

USER SELF-SERVICE DESK

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

1. Overview

This Web application is mostly designed for internal (corporate) use and includes several self-management features like:

- › Manage account information such as email, mobile phone numbers, etc.
- › Reset LDAP password according to a configurable password policy
- › Enroll, re-synchronize and test a Software / Hardware Token or Yubikey
- › Manage SSH keys (SpanKey)
- › Manage PDF Signatures
- › Manage own user certificates

The installation of SelfDesk is straightforward and only consists of running the self-installer or installing it from the RCDevs repository and configure the application in WebADM.

You do not have to modify any files in the SelfDesk install directory! The web applications configurations are managed and stored in LDAP by WebADM. To configure SelfDesk, just enter WebADM as super administrator and go to the 'Applications' menu. Click SelfDesk to enter the web-based configuration.

SelfDesk application logs are accessible in the Databases menu in WebADM.

Note

To be able to use SelfDesk, any LDAP user must be a WebADM account. That means usable LDAP accounts are those containing the webadmAccount LDAP object class. You can enable the WebADM features on any LDAP user/group by extending it with the webadmAccount object class (from object extension list).

Inline WebApps: You can embed a Web app on your website in an HTML iFrame or Object.

#Example

```
<object data="https://<webadm_addr>/webapps/selfdesk?inline=1" />
```

2. User Self-Service Desk Installation

The User Self-Service Desk application is included in the *webadm_all_in_one* package.

2.1 Installation with Redhat Repository

On a RedHat, CentOS or Fedora system, you can use our repository, which simplifies updates. Add the repository:

```
yum install https://repos.rcdevs.com/redhat/base/rcdevs_release-1.1.1-1.noarch.rpm
```

Clean yum cache and install Self-Service Desk (SelfDesk):

```
yum clean all  
yum install selfdesk
```

The User Self-Service Desk application is now installed.

2.2 Installation with Debian Repository

On a Debian system, you can use our repository, which simplify updates. Add the repository:

```
wget https://repos.rcdevs.com/debian/base/rcdevs-release_1.1.1-1_all.deb  
apt-get install ./rcdevs-release_1.1.1-1_all.deb
```

Clean cache and install the User Self-Service Desk application (SelfDesk):

```
apt-get update  
apt-get install selfdesk
```

The User Self-Service Desk application is now installed.

2.3 Through the self-installer

Download the Selfdesk package from the RCDevs website, copy it on your WebADM server(s) and run the following commands:

```
[root@webadm1 tmp]# gunzip selfdesk-1.1.8-1.sh.gz
[root@webadm1 tmp]# sh selfdesk-1.1.8-1.sh
Selfdesk v1.1.8-1 Self Installer
Copyright (c) 2010-2018 RCDevs SA, All rights reserved.
Please report software installation issues to bugs@rcdevs.com.
```

```
Verifying package update... Ok
Install selfdesk in '/opt/webadm/webapps/selfdesk' (y/n)? y
Extracting files, please wait... Ok
Removing temporary files... Ok
Selfdesk has been successfully installed.
Restart WebADM services (y/n) y
Stopping WebADM HTTP server... Ok
Stopping WebADM Watchd server..... Ok
Stopping WebADM PKI server... Ok
Stopping WebADM Session server... Ok
Checking libudev dependency... Ok
Checking system architecture... Ok
Checking server configurations... Ok
```

```
Found Trial Enterprise license (RCDEVSSUPPORT)
Licensed by RCDevs SA to RCDevs Support
Licensed product(s): OpenOTP,SpanKey,TiQR
```

```
Starting WebADM Session server... Ok
Starting WebADM PKI server... Ok
Starting WebADM Watchd server... Ok
Starting WebADM HTTP server... Ok
```

```
Checking server connections. Please wait...
Connected LDAP server: YO_AD-DC (192.168.3.50)
Connected SQL server: SQL Server (192.168.3.58)
Connected PKI server: PKI Server (192.168.3.54)
Connected Mail server: SMTP Server (78.141.172.203)
Connected Push server: Push Server (91.134.128.157)
Connected Session server: Session Server 2 (192.168.3.55)
Connected License server: License Server (91.134.128.157)
```

```
Checking LDAP proxy user access... Ok
Checking SQL database access... Ok
Checking PKI service access... Ok
Checking Mail service access... Ok
Checking Push service access... Ok
Checking License service access... Ok
```

```
Cluster mode enabled with 2 nodes (I'm slave)
Session replication status: Active (0.0003 sec)
Please read the INSTALL and README files in /opt/webadm/webapps/selfdesk.
```

Selfdesk is now installed and can be configured under the WebADM Admin GUI.

3. Selfdesk configuration

To configure the PWRreset application, you have to log in on the WebADM Admin GUI > **Databases** Tab > **Self-Service** > **User Self-Service Desk (selfdesk)** > **CONFIGURE**.

The User Self-Service Desk application can be published through the WebADM Publishing Proxy for the end-user access with the setting **Publish on WAProxy**. This setting is only available when WAProxy is configured with WebADM. Have a look at this [documentation to setup WAProxy](#).

To help you end-users to download a Token application on their phone, you can configure the Token Download URLs setting. For example:

```
IOS=https://itunes.apple.com/us/app/openotp-token/id1148075952,  
Android=https://play.google.com/store/apps/details?id=com.rcdevs.auth
```

Misc Settings

☒ **Token Download URL**

IOS=https://itunes.apple.com/us/app/openotp-token/id1148075952,
Android=https://play.google.com/store/apps/details?id=com.rcdevs.auth

The Software Token download page on an external website.
When configured, a download button is included in the OTP section.
Ex. <http://www.rcdevs.com/tokens/?type=software>

It will look like that for the end-user:

User Self-Service Desk

RCDevs
security solutions

You can find your Software Token compatible with your device here:

IOS

Android


Choose a Software Token, according to your mobile device type.
Install the Token Application on your mobile phone via direct download or AppStore URL.

Instructions to install and setup your Software Token:

1. Install the Software Token application on your mobile device.
Installation procedure may differ depending on your mobile device and selected Token.
2. Start the Software Token setup (you may read vendor documentation for installation).
3. Click 'Next' to register your Software Token with OpenOTP.

Next

Ok

 Provided by **RCDevs SA**

The other settings are described under the User Self-Service Desk configuration page.

Object Settings for **cn=SelfDesk,dc=WebApps,dc=WebADM**

Web Application Settings

☒ Disable WebApp

☐ Yes ☒ No (default)

☒ Hide WebApp

☐ Yes ☒ No (default)

Hide application from WebApps portal.

☐ Publish on WAProxy

☐ Yes ☒ No (default)

Make WebApp accessible from WAProxy reverse-proxies.

☒ Default Domain

Default ▾

This domain is automatically selected when no domain is provided.

☐ Group Settings

☒ Yes (default) ☐ No

Resolve application settings on user groups (direct and indirect).
Warning: Impacts performances.

☐ Access Locked

☐ Yes ☒ No (default)

Login is not permitted unless the user is temporarily authorized.
To authorize a user, use the 'Unlock WebApp access' action for the user.
IMPORTANT: Self-service applications published on the Internet should be locked.

☐ Non-locked IP Addresses

Comma-separated list of IP addresses with netmasks for which access is never locked (ex: 192.168.1.0/24).

☐ Allowed IP Addresses

Comma-separated list of IP addresses with netmasks (ex: 192.168.1.0/24).
If not set then any source IP is allowed. The localhost is always allowed.

☐ Custom CSS File

Edit

CSS files and additional custom resources must be stored under /opt/webadm/lib/htdocs/custom/.

☒ Default Language

DE ▾

☐ Show Domain List

☒ Yes (default) ☐ No

WebADM Domains are displayed in a drop-down list on the login page.

☒ Require User Certificate

☐ Yes ☒ No (default)

If enabled, a user certificate must be provided to enter the self-service.

☐ Require Second Factor Always ▾

If enabled, a second factor (OTP or FIDO) is required to enter the self-service.
With 'Enrolled' the authentication falls-back to LDAP-only when no OTP/FIDO method is available.

Allowed Features

☒ Allow User Infos Management ☒ Yes (default) ☐ No

When enabled, users can change their mobile, email and language.

☒ Allow User Password Change ☐ Yes (default) ☒ No

When enabled, users can change their LDAP password.
Password change requires the PwReset WebApp to be installed and enabled.
The password policy settings should be configured in PwReset.

☒ Allow OTP Management ☐ Yes ☒ No (default)

When enabled, users can configure their OTP authentication settings.

☒ Allow SSH Management ☐ Yes ☒ No (default)

When enabled, users can configure their SSH private key settings.

☒ Allow PKI Management ☒ Yes ☐ No (default)

When enabled, users can manage their X.509 certificates.

- ☒ TOKEN
- ☒ SMS
- ☒ MAIL
- ☒ LIST
- ☒ LASTOTP

Choose which items are available for primary and fallback OTP methods.
If not set, any method can be selected.

