Application Note

How to use SSH with Idem Key

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, contact support@GoTrustID.com.

Date Aug-31-2022

1. Introduction

FIDO is already natively supported by many operating systems, such as Windows, macOS, Linux, iOS, and Android. SSH (Secure Shell) which is designed in Unix-like system such as Linux also supports using FIDO security key to protect the communication. This document describes the steps to install and configure of SSH in Ubuntu. These steps should also apply to other Linux distributions.

2. Configure OpenSSH Client and Idem Key

1.1 Prerequisite

Prepare Idem Key

To use OpenSSH with Idem Key, the **FIDO2 PIN MUST be set**. In Windows, you can use management console in “Windows Settings” -> “Accounts” -> “Sign-in Options” -> “Security Key”. Please refer to the video: https://www.youtube.com/watch?v=Skx8s5C95c0. In other systems such as macOS or Linux, you can use Chrome setting by visiting the URL “chrome://settings/securityKeys”

OpenSSH Version in Linux

OpenSSH version **must be later than 8.4**. Althouth OpenSSH 8.2 already support FIDO2 secuirty, Idem Key cannot be used in this version due to a known bug in OpenSSH 8.2. You can refer the issue report for more details: https://github.com/google/OpenSK/issues/90

Here is the list of Linux OS distribution with compatible OpenSSH version. Any OS version later than this list shall be able to use Idem Key.

Linux OS Version	OpenSSH Version	Build Date
Ubuntu 21.10	8.4	24-Aug-21
CentOS Stream 9	8.7	14-Dec-21
RedHat Enterprise 9	8.7	14-Dec-21
Fedora 35	8.7	24-Aug-21
Fedora 36	8.8	15-Mar-22
Debian 11.4	8.4	15-Mar-22

OpenSSH client in macOS

macOS may pre-load old version of OpenSSH. You can update OpenSSH to latest build by following commands

```
# Install libfido2
brew install libfido2

# Install OpenSSH
brew install openssh

# Check ssh version.
# Example result: OpenSSH_9.0p1, OpenSSL 1.1.1q 5 Jul 2022
ssh -V
```

OpenSSH client in Windows

PuTTY CAC is a branch version of PuTTY. Comparing with the standard version of PuTTY, it adds Windows Certificate API (CAPI), Public Key Cryptography Standards (PKCS) library, and FIDO security key functions to.

You can download the latest version of PuTTY CAC from GitHub.
https://github.com/NoMoreFood/putty-cac

1.2 Generate Key Pair with Idem Key

Please note that Current version of Idem Key only supports key type "**ecdsa-sha2-nistp256**" which can be generated by the parameter "ecdsa-sk" of ssh command.

Configuration in Linux and macOS

1. Plug Idem Key to computer and open a Terminal with entering the command

   ```
   ssh-keygen -t ecdsa-sk
   ```

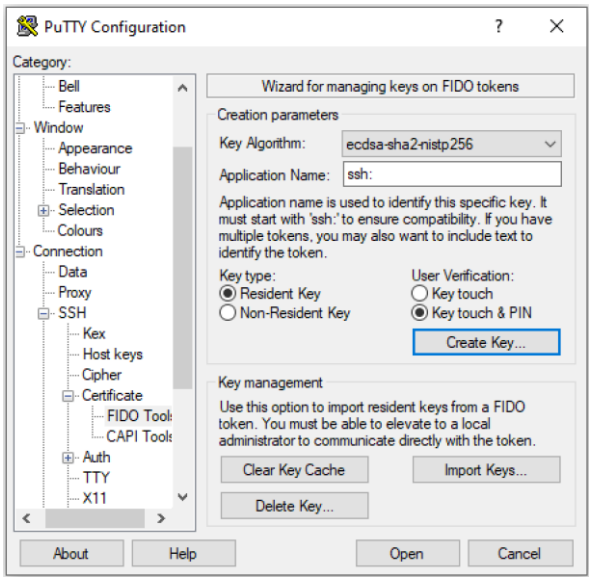
2. SSH will request to enter the PIN and touch the device. Idem Key will flash when this occurs.

