First-time 2FA Setup via a Personal Computer

Preliminary Actions

You need to install a *program* on your personal computer which will

- store the **secret key** that the IL authentication system will share with you
- calculate TOTP passcodes using the **secret key** as a seed

We advise Free Softwares such as KeePassXC (multiplatform with GUI) or the OATH Toolkit (GNU/Linux terminal), but you are free to choose any programs that implement the open OTP standards.

Setup

Step 1

Navigate to any of the Lorentz Institute SSO web applications, such Account Services, Remote Workspace, etc.

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

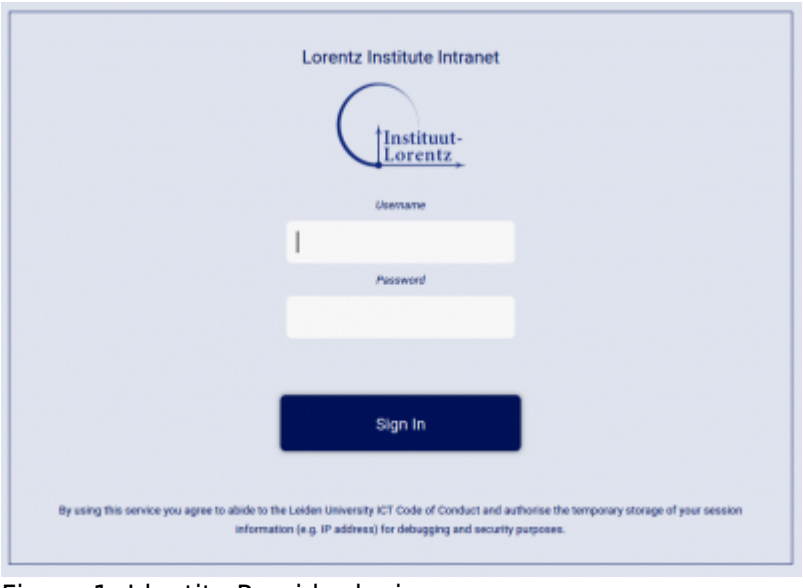

Figure 1: Identity Provider login page

Step 2

Enter your IL credentials to sign in. Upon successful login, you will be redirected to a page containing a QR code. Click on “Unable to Scan?” to display your shared **secret key** and the other parameters to input in your OTP program to set it up (Figure 2).

Note the secret key, the algorithm, the number of digits, and the time interval. You will need them in Step 3.

Figure 2: TOTP Setup Page (QR code and other sensitive information deliberately blurred)

Step 3

Open KeePassXC (installed on all IL workstations), create a new passwords database if you do not want to use an existing one and click on *Entries* → *TOTP* → *Set Up TOTP*. Insert your private key, algorithm, time interval and number of digits from Step 2 and confirm by clicking on `OK'.