- ☐ Token1
- ☐ Token2
- ☐ Token3
- ☐ OTPList
- ☐ AppKeys
- ☐ FIDO
- ☐ SSHKey
- ☐ TiQR
- ☐ [None]

☐ Allowed Self-Registration

Choose which items users are enabled for self-registration.
If not set, any items can be self-registered.

OTP Token Management

☒ Allowed Token Types

- ☒ HARDWARE-OATH
- ☒ HARDWARE-YUBIKEY
- ☒ QRCODE-TOTP
- ☒ QRCODE-HOTP
- ☒ MANUAL-YUBIKEY
- ☒ MANUAL-TOTP
- ☒ MANUAL-HOTP
- ☒ MANUAL-OCRA

Selection of OpenOTP Token types users are able to register.
Hardware options are used for inventoried Tokens and YubiKeys.
If not set, any Token type can be self-registered.

☐ Default Token Type HARDWARE-OATH ▾

If set, this Token type is pre-selected in the Token registration form.

Emergency OTP Management

☒ Emergency OTP Expiration 3600 ▾

When enabled, users can set an emergency OTP valid for the configured time.
Uncheck or set to '0' to disable emergency OTP management.

☐ Emergency OTP Max Use 0 ▾

When enabled, the OTP can be used a maximum number of times.
Uncheck or set to '0' for unlimited usage count.

SSH Key Management

☐ Allowed SSH Key Types ☐ HARDWARE ☐ SOFTWARE

Selection of SpanKey public key types users are able to register.
HARDWARE option requires inventoried SSH PIV devices.
MANUAL-PWD issues only password-protected SSH private keys.
If not set, any key type can be self-registered.

☐ Key Password Length 0 ▾

Minimum password length for newly-generated software SSH private keys.
Set '0' to disable password requirement.

Misc Settings

☒ Support Email

Your Organization support address.
When configured, a support request form is presented in the home page of the self-service.

☒ Token Download URL

The Software Token download page on an external website.
When configured, a download button is included in the OTP section.
Ex. <http://www.rcdevs.com/tokens/?type=software>

☐ TiQR Download URL

The TiQR mobile download page on an external website.
When configured, a download button is included in the OTP section.
Ex. <http://www.rcdevs.com/tokens/?type=tiqr>

4. Proxy_user rights on AD for SelfDesk app

The proxy_user will operate for the end user to reset the password, change user account information like mobile, mail, preferred languages... That means that the proxy_user account must have the required rights at the AD level to do these actions.

Note

Note that `CN=Users,DC=test,DC=local` used below is the user search base configured under the **WebADM Admin GUI** > **Admin** tab > **Local Domains** > **YOUR_DOMAIN** > **CONFIGURE** > **User Search Base** setting.

4.1 Rights for domain user accounts

For domain users, you have to configure the following rights for the proxy_user:

Token registration rights for a not extended schema

```
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootfile'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootparameter'
```

Token registration rights for an extended schema

```
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmsetting'
dscls "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmdata'
```

Common attributes rights

```
dscls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;mail'
dscls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;mobile'
dscls "CN=Users,DC=test,DC=local" /G 'TEST\proxy_user:WPRP;preferredLanguage'
```


Password reset rights

```
dsacIs "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;userPassword'  
dsacIs "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;pwdlastset'
```

Voice rights (if Schema extended)

```
dsacIs "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmVoice'
```

Voice rights (if Schema not extended)

```
dsacIs "CN=Users,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;audio'
```

4.2 Rights for domain administrator accounts

For domain admin users, you have to configure the rights on the AdminSDHolder object else, rights will be overridden after an hour.

Token registration rights for a not extended schema

```
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;bootfile'  
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G  
'TEST\proxy_user:WPRP;bootparameter'
```

Token registration rights for an extended schema

```
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G  
'TEST\proxy_user:WPRP;webadmsetting'  
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmdata'
```

Common attributes rights

```
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G 'TEST\webadm_admins:WPRP;mail'  
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G 'TEST\webadm_admins:WPRP;mobile'  
dsacIs "CN=AdminSDHolder,CN=System,DC=test,DC=local" /G  
'TEST\webadm_admins:WPRP;preferredLanguage'
```

Password reset rights

```
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;userPassword'  
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;pwdlastset'
```

Voice rights (if Schema extended)

```
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;webadmVoice'
```

Voice rights (if Schema not extended)

```
dscls "CN=AdminSDHolder,CN=System,DC=test,DC=local" /I:T /G 'TEST\proxy_user:WPRP;audio'
```

5. SelfDesk Usage

The **Self-Service** application is accessible via the following address:

https://YOUR_WEBADM/webapps/selfdesk/index.php

and through the **WAProxy** it is:

https://YOUR_WAPROXY/selfdesk/index.php



5.1 Manage personnel information

The **Home** tab allow you to view and manage account information such as mobile phone number, e-mail address, the preferred language and change his LDAP password.

User Self-Service Desk

Home

OTP

FIDO

SSH

Sign


PKI


Logout

Hello **test-user**.
Welcome to the Self-Service Portal at *com*.

User Information


User Name: *test-user*
User Domain: *Default*
Mobile Number: *[Not Set]*
Email Address: *[Not Set]*
Language: *[Not Set]*





Edit Information

Change Password




Provided by **RCDevs Security SA**

Click on **Edit Information** to change the user's information.


User Self-Service Desk

Login Name:




Mobile Number:

Email Address:

Language: 

Update

Cancel



Provided by **RCDevs Security SA**

Click on **Update** to update new information provided on your account.

User Self-Service Desk

Home

OTP

FIDO

SSH

Sign


PKI


Logout

Hello **test-user**.
Welcome to the Self-Service Portal at *com*.

User Information


User Name: *test-user*
User Domain: *Default*
Mobile Number: *352 123456*
Email Address: *test-user@rcdevs.com*
Language: *EN*





Edit Information

Change Password

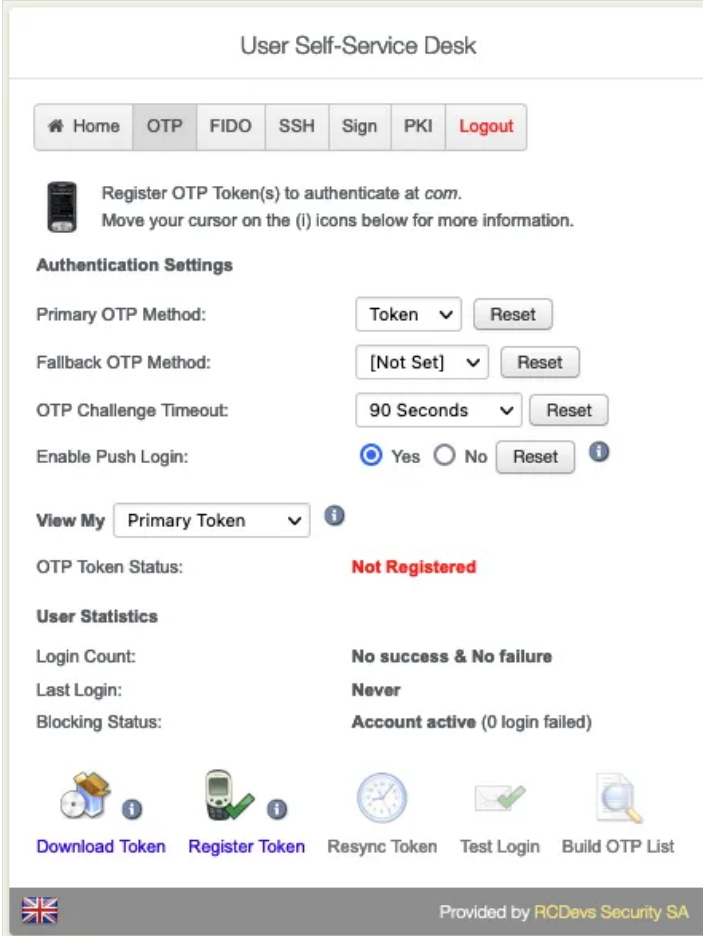


Provided by **RCDevs Security SA**

Click on [Change Password](#) and follow the instructions provided to change your password.

5.2 OTP Tokens enrollment

Go to the [OTP](#) tab. Choose the **Authentication Settings** like [Primary/Fallback OTP Method](#) and [Push Login](#).



