen -K`

3. After downloading the keypair `~/.ssh` contains keys `id_ecdsa_sk_rk_YourText` and `id_ecdsa_sk_rk_YourText.pub`

4. Log into the remote server using the downloaded key from the Security Key
   `ssh -i ~/.ssh/ id_ecdsa_sk_rk_YourText user@host`

   - It is possible to change the name of the private key from `id_ecdsa_sk_rk_YourText` to `id_ecdsa_sk` to use a command `ssh user@host` for login

4. Configuring additional Security Keys

(f. e., backup key)

1. Insert a new Security Key into a local system and follow the first steps from a *Local system configuration.*

2. When asked for file names for the new keypair, enter a name of your choice – otherwise if the system already has keypairs saved with default names, the existing keypair will be overwritten by the new keypair.

3. Copy the contents from the newly created public key file `~/.ssh/YourKey.pub` from the local system to the file `~/.ssh/authorized_keys` of the remote system.

4. Restart SSH of the remote system and log into the remote server with your added keys using

```
ssh -i ~/.ssh/YourKey user@host
```

Contact Us

We value your feedback and are here to assist you.
If you have any questions, comments, or suggestions related to this document or our services, please feel free to contact us through:

Email: info@spear.fi

Phone: +358 40 5544 380

Website: https://spear.fi/

Mailing Address: Eteläpuisto 17 D, 28100 Pori.

We strive to respond to all inquiries.

Thank you for your interest and support!