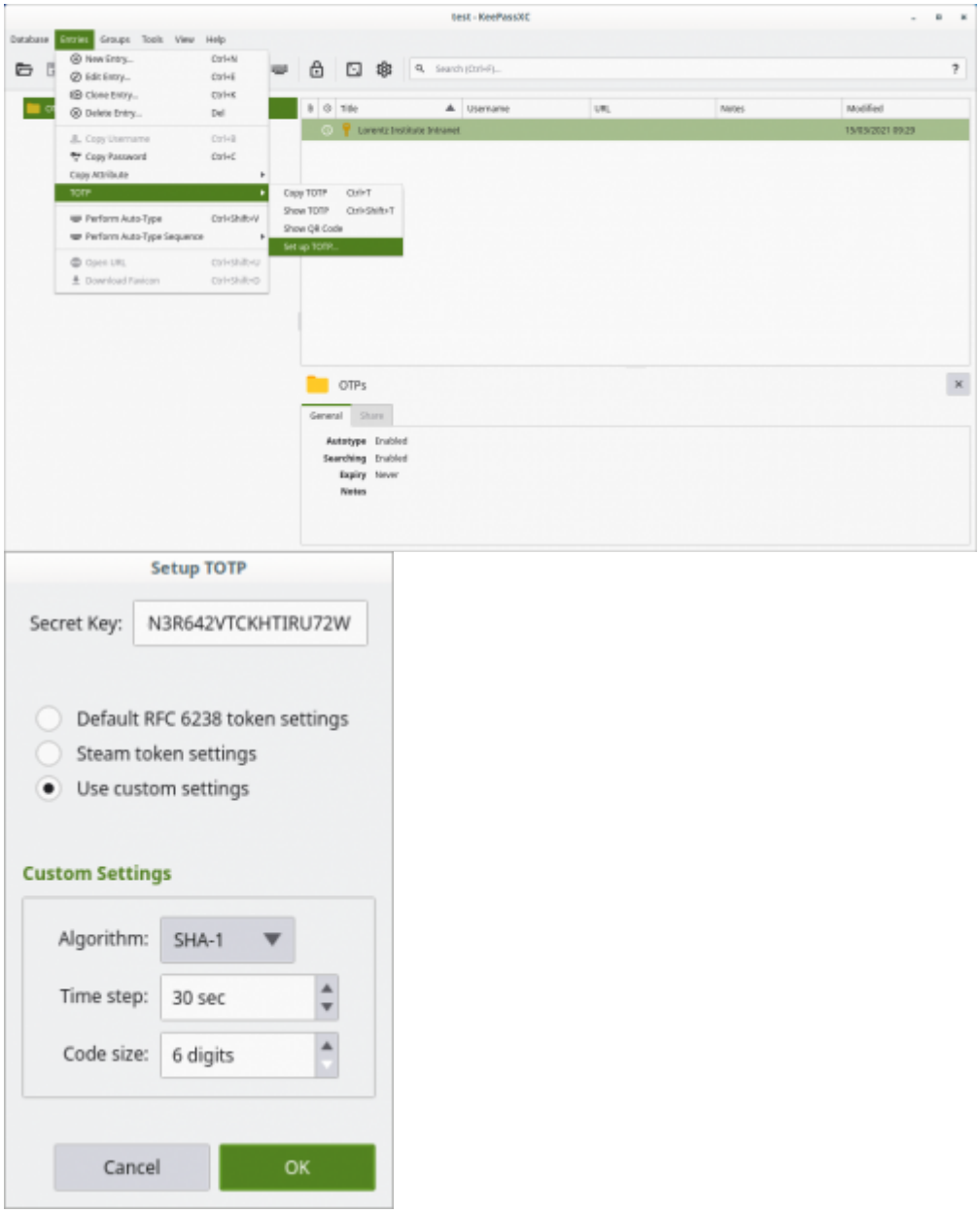

Figure 3: TOTP Setup with KeePassXC. Use the TOTP settings described in Step 2.

Generate a OTP by clicking on *Entries* → *TOTP* → *Show TOTP*. Insert this TOTP in the *One-time code* form input and, if you wish, a label in the form input called *Device Name*. This label is meant to help you keep track with which device the **secret key** has been shared. Click on *Submit*.