The screenshot displays the 'User Self-Service Desk' interface. At the top, there is a navigation bar with tabs: Home, OTP (selected), FIDO, SSH, Sign, PKI, and Logout. Below the navigation bar, a message states: 'Register OTP Token(s) to authenticate at com. Move your cursor on the (i) icons below for more information.' The 'Authentication Settings' section includes: 'Primary OTP Method:' with a dropdown set to 'Token' and a 'Reset' button; 'Fallback OTP Method:' with a dropdown set to '[Not Set]' and a 'Reset' button; 'OTP Challenge Timeout:' with a dropdown set to '90 Seconds' and a 'Reset' button; and 'Enable Push Login:' with radio buttons for 'Yes' (selected) and 'No', and a 'Reset' button. Below this is a 'View My' dropdown set to 'Primary Token' with an information icon. The 'OTP Token Status:' is displayed as 'Not Registered' in red. The 'User Statistics' section shows: 'Login Count:' as 'No success & No failure'; 'Last Login:' as 'Never'; and 'Blocking Status:' as 'Account active (0 login failed)'. At the bottom, there are five icons with labels: 'Download Token', 'Register Token' (highlighted in blue), 'Resync Token', 'Test Login', and 'Build OTP List'. The footer includes a UK flag and the text 'Provided by RCDevs Security SA'.

Click on [Register Token](#). Choose between [Hardware](#), [YubiKey](#), [QRCode-based](#) or [Manual Registration](#) of the Token according to the type of Token you want to register.

5.2.1 Software Token


Press I use QRCode-Base authenticator and then a QRCode is prompted as the below example :

User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register a QRCode-based Software Token:

1. [Install the Software Token](#) on your mobile device.
2. Start your software Token and Scan the QRCode displayed below.
3. Click the 'Register' button below after scanning.



☐ I use a Hardware Token (Inventoried)

☐ I use a Yubikey Token (Inventoried / YubiCloud)

☒ I use a QRCode-based Authenticator (Time-based)


☐ I use a QRCode-based Authenticator (Event-based)

☐ I use another Token (Manual Registration) [i](#)

Register As:

Primary Token

QRCode:
([Enlarge](#))



[i](#)


Enter OTP:

.....

[i](#)

Register

Cancel



Provided by [RCDevs Security SA](#)


Scan the QRCode with your Token application previously installed on your phone. It should create a token entry in your application and 6 digits code should appears.

Enter the **OTP** provided by your application. This step is needed only if you are not using Push login. With Push login enabled, you don't need to provide the OTP as the registration will be done with a communication coming from OpenOTP Token application (phone) to the server.

User Self-Service Desk

Your Primary Token has been registered

Ok



Provided by [RCDevs Security SA](#)

Click on [Test Login](#) to verify if the **Software Token** has successfully enrolled.

User Self-Service Desk

Home

OTP


FIDO

SSH

Sign

PKI

Logout



Register OTP Token(s) to authenticate at *com*.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method:

Token

Reset

Fallback OTP Method:

[Not Set]

Reset

OTP Challenge Timeout:


90 Seconds

Reset

Enable Push Login:


☒ Yes ☐ No

Reset




View My

Primary Token



OTP Token Status:

Ok (Disable) (Unregister)



Token Type:

OATH Time-based (160 bits)

Time Interval:

30 Seconds

Max Time Offset:

120 Seconds

User Statistics

Login Count:


No success & No failure


Last Login:


Never


Blocking Status:


Account active (0 login failed)












Download Token

Register Token

Resync Token

Test Login

Build OTP List



Provided by *RCDevs Security SA*

Enter the **OTP** from the **OpenOTP Smartphone App**. (Only without the **Push Login**.)

User Self-Service Desk

This page allows you to test an authentication with the selected OTP methods.

Checking OpenOTP server status... **Ok**

Sending OTP authentication request... **Ok**

Result: **Challenge**


Message: Enter your TOKEN password

Timeout: 67 seconds

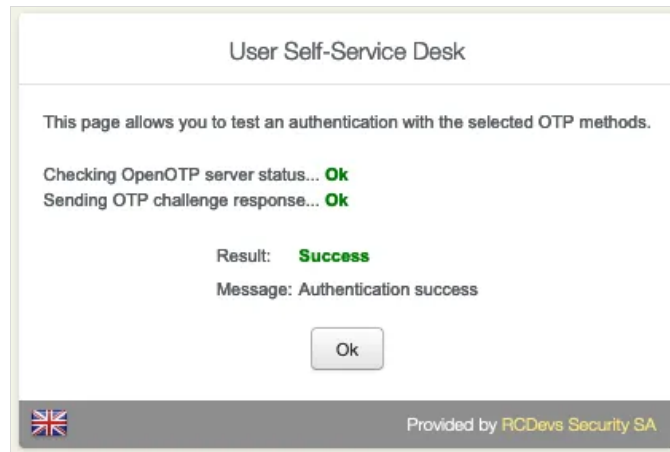
OTP:

Continue

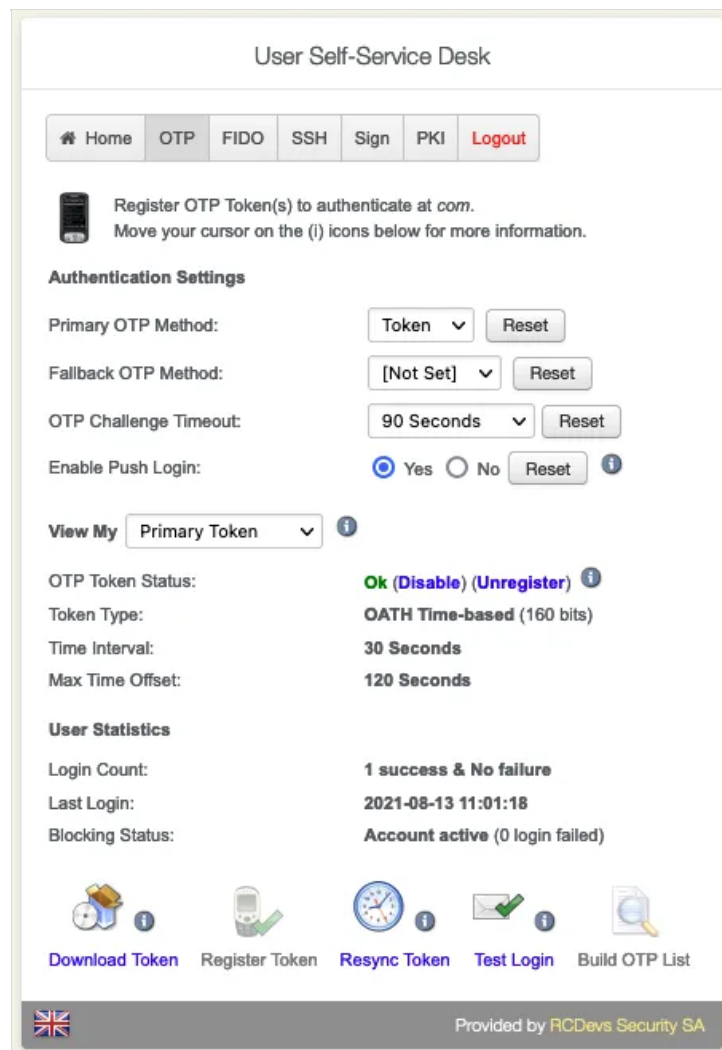
Cancel



Provided by *RCDevs Security SA*



In the **User Statistics**, there is the **Login Count**, **Last Login** and **Blocking Status**.



Click on **Resync Token** if the **Software Token** is out of sync. Always use an **NTP Server** on the **WebADM Servers** and the **Endpoints**.

5.2.2 Hardware Token (Inventoried)


To register an inventoried hardware token, select the correct option as shown in the screenshot below, and you need to provide the serial number written on the back of the token and the OTP in order to validate the enrollment and to initialize the Token.

User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register your Hardware Token:

1. Enter the serial number displayed on the back side of your Token.
2. Click the 'Register' button below.



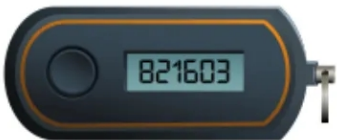
☒ I use a Hardware Token (Inventoried)

☐ I use a Yubikey Token (Inventoried / YubiCloud)

☐ I use a QRCode-based Authenticator (Time-based)

Register As:

Second Token



Token Serial:


2308700400845

Enter OTP:

.....

Register

Cancel




Provided by RCDévs Security SA

Press **Next** button and if all information provided can be successfully validated by the server, the token is enrolled on the account.

User Self-Service Desk

Your Primary Token has been registered

Ok



Provided by RCDévs Security SA

5.2.3 Yubikey (Inventoried/Yubicloud)


To enroll a Yubikey, select the correct option as shown in the screenshot below and press the Yubikey when you are invited to do it :

User Self-Service Desk

You must first register your Software or Hardware Token to start using it.
The registration consists in synchronizing a Secret Key and an initial Token state.

Instructions to register your Yubikey Token:


1. Plug the Yubikey in a USB port on your computer.
2. Press the Yubikey button to finish the registration.



☐ I use a Hardware Token (Inventoried)
☒ I use a Yubikey Token (Inventoried / YubiCloud)
☐ I use a QRCode-based Authenticator (Time-based)


Register As:

Third Token



[Press your Yubikey]

Cancel


 Provided by **RCDevs Security SA**

If the enrollment finished successfully, a confirmation message like below appears.

