# NITROKEY - PIV

# Nitrokey - PIV

nitrokey PIV

## Authentication with a Nitrokey / PIV

In this How-To we will configure a user in WebADM for using a PIV key. We need a WebADM server already configured.

### 1. Import the Inventory

We need to create an inventory file like this:

```
"Type","Reference","Description","DN","Data","Status"
"PIV Device","<ID1>","PIV Nitrokey","","PublicKey=<pub_key1>","Valid"
"PIV Device","<ID2>","PIV Nitrokey","","PublicKey=<pub_key2>","Valid"
"PIV Device","<ID3>","PIV Nitrokey","","PublicKey=<pub_key3>","Valid"
```

For my test, I have a Nitrokey Start with a PIV certificate and I use `gpg2 --card-edit` for the management of the Nitrokey. Please follow this documentation Nitrokey - Installation.

We need to extract the public key. I do it with `pkcs15-tool`:

```
-bash-4.2# pkcs15-tool --read-public-key 03
Using reader with a card: Nitrokey Nitrokey Start
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwiBZ8g4yHliKPSr/Kg4E
cAJLHch+Kh6w6emzn9ZRxSfrBofSO45x17oi7UsG8OIrBRMIVTgXOzqMbTwnnPjk
pep9dKe4FHEMaPEvNYhAwHDMGVhbYBcf7Ru3CsCM9NPqmbjeV/+zGsMxq8XbZLKP
doW4EjtneTpqD8ummip1ZBTuaFXGi3D/SDxAWTy3DlA+QtU5E2HpU7tZghi5ygiy
9przQct/pMCNX8WJgkLC58g/UtnVeClkh2GGalFrODR2hY0lhWQYhzNH5FzIBmEE
NcPucSwB7/r0abV9hdW52qWXECGBIjKAXrA16n/4QsFJNlPJaysl5Pv4ZBqM86jo
gwIDAQAB
-----END PUBLIC KEY-----
```

We can create a file called `nitrokey.csv` with the serial number as ID and the right public key:

```
"Type","Reference","Description","DN","Data","Status"
"PIV Device","67090940","PIV
NitroKey","","PublicKey=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwiBZ8g4yHliKPSr/Kg4Ec
```

We import the file. Under the the `Import` tab, we click on `Import Inventory File`:

We choose the `nitrokey.csv` file and click on `Import`:

Now, the PIV key is present in the inventory:

## 2. Assign the Nitrokey

We select the user in the LDAP tree on the left and add a `UNIX Account` extension:

We click on `Proceed`:

We `Extend Object`:

We click on `SSH Publick Key Server`:

We click on `Register / Unregister SSH Key`:

We select `Register a hardware key (Inventoried)`, enter the `Serial Number` (Reference) and `Register`:

Now, the PIV key is well registered.

## 3. Test with SSH

We'll try with a CentOS 7 as an ssh server.

We install and configure `spankey_client` on it:

```
[root@centos7-client ~]# yum install
https://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.noarch.rpm
[root@centos7-client ~]# yum clean all
[root@centos7-client ~]# yum install spankey_client -y
[root@centos7-client ~]# /opt/spankey/bin/setup
Enter one of your running WebADM node IP or hostname []: 192.168.3.236
Do you want to enable SpanKey Client for OpenSSH server (y/n)? [N]: y
Do you want to enable SpanKey Client NSS plugin (y/n)? [Y]:
Do you want to register SpanKey Client logrotate script (y/n)? [Y]:
Do you want SpanKey Client to be automatically started at boot (y/n)? [Y]:

    Primary OpenOTP service URL is: 'https://192.168.3.236:8443/spankey/'
    Secondary OpenOTP service URL is: 'NONE'
    Enable SpanKey Client for OpenSSH server: 'YES'
    Enable SpanKey Client NSS plugin: 'YES'
    Register SpanKey Client logrotate script: 'YES'
    SpanKey Client must be automatically started at boot: 'YES'

Do you confirm (y/n)?: y

Applying SpanKey Client settings from default configuration files... Ok
Retrieving WebADM CA certificate from host '192.168.3.236'... Ok
The setup needs now to request a signed 'SpanKey' client certificate.
This request should show up as pending in your WebADM interface and an administrator
must accept it.
Waiting for approbation... Ok
Updating entry 'client_id' in file '/opt/spankey/conf/spankey.conf'... Ok
Updating file '/etc/ssh/sshd_config'... Ok
Updating file '/etc/nsswitch.conf'... Ok
Updating file '/etc/pam.d/password-auth'... Ok
Registering SpanKey Client service...
Registering SpanKey Client service... Ok
Adding logrotate script... Ok

SpanKey Client has successfully been setup.

IMPORTANT: Do not forget to perform the following actions before you exit this session:
 - Start SpanKey (/opt/spankey/bin/spankey start)
 - Restart 'sshd'
 - Restart 'nscd'

[root@centos7-client ~]#
```

For the ssh client, we use a mac mini. We configure it for using the smartcard:

```
[LO@Mac-mini ~]$ brew install opensc
```

We try the authentication:

```
[LO@Mac-mini ~]$ ssh -I opensc-pkcs11.so test-user@192.168.3.120
Enter PIN for 'User PIN (OpenPGP card)':


Session recording is disabled.
Audit logs recording is disabled.
Session lock is disabled.
Session's max duration is unlimited.

[test-user@centos7-client ~]$ pwd
/home/test-user
[test-user@centos7-client ~]$ exit
exit

>>>> Session's duration was aprox 42 seconds <<<<

Connection to 192.168.3.120 closed.
```

I’m connected to the server with a user from the LDAP database and authenticated with my PIV key.