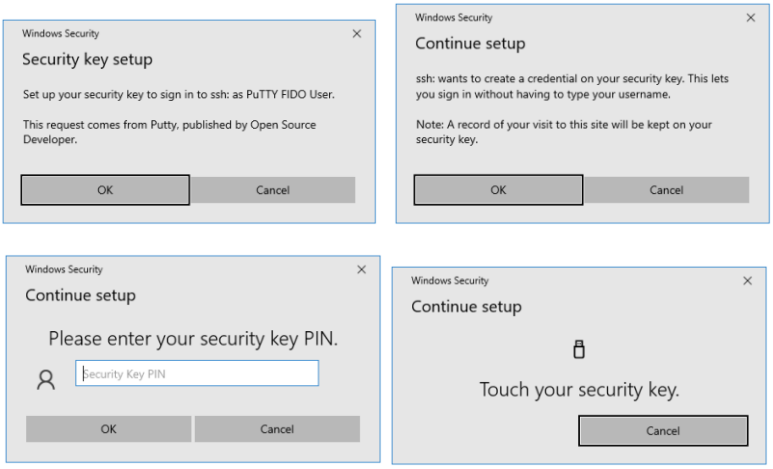
3. SSH will create 2 files “id_ecdsa_sk” and “id_ecdsa_sk.pub”. “id_ecdsa_sk” contains the private key which is stored inside Idem Key and “id_ecdsa_sk.pub” contains the public key which is required to added to the remote SSH server.
4. Copy the public key file “id_ecdsa_sk.pub” to the remote SSH server under folder “~/.ssh/” and execute the command

```
cat id_ecdsa_sk.pub >> authorized_keys
```

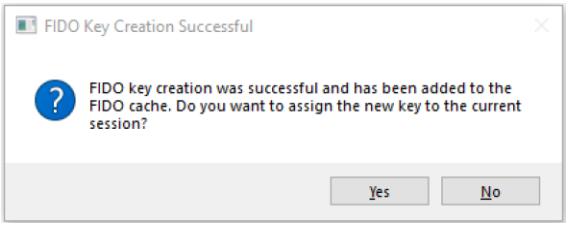
Configuration by Putty CAC in Windows

1. Download and install Putty CAC: https://github.com/NoMoreFood/putty-cac
2. Open Putty and go to settings: “Connection” -> “SSH” -> “Certificate” -> “FIDO Tools”
3. Choose Key Algorithm “**ecdsa-sha2-nistp256** “ and leave application name as default “ssh:”.
4. Choose Key type either “Resident Key” or “Non-Resident Key”
5. Choose User Verification “Key Touch”. (Windows shall ask you to enter PIN anyway).
6. Click “Create Key” and there will be several pop-up windows to ask you to insert Idem Key, enter PIN, and touch it.

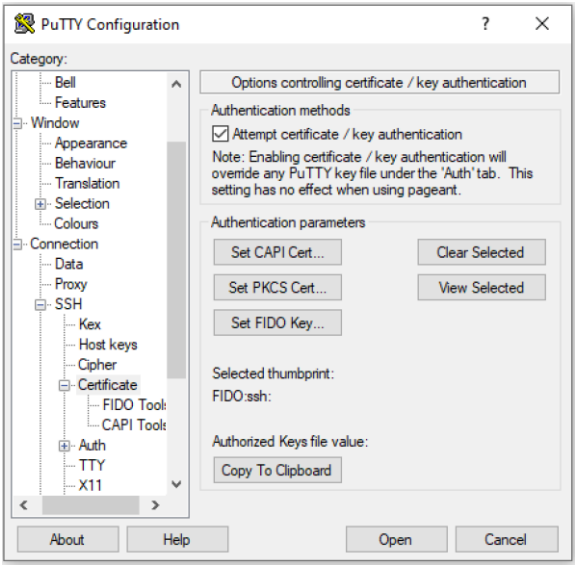




7. After FIDO key pair is generated, Putty will ask if you want to assign the new key to current session. Click “Yes”.



8. Go to setting page “Certificate” and click “Copy To Clipboard.



9. You will have public key content in clipboard like this

```
sk-ecdsa-sha2-nistp256@openssh.com AAAAInNrLWVjZHNhLXNoYTItb
```

10. Copy the public key content to file “~/.ssh/authorized_keys” in the remote SSH server

11. Open the session to connect to the remote SSH server. Putty will ask you to enter username and use (insert and touch) Idem Key to login.