User Self-Service Desk

Your Primary Token has been registered

Ok


 Provided by **RCDevs Security SA**

5.2.4 VOICE biometric enrollment

Go to the **View My** drop menu and choose **Voice Biometrics** then click on **Click to Register**.

User Self-Service Desk


[Home](#) | [OTP](#) | [FIDO](#) | [SSH](#) | [Sign](#) | [PKI](#) | [Logout](#)

 Register OTP Token(s) to authenticate at *com*.
 Move your cursor on the (i) icons below for more information.

Authentication Settings


Primary OTP Method: Token ▼ Reset
 Fallback OTP Method: [Not Set] ▼ Reset
 OTP Challenge Timeout: 90 Seconds ▼ Reset
 Enable Push Login: ☒ Yes ☐ No Reset i


View My Voice Biometrics ▼


Voice Login Status: 
Click to Register


User Statistics


Login Count: **2 success & No failure**
 Last Login: **2021-08-13 16:35:27**
 Blocking Status: **Account active (0 login failed)**



[Download Token](#)


[Register Token](#)


[Resync Token](#)


[Test Login](#)


[Build OTP List](#)



Provided by RCDevs Security SA

The **Voice Biometrics** consists in speaking several times the same secret passphrase.


User Self-Service Desk

The voice registration consists in speaking several times the same secret passphrase.
 To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
 Or: *My name is test-user and my voice is my password.*



Click to Start
Cancel


Provided by RCDevs Security SA

Repeat the same **Passphrase**.

User Self-Service Desk


The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*

2

Click to Start

Cancel



Provided by [RCDevs Security SA](#)

Again, repeat the same **Passphrase**.

User Self-Service Desk


The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*

3

Click to Start

Cancel



Provided by [RCDevs Security SA](#)

Finally, repeat one last time the same **Passphrase**.

User Self-Service Desk


The voice registration consists in speaking several times the same secret passphrase.
To be secure, the chosen passphrase must be long enough (minimum 3 seconds).

Example passphrase: *Please authenticate me with my voice.*
Or: *My name is test-user and my voice is my password.*

4

Click to Start

Cancel




Provided by [RCDevs Security SA](#)

The **Voice Fingerprint** is successfully enrolled.

User Self-Service Desk

Your voice fingerprint has been registered

Ok



Provided by [RCDevs Security SA](#)

Click on [Test Login](#) to verify if the **Voice Fingerprint** has successfully enrolled.

User Self-Service Desk

Home

OTP


FIDO

SSH

Sign

PKI

Logout



Register OTP Token(s) to authenticate at *com*.
Move your cursor on the (i) icons below for more information.

Authentication Settings

Primary OTP Method:

Token

Reset

Fallback OTP Method:

[Not Set]

Reset

OTP Challenge Timeout:

90 Seconds


Reset

Enable Push Login:

☒ Yes

☐ No

Reset



View My

Voice Biometrics

Voice Login Status:

Ok (Unregister)

User Statistics

Login Count:


2 success & No failure

Last Login:


2021-08-13 16:35:27

Blocking Status:


Account active (0 login failed)




Download Token




Register Token




Resync Token



Test Login



Build OTP List



Provided by RCDévs Security SA

Hit the **Click to Speak** button and repeat your secret passphrase.

User Self-Service Desk

This page allows you to test an authentication with the selected OTP methods.

Checking OpenOTP server status... **Ok**

Sending OTP authentication request... **Ok**

Result:

Challenge


Message:

Enter your VOICE password

Timeout:

83 seconds


Voice Biometrics:



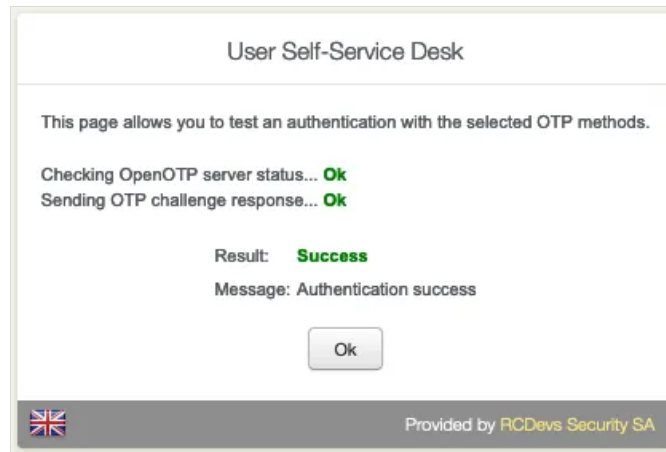
Click to Speak

Continue

Cancel



Provided by RCDévs Security SA

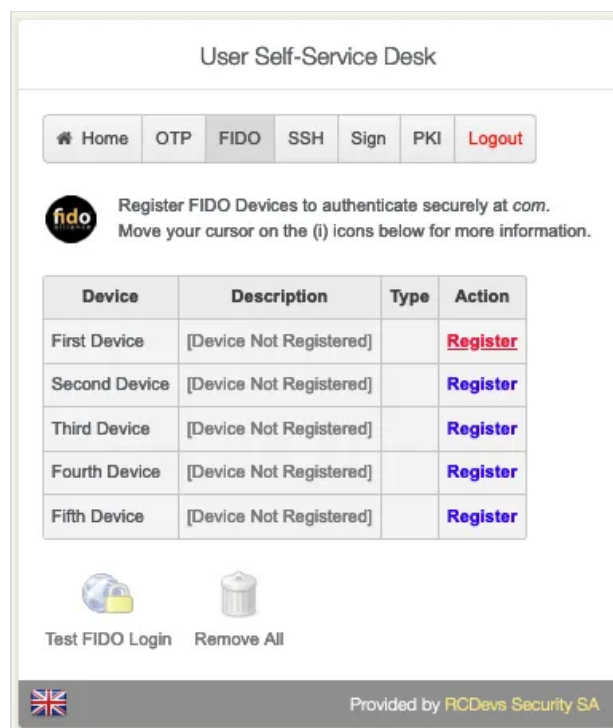


Note

For easy interaction with any integrations, the VOICE password can be provided through OpenOTP Token application if the configuration is allowed in OpenOTP server configuration. The setting to allow that is **Mobile Voice Login** set to **Yes**. VOICE biometric usage for MFA logins requires VOICE option as part of your license. Contact RCDevs Sales team for more information regarding that feature.

5.3 FIDO devices enrollment

Go to the **FIDO** tab and click on the first **Register** button available to register the new **FIDO device**.



Once you are on the following screen, plug the FIDO device you want to register on your computer and press the red message which is blinking.

User Self-Service Desk

You must first register your FIDO Device or Token to start using it.
If any of the checks below fails then the registration cannot be done.

Your Web browser supports FIDO: **Yes** ⓘ

Self-Service URL is enabled for FIDO: **Yes**

Instructions to register your FIDO Device:

- Plug the FIDO Device in a USB port on the computer.
- Click the blinking message below (or press Enter) to initiate the registration.
- When the device starts blinking, press the button to proceed the registration.



Friendly Name: ⓘ

Device Type: **FIDO2**

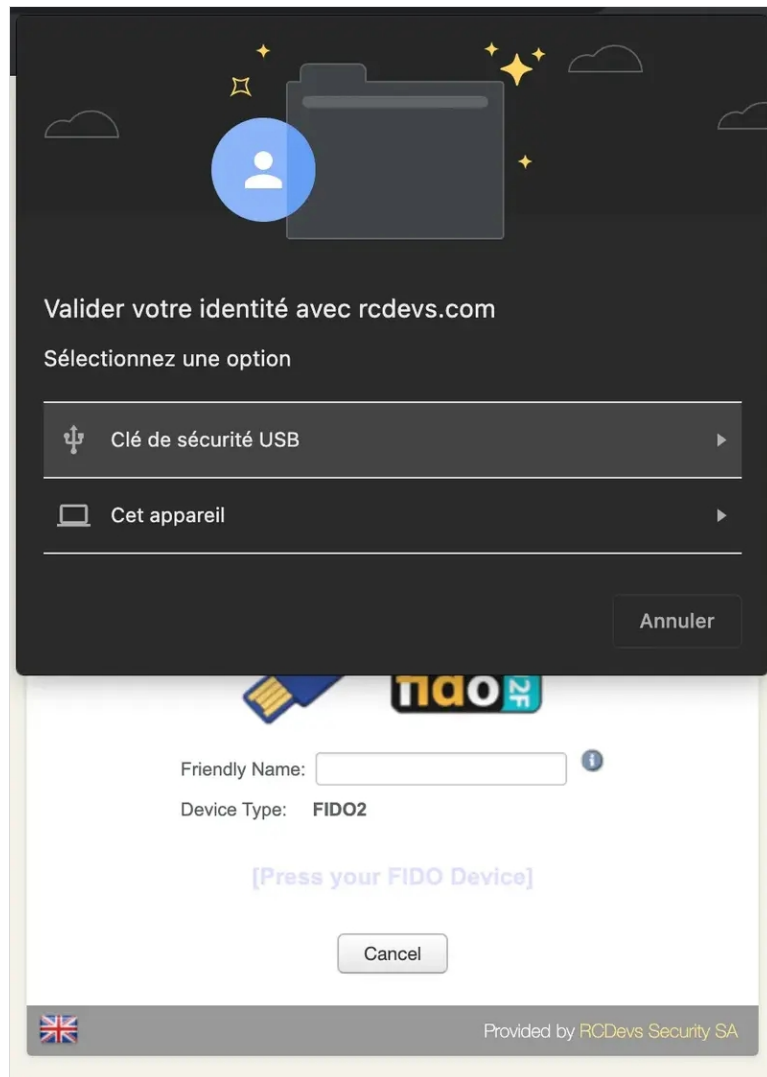
[Click Here or Press Enter]

