# 2FA Setup via a FIDO2 Security Key

## Introduction

FIDO2 security keys offer a safer alternative to the combo credentials/TOTP. With a security key (SK), you will substitute the TOTP authentication step with public key cryptography. If you register your SK with the IL, you basically create a private-public keypair (known as a credential) and store the private key in your SK while sending the public key and a randomly generated credential ID to the IL system for storage. Upon logging in, the IL system uses your public key to prove your identity. For more information see

| |
|---|
| https://webauthn.guide/ |
| https://fidoalliance.org/fido2/ |

| |
|---|
| Because 2FA via a security key offers the strongest protection against cyber criminals, the IL encourages you always to use this method to login to all IL services. |
| If you have obtained a security key from the Lorentz Institute, you must return it upon termination of your appointment at the Institute |

## Preliminary Actions

Make sure your security key is FIDO2-compatible by checking the vendor's website or obtain one from the Lorentz Institute IT Department. If you obtain a security key from the IL, you are **required** to return it upon termination of your contract and you are **obliged** to notify support@lorentz.leidenuniv.nl in case of key loss or theft. If you would like to use your private security key, notify support@lorentz.leidenuniv.nl your intention to register this device so that you can be guided through the procedure.

Once setup/registered, the same security key will be a valid second factor to access all IL 2FA-protected web services, the IL GNU/Linux workstations, and decrypt the disk of the IL rental laptops.

The setup of your security key differs slightly depending on whether you have already 2FA setup under your account, for instance via TOTP, or not. Follow the workflow below that is appropriate to your situation.

## Setup without previous 2FA in place

### Step 1

Notify the intention of registering a private key to support@lorentz.leidenuniv.nl.

Navigate to any of the Lorentz Institute SSO web applications, for instance our Remote Workspace.

You will be redirected automatically to the Lorentz Institute Identity Provider login page as in **Figure 1**.

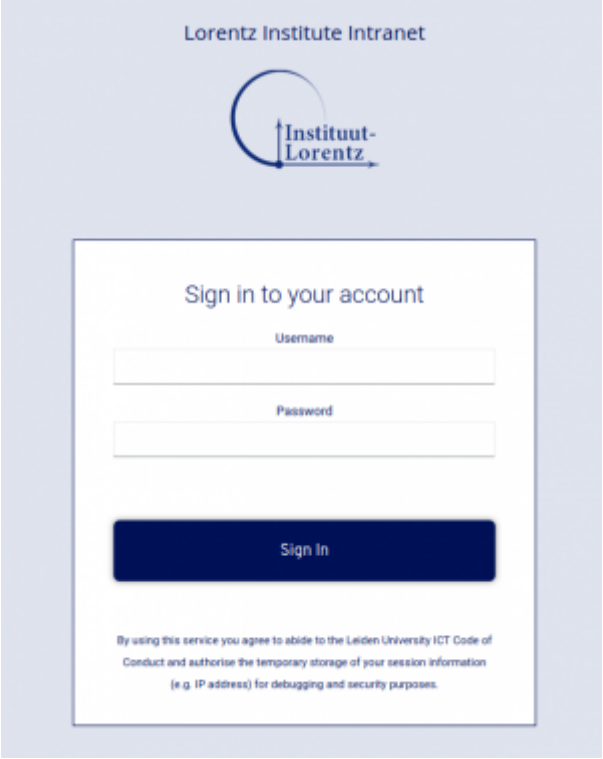

Figure 1: Identity Provider login page

## Step 2

Enter your IL credentials to sign in. Upon successful login, your browser will ask you to register your security key (Figure 2). Plug your security key into an available USB-A port of your PC/laptop and confirm by pressing or touching the key button [1)].

Figure 2: Security Key Registration

## Step 3

Once your security key has been successfully added, your browser will ask you to add a label if you wish (Figure 3). Click on `OK'. Your SK setup is completed.

