



Identify - Authenticate - Anywhere

Fido2 Device Registration and Use with Virtual Smartcard

Document Control

Status	Version	Date	Owner	Description
Complete	1.0	15/05/2019	Josh Stannard	Completed guide

Contents

1. Introduction	4
2. Overview	4
3. Registration	4
4. Authentication	7

1. Introduction

This document seeks to guide the user through the process of registering a Fido2 device to use as a second factor in their Virtual Smartcard authentication. This guide will cover the registration process followed as well as the authentication process using a Fido2 device.

2. Overview

There are prerequisites for this guide. They are as follows:

- iO Identity Agent
- Virtual Smartcard enrolled
- Registration Authority role on smartcard
- A PC

The RA (Registration Authority) will need to go through this process with a user.

3. Registration

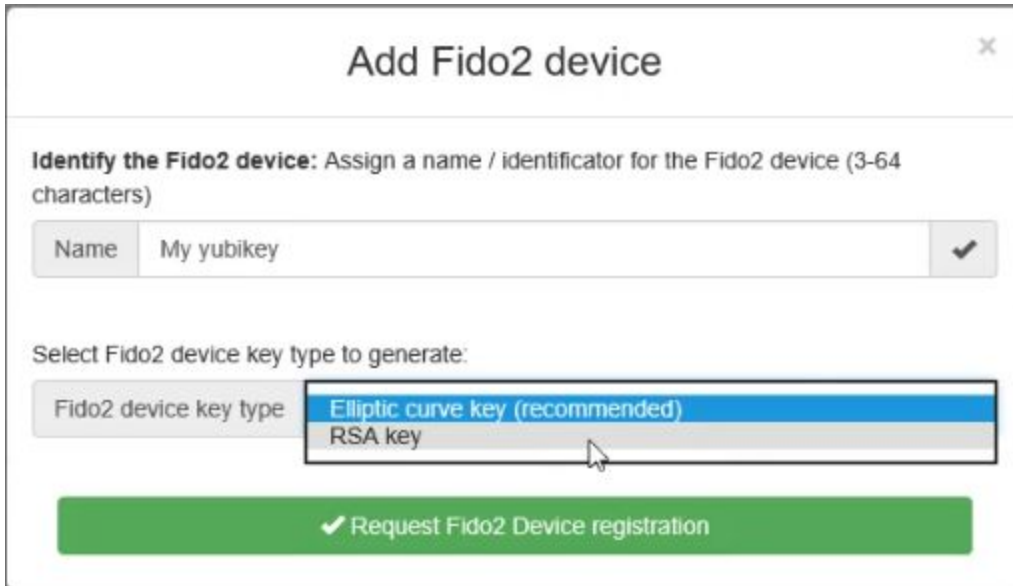
In order to register a Fido2 device the RA will need to open the VSC Management page.

From the management page select the user who you wish to add a Fido2 device for. Once on the users page select **Add Fido2 Device**.

This will bring up the Fido2 device registration box. Give the device a name and select the type of key encryption you would like to use.


A Fido2 device can hold up to a maximum of 25 keys and only 2 may be RSA keys. Authentication is also faster with an elliptical key.

- RSA encryption creates a large key size and a single Fido2 device will only be able to hold 2 RSA keys
- Elliptical curve is a smaller key size and a single Fido2 device can hold multiple keys



The screenshot shows a web form titled "Add Fido2 device" with a close button (X) in the top right corner. Below the title, there is a section "Identify the Fido2 device: Assign a name / identifier for the Fido2 device (3-64 characters)". This section contains a text input field with the name "My yubikey" and a checkmark icon on the right. Below this, there is a label "Select Fido2 device key type to generate:" followed by a dropdown menu. The dropdown menu is open, showing two options: "Elliptic curve key (recommended)" which is highlighted in blue, and "RSA key". At the bottom of the form is a large green button with a white checkmark and the text "Request Fido2 Device registration".

Once the device has been given a name and the encryption type set select **Request Fido2 Device registration**.

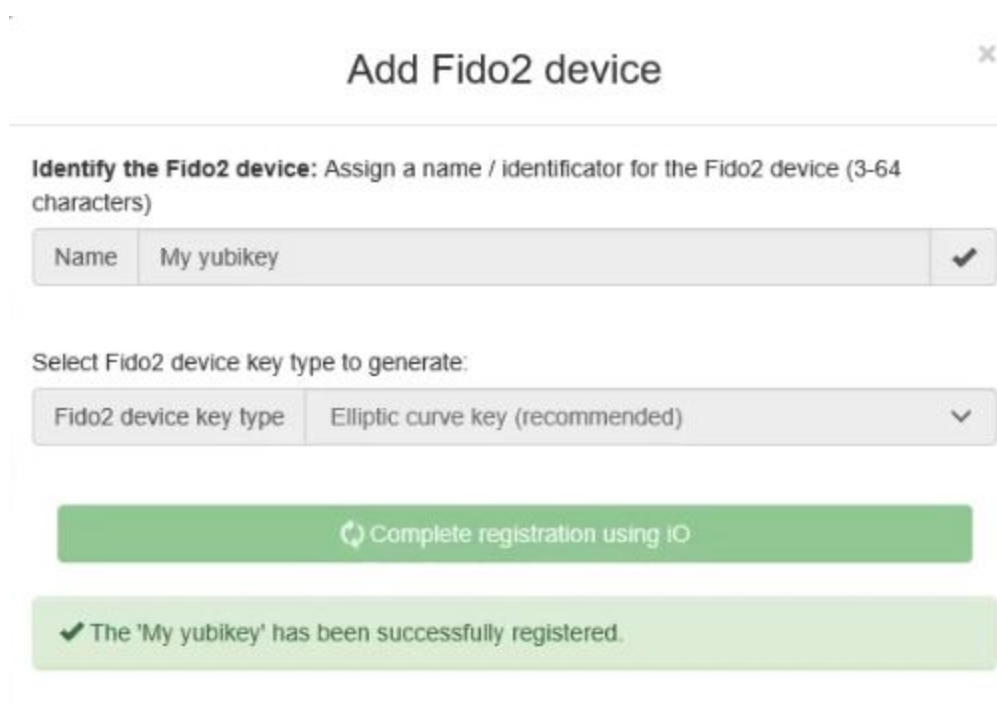


This screenshot is identical to the one above, showing the "Add Fido2 device" form. In this version, the green "Request Fido2 Device registration" button is highlighted with a mouse cursor pointing at it.

The Yubikey device will prompt the user to present their Yubikey device and enter the PIN that was set for the device.



Once the device has been presented and the PIN entered (correctly!) then the device will be successfully enrolled for use with Isosec's Virtual Smartcard.



4. Authentication

Using the Yubikey as a second factor for authentication with iO is simple. Once the device has been registered to the users card , as long as iO is configured to require the Yubikey then it will prompt for the device after the Virtual Smartcard passcode has been entered.



Once the passcode has been entered correctly and the device is present in the machine the following prompt will show.



Press your finger on the device on the highlighted area within 5 seconds and you will be authenticated.