Cancel

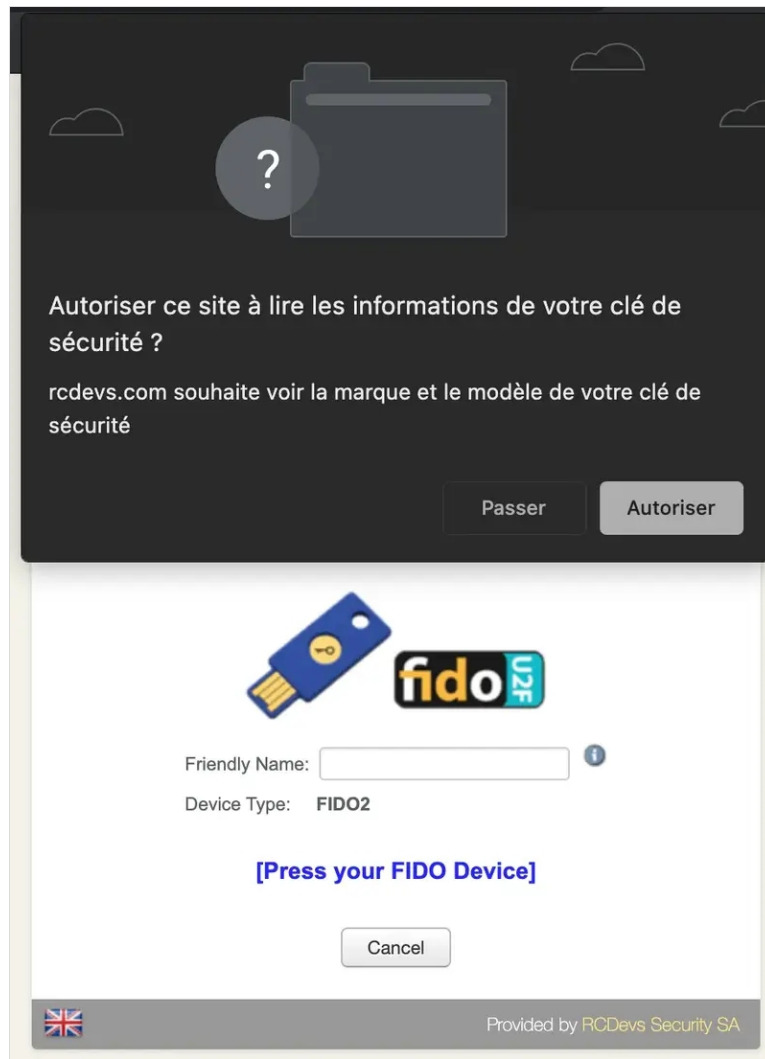


Provided by **RCDevs Security SA**

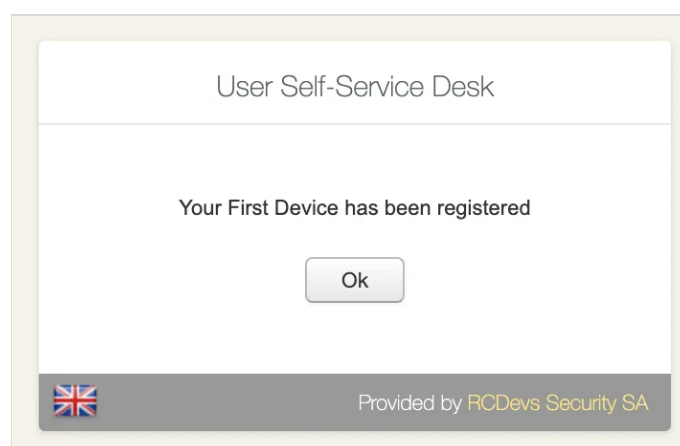
Once you clicked on the red message, if multiple FIDO devices are detected, you are prompted to choose the one you want to register. I selected my security key.



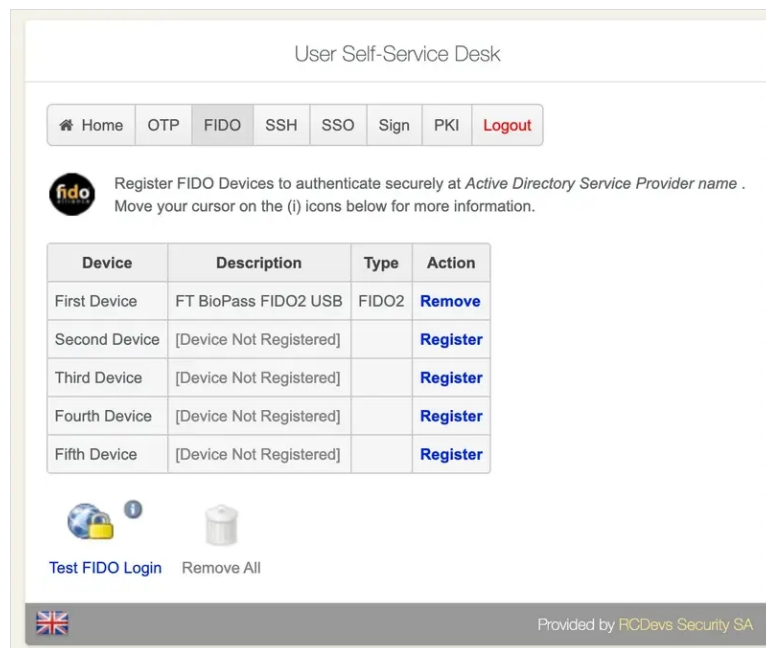
Then I have to allow the access to my security key in order to perform the registration. The key is now ready to be enrolled and my key (Feitian BioPass FIDO2) is blinking, which means I have to press the key to perform the enrollment.



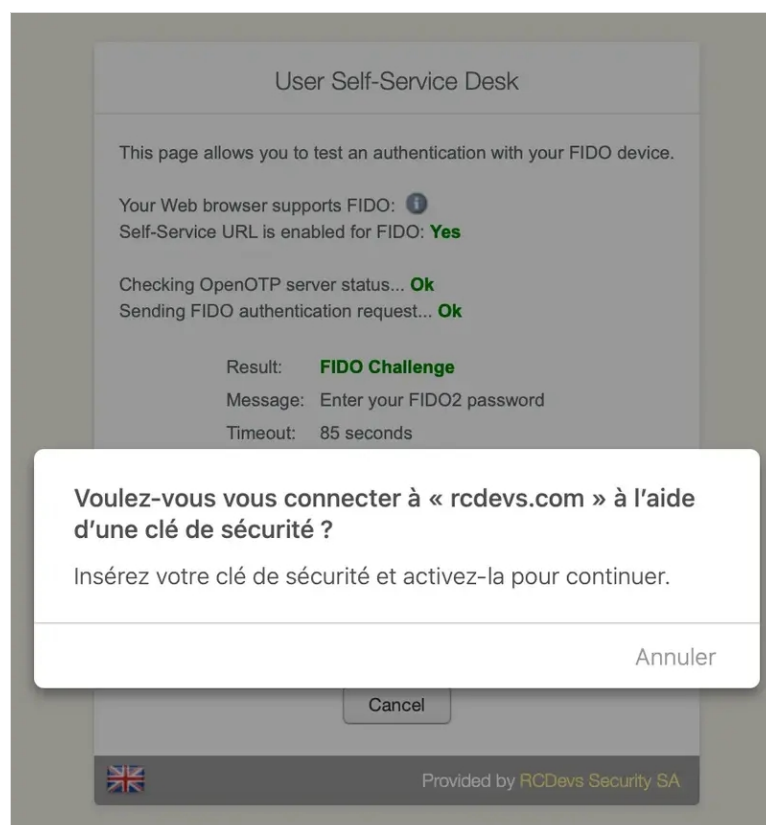
After pressing the key, the FIDO device is enrolled and can be used to log in on systems requiring FIDO authentication.