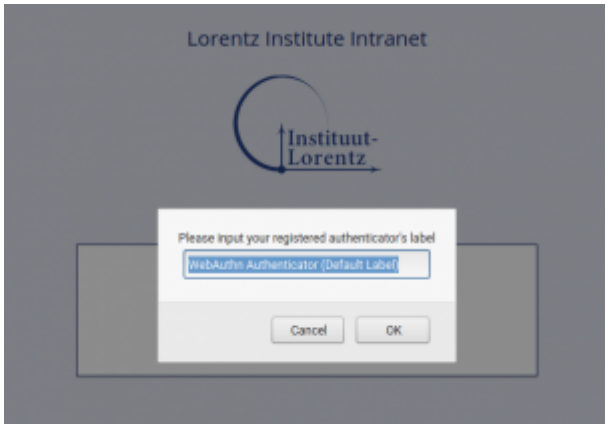

Figure 3: Key registration confirmation and label

## Step 4

If Step 3 succeeds but your private e-mail address has not been validated yet, the system will send you an email to your private (not @lorentz) e-mail address with precise instructions on how to verify your identity. If your identity cannot be validated, you will not be granted access to the system.

Figure 4: Verrify your private email address.

## Step 5

Verify your identity by visiting your private email inbox. You should have received an email from the Lorentz Institute Identity Provider [2]. Open that email and copy (for instance using on most platforms Control-C or right-mouse click copy) the secret code in the body of the message. Visit https://www.lorentz.leidenuniv.nl/idp/ and paste (on most platforms Control-P or right-mouse click paste) the secret code in the white text area. Click on `Submit'. Your identity is now verified.

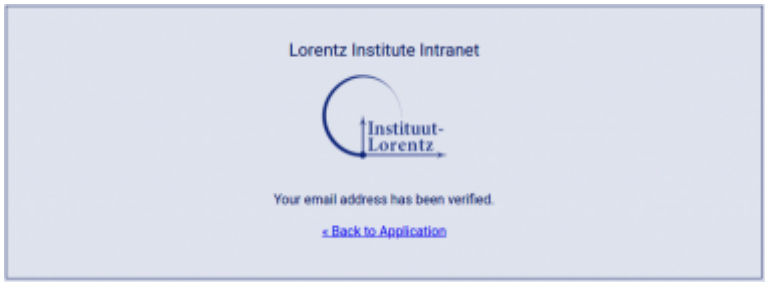

Figure 5: Screenshot of e-mail verification process.

### Step 6

Click on *Back to application* to redirect your browser to the Lorentz Institute SSO web application from which you started the whole process or close the browser. Your setup is complete.

## Setup with previous 2FA in place

### Step 1

Notify the intention of registering a private key to support@lorentz.leidenuniv.nl.

Navigate to any of the Lorentz Institute SSO web applications, for instance our Remote Workspace.

You will be redirected automatically to the Lorentz Institute Identity Provider login page as in **Figure 1**.

Figure 6: Identity Provider login page

### Step 2

Enter your IL credentials and the correct TOTP to sign in. Upon successful login, your browser will ask you to register your security key (Figure 2). Plug your security key into an available USB-A port of your PC/laptop and confirm by pressing or touching the key button [3)].