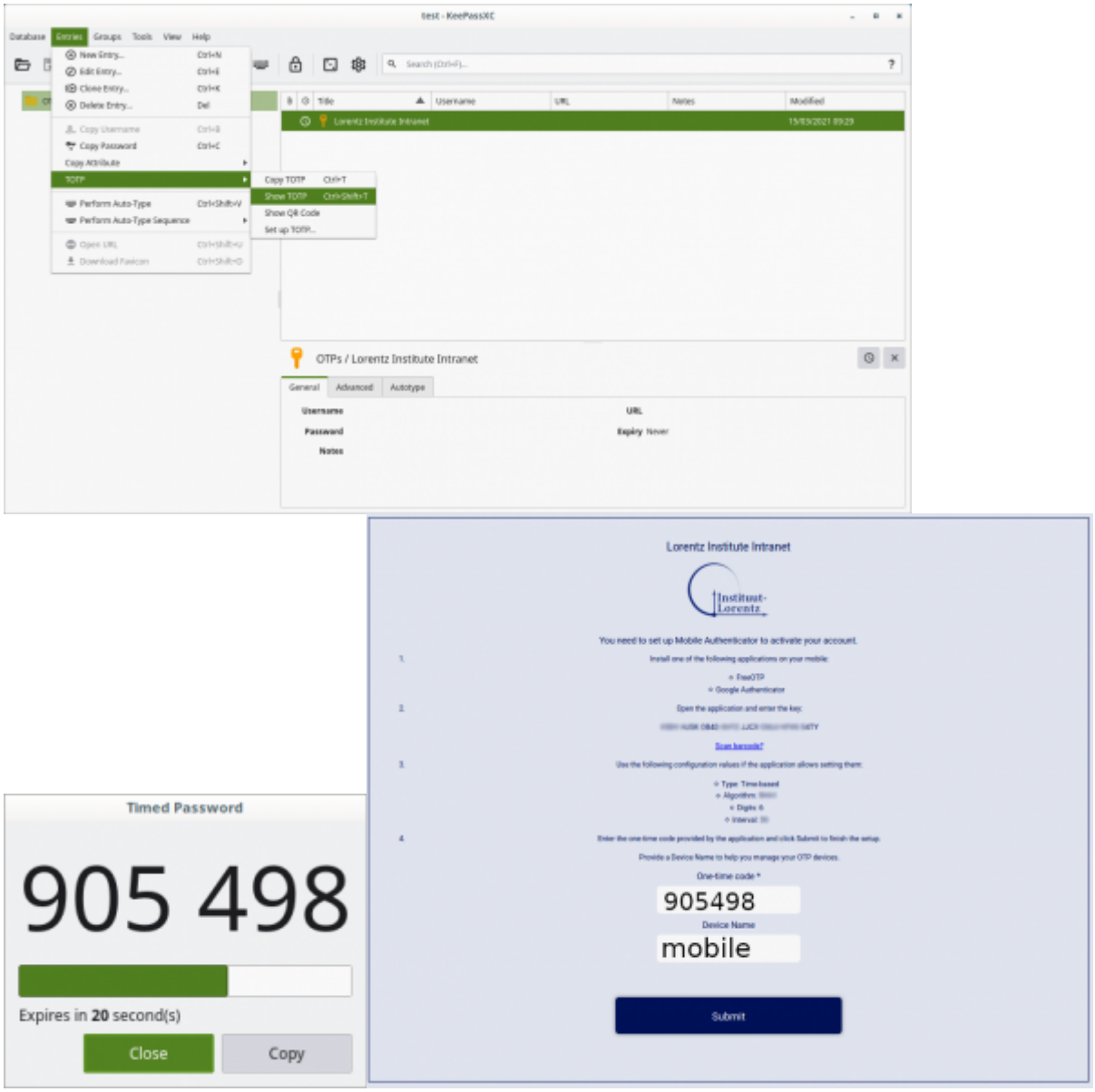

Figure 4: TOTP generation KeePassXC and final 2FA setup on the Lorentz Institute Identity Provider

Step 4

If Step 3 succeeds (errors might occur if there is too much lag time, i.e. the OTP expired), 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 5: Screenshot of e-mail verification process.

Step 5

Verify your identity by visiting your private email inbox. You should have received an email from the Lorentz Institute Identity Provider [1]. 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.

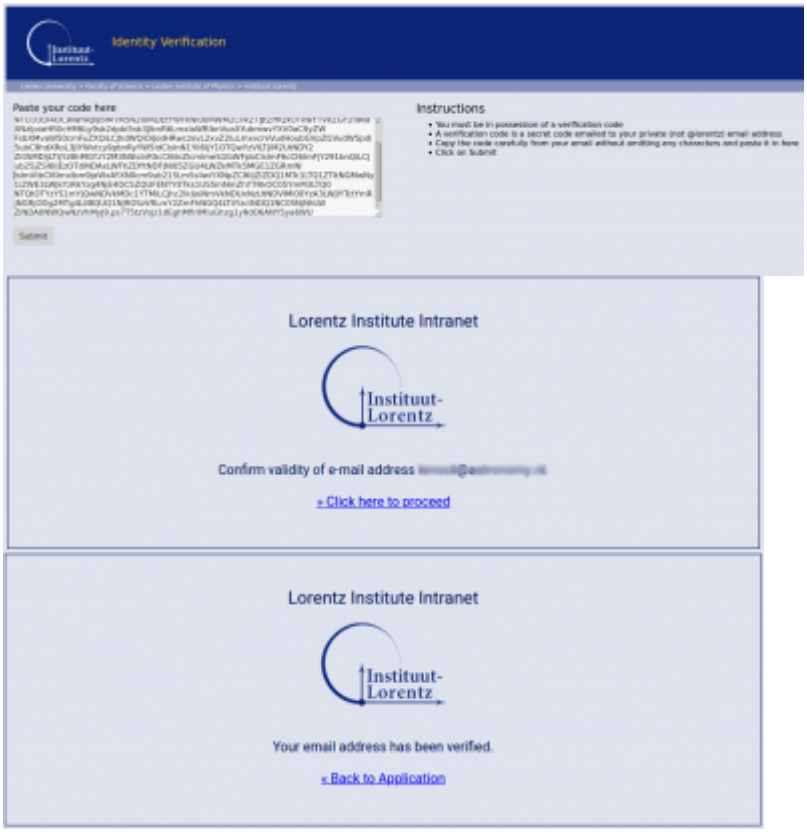

Figure 6: Screenshot of e-mail verification process.

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.

Problems and Solutions

I cannot setup 2FA/access the system	Make sure we have your private email address on record
I lost my smartphone/PC with my OTP secret	Notify support@lorentz.leidenuniv.nl Change your IL credentials
How do I disable 2FA?	2FA is mandatory on all SSO web services and to access our SSH server
My TOTP is incorrect	Make sure your phone's (PC's) clock is synchronised to the SSH server time and you scanned/copied all TOTP settings correctly
My OTP secret is compromised	Notify support@lorentz.leidenuniv.nl Change your IL credentials

1)

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

From:
https://helpdesk.physics.leidenuniv.nl/wiki/ - **Computer Documentation Wiki**

Permanent link:
https://helpdesk.physics.leidenuniv.nl/wiki/doku.php?id=institute_lorentz:2fa-pc&rev=1617289101

Last update: **2021/04/01 14:58**