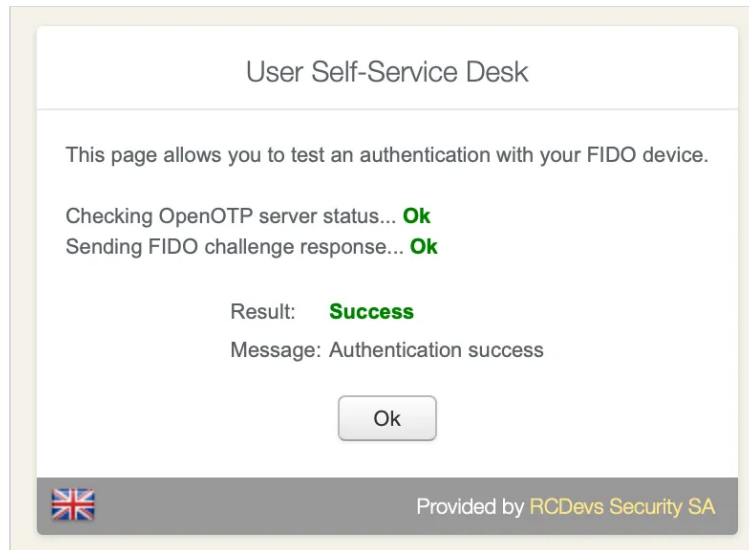
You can see now, the key registered on the account :



You can test if the key is working correctly by clicking the [Test FIDO login](#) button. My key is detected by my web browser and is blinking. I have to press the security key in order to be authenticated.

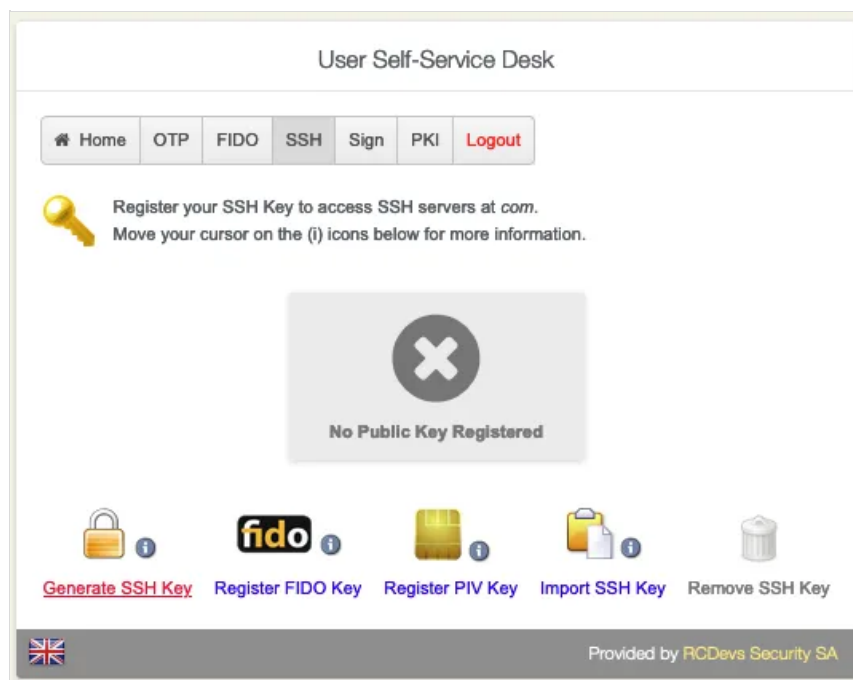


I am successfully authenticated, my FIDO device is correctly registered and ready to be used in my company's FIDO integrations.

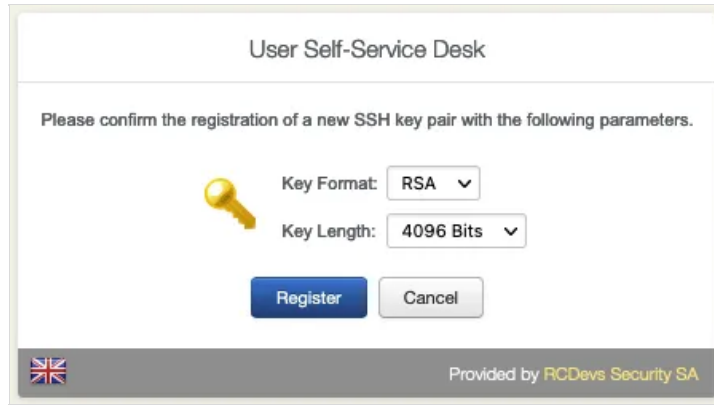


5.4 SSH Key enrollment for Spankey usage

Go to the **SSH** tab. Choose if you would like to **Generate SSH Key**, **Register FIDO Key**, **Register PIV Key**, **Import SSH KEY** or **Remove SSH KEY**.




Click on **Generate SSH Key** to add the FIDO Device.




User Self-Service Desk

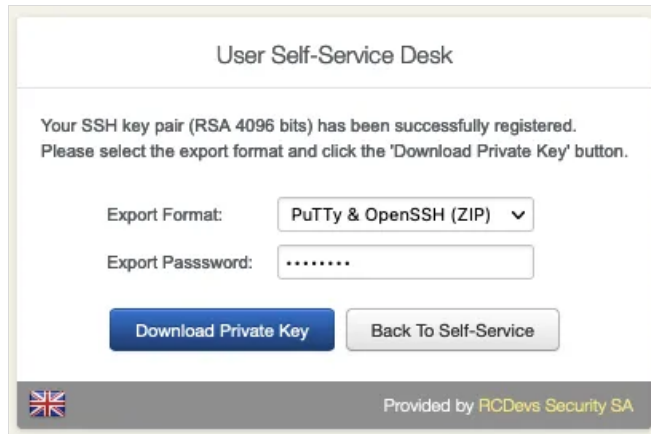
Please confirm the registration of a new SSH key pair with the following parameters.

 Key Format: RSA ▾

Key Length: 4096 Bits ▾

 Provided by **RCDevs Security SA**

Choose the **Key Format** and the **Key Length**.




User Self-Service Desk

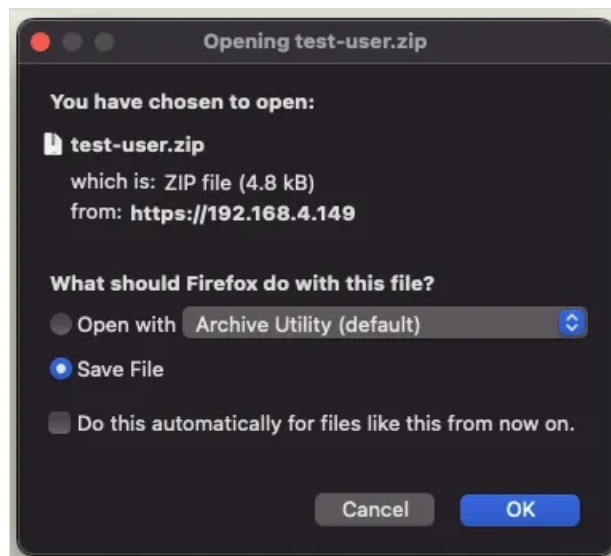
Your SSH key pair (RSA 4096 bits) has been successfully registered.
Please select the export format and click the 'Download Private Key' button.

Export Format: PuTTY & OpenSSH (ZIP) ▾

Export Password:

 Provided by **RCDevs Security SA**

Set a strong **Password** and download the **Private Key**.



In the **User Statistics**, there is the **Login Count** and **Last Login**.

User Self-Service Desk

Home
OTP
FIDO
SSH
Sign
PKI
Logout

An SSH public key is already registered on your account and is **VALID**.
 The key does not have an expiration date and will not auto-expire!
 The key does not have a maximum usage count!

SSH Public Key:
(RSA 4096 Bits)

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCAQCi8PiLu+AdPzdH1
7yzoK1UiqeEYFaUfYuLFbxZrhSzJ3JzVant6xsx4GqMQO
Fc15Y00U0xy/wLq5d88W1IWbDtKWORrJK
/B+eTuSyC9wrB5DptIXC6YWnJ7ErkWYtLV/nweld6mp6T
//TKRMhazT0d1cgPWwsEBk9hr0XLaoSOS1hVNpd2BNhG
T1q+3foNWxutNjpTjTkLCleLzidg8q92RfZN7I9nJn8Rj
3hDngMXWQ433TrnCN+N8hvj9H
/C9JA8I99YNL3BbxHylkJ+ewQP5xiN0TNbFzdYbf
/tIusMmQMDCROzy2FqvNGlam9QOtEV6CtMxmjJH5WfDx3
QaZ1c8LxJHI4HE/Z11siVz67ZzyF/J4B39e
/m0KxMmW6E1xY5EakiYR8Z80xwD9H8Nka96+2267w9C
```

User Statistics

Login Count: **No success & No failure**

Last Login: **Never**

[Renew SSH Key](#)

[Register FIDO Key](#)

[Register PIV Key](#)

[Import SSH Key](#)

[Remove SSH Key](#)

Provided by RCDevs Security SA

5.5 Submit PDF for Signature

The new Sign functionality allows the user connected to the Selfdesk application, the possibility to electronically sign a document. That feature is available since WebADM 2.0.23, Selfdesk 1.2.6 and OpenOTP 2.0. It also requires the OpenOTP Token application, the Push functionality must be configured in your WebADM infrastructure and a Push token enrolled on the user account. Go to the Sign tab.

User Self-Service Desk

Home

OTP

FIDO

SSH

SSO

Sign

PKI


Logout

Drag and drop a PDF document to sign it electronically.
Choose Advanced Signature mode to sign a printable document on your mobile.
Choose Qualified Signature to electronically sign with an external signing device.

Signature Mode:

Advanced (Handwritten Signature) ▼

Drop files here to upload



Provided by RCDevs Security SA

You can choose the Signature Mode you want to use. For more information regarding the 2 modes, please refer to the [REGULATION \(EU\) No 910/2014 OF THE EUROPEAN PARLIAMENT](#).

Drag and drop the document you want to send for Signature or click in the white zone to import the PDF you want to sign. Once the file has been loaded in the Selfdesk application, you will receive a push notification.

User Self-Service Desk

Home

OTP

FIDO

SSH

SSO

Sign


PKI

Logout

Drag and drop a PDF document to sign it electronically.
Choose Advanced Signature mode to sign a printable document on your mobile.
Choose Qualified Signature to electronically sign with an external signing device.


Signature Mode:

Advanced (Handwritten Signature) ▼



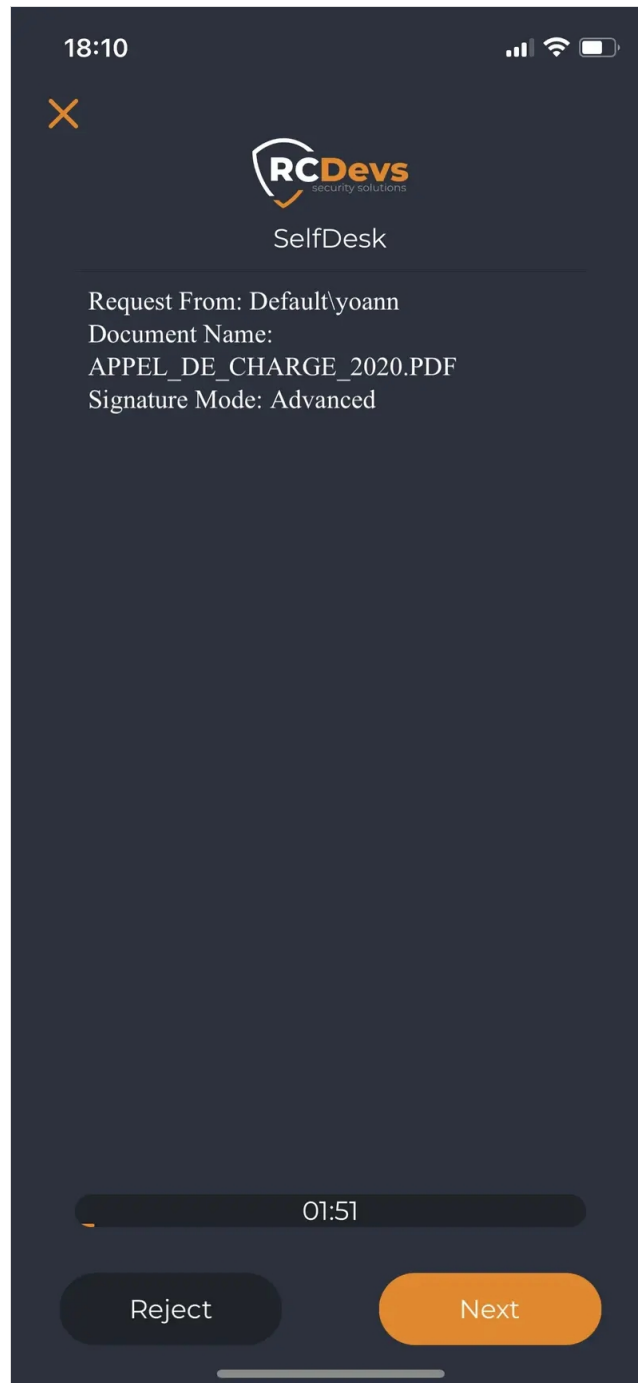
Sending PDF to your mobile phone...

Remaining time: 113 seconds



Provided by RCDevs Security SA

Once the document is uploaded, the user receives a notification on the OpenOTP Token application to sign the document.



Click the **Next** button to review the document:



Exercice du 01/01/20 au 31/12/20
METZ le 07/07/21
Page : 0001

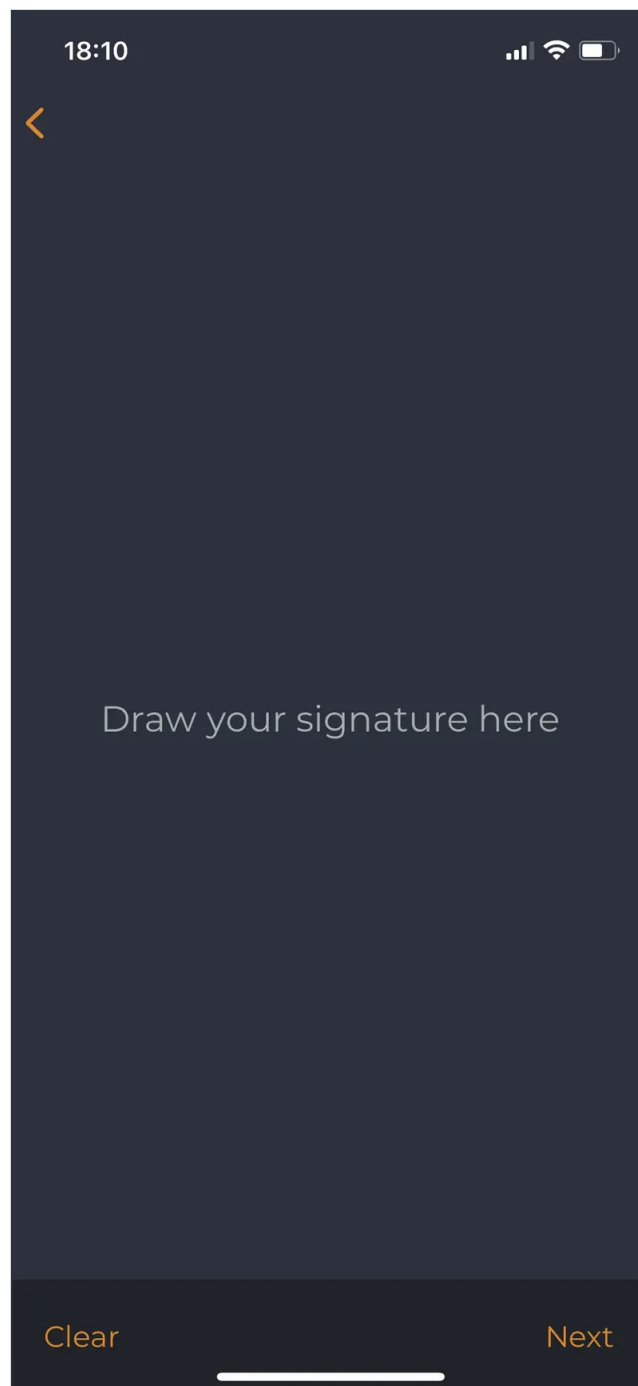
	LIBELLE	DEPENSES TTC	DONT T V A	CHARGES LOCATIVES	Fournisseurs
	Charges Courantes				
01 PARTIES COMMUNES GENERALES					
	615000 Entretien et petites réparatio				
	Entretien escaliers				
	INTERVENTION DU 04.12.2019	92,24	8,39	92,24	EST INCONNUE
	Travaux espaces verts				
	DEBROUSILLAGE	250,00			KERRER SEBASTIEN
	TOTAL 615000 Entretien et petites réparatio	342,24	8,39	92,24	
	621300 Frais postaux & photocopies				
	Télégram & photocopies				
	COMMUNICATION AG DU 04.02.20	86,64			GENERAL IMMOBILIER
	TOTAL 621300 Frais postaux & photocopies	86,64			
	TOTAL CLE 01 PARTIES COMMUNES GENERALES	428,88	8,39	92,24	
04 PC3 - CAGE ESCALIERS					