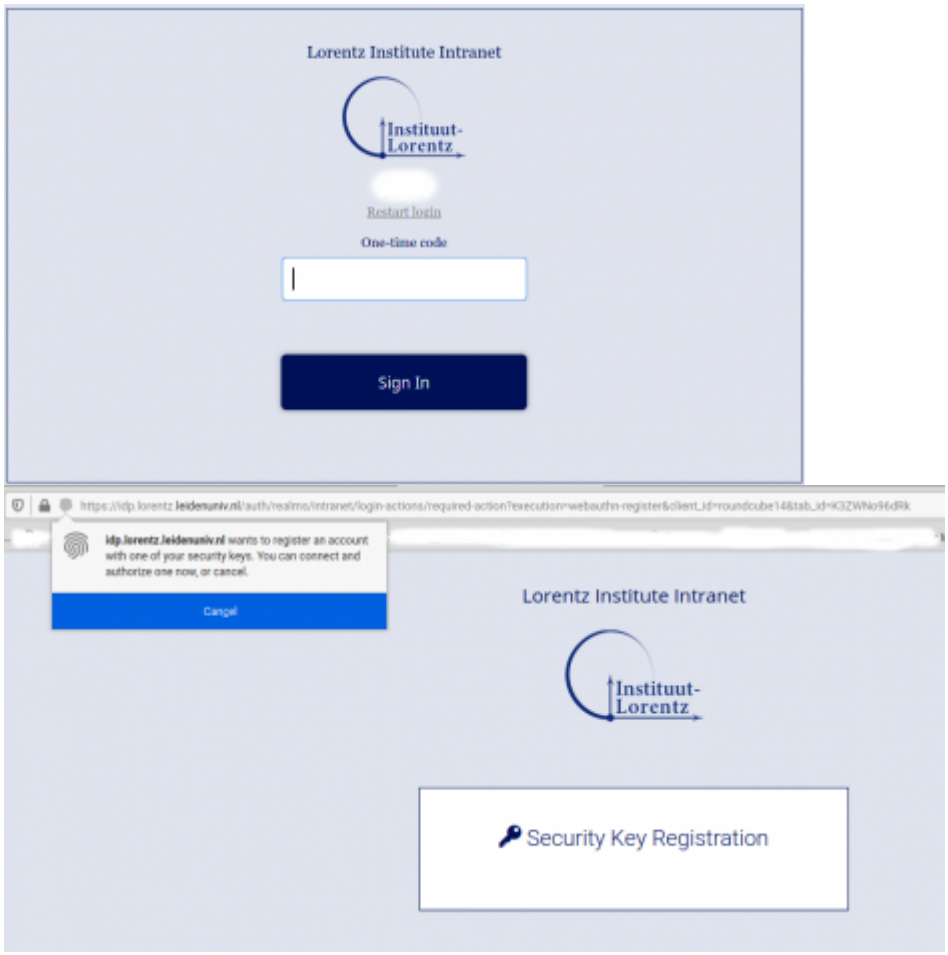


Figure 7: TOTP validation and Security Key Registration

### Step 3

Once your security key has been successfully added, your browser will ask you to add a label if you wish (Figure 3). Click on `OK'. Your SK setup is completed.

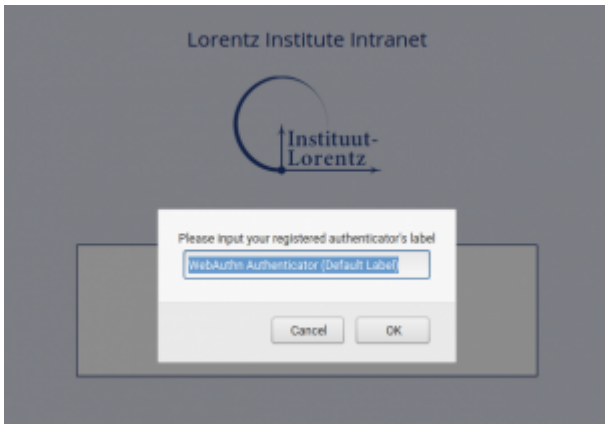


Figure 8: Key registration confirmation and label

## Problems and Solutions

| | |
|---|---|
| I cannot setup 2FA/access the system | Make sure we have your private email address on record |
| I lost my security key | Notify support@lorentz.leidenuniv.nl<br>Change your IL credentials |

| | |
|---|---|
| Someone stole my security key | Notify support@lorentz.leidenuniv.nl<br>Change your IL credentials |
| How do I disable 2FA? | 2FA is mandatory on all SSO web services and to access our SSH server |

[1)] [3)]
,

Key confirmation actions, such as pushing or touching, depend on the key used, please read the manual of your key's vendor

[2)]

Details of this email are not disclosed here to prevent phishing.