	602000 Electricité				
	Eclairage des communs				
	DU 27.03.2020 - 414 kWh	111,98	14,25	111,98	EDF SERVICE CLIENTS
	DU 27.03.2020 - 529 kWh	98,19	14,04	98,19	EDF SERVICE CLIENTS
	DU 29.07.2020 - -229 kWh	-13,78	-4,61	-13,78	EDF SERVICE CLIENTS
	DU 27.09.2020 - 304 kWh	67,84	8,75	67,84	EDF SERVICE CLIENTS
	DU 26.11.2020 - 353 kWh	81,65	9,92	81,65	EDF SERVICE CLIENTS
	TOTAL Eclairage des communs	345,48	44,35	345,48	
	TOTAL 602000 Electricité	345,48	44,35	345,48	
	606000 Fournitures				
	Fournitures diverses				
	ACHATS 2 TAPIS EXT	83,70	13,94	83,70	M. KLEIN
	ACHAT TAPISQU AFFICHAGE	105,39	17,57	105,39	M. KLEIN
	ACHATS 1 TAPIS INT	35,28	5,88	35,28	M. KLEIN
	ACHATS 1 TAPIS INT	35,28	5,88	35,28	M. KLEIN
	TOTAL Fournitures diverses	259,65	43,27	259,65	
	TOTAL 606000 Fournitures	259,65	43,27	259,65	
	611000 Nettoyage des locaux				

Sarl au capital de 100 000 euros - RCS Metz T1 N° 812 888 611 - N° TVA intracommunautaire FR : 69 812 888 11
Garantie par GALIAN - Carte professionnelle N° CPE 5701 2015 000 0001 141 - APE 6832A

ETAT DES CHARGES DE COPROPRIETE	
1	2
3	4
5	6
7	8
9	10
11	12
13	14
15	16
17	18
19	20
21	22
23	24
25	26
27	28
29	30
31	32
33	34
35	36
37	38
39	40
41	42
43	44
45	46
47	48
49	50
51	52
53	54
55	56
57	58
59	60
61	62
63	64
65	66
67	68
69	70
71	72
73	74
75	76
77	78
79	80
81	82
83	84
85	86
87	88
89	90
91	92
93	94
95	96
97	98
99	100

Next

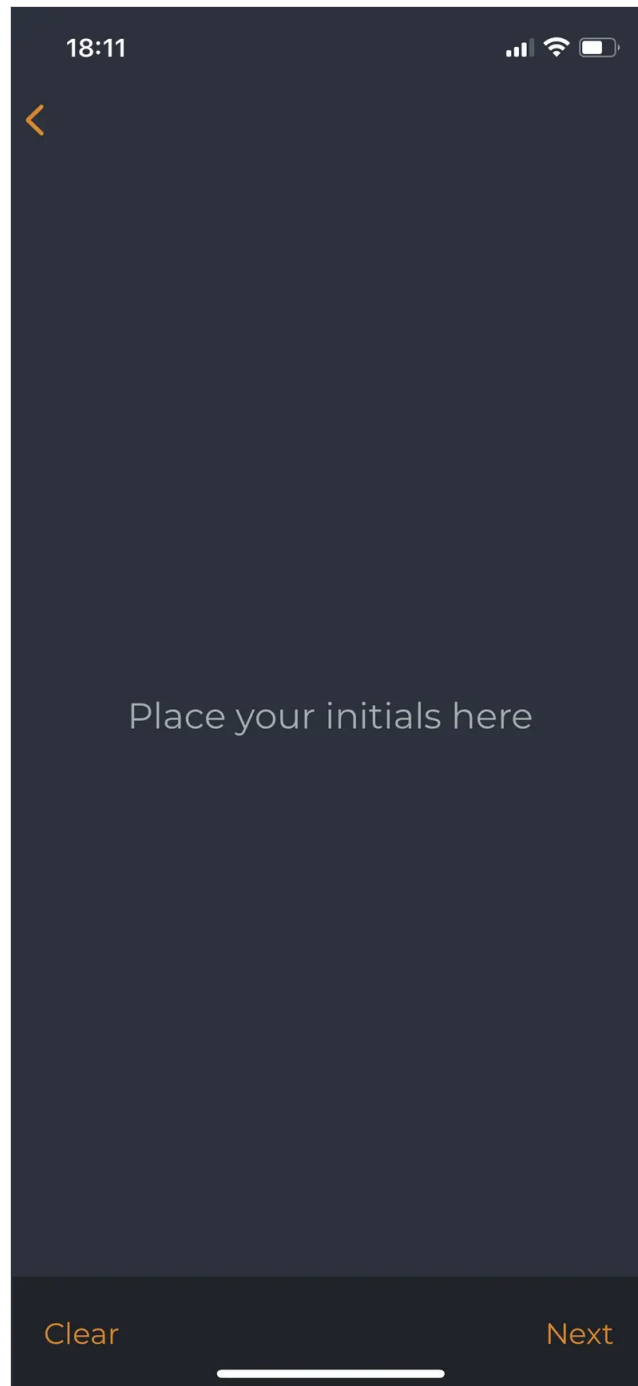
On the next screen, you are prompted on your phone to provide your handwritten signature which will be incorporated into the final document.



I provide my signature :



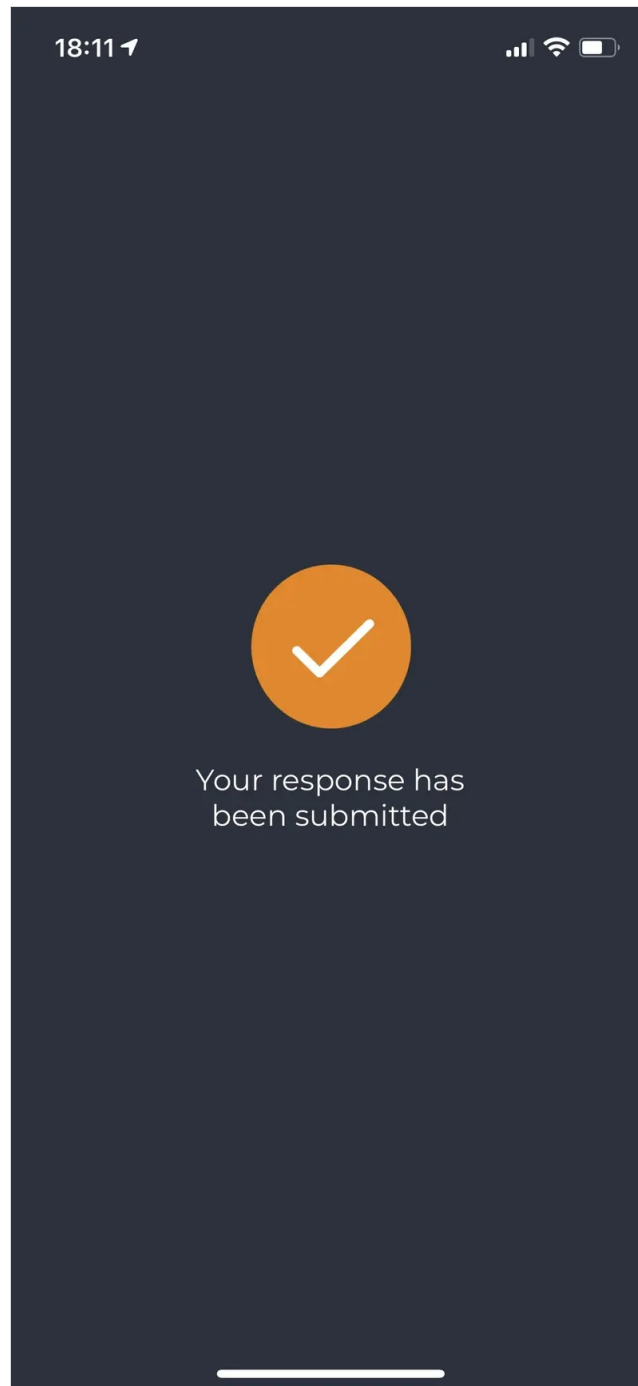
If the PDF contains multiple pages, you are invited to provide your paraps, which will be incorporated into all other pages.



I provide my paraps and then click **Next** :



The transaction is submitted to the server.



After that screen, the PDF is auto-prepared by RCDevs Cloud Services with the handwritten signature at the end of the document and paraps are added on intermediate pages. On top of that, the PDF is electronically signed and sealed with RCDevs certificates. If you check the signature validity/status, the status of the signature will depend on the type of mode of signature (Advanced/Qualified) that has been chosen at the beginning of the workflow to sign that document. For example, Adobe Reader will by default, show the signature validity in green as soon as the document has been signed with a qualified device. For advanced signature, it may appear in orange if the certificate authority file of RCDevs is not trusted in Adobe Reader.


Once the workflow is finished successfully, you can see the following screen on the SelfDesk application and the version of the signed PDF is automatically downloaded.

User Self-Service Desk


Home
OTP
FIDO
SSH
SSO
Sign
PKI
Logout

Drag and drop a PDF document to sign it electronically.
 Choose Advanced Signature mode to sign a printable document on your mobile.
 Choose Qualified Signature to electronically sign with an external signing device.

Signature Mode: Advanced (Handwritten Signature) ▼



PDF file signed successfully


Provided by RCDevs Security SA

You can verify the electronic signature with Adobe Reader or with a PDF digital signature validator.

Signed and all signatures are valid.

Signatures

✓ **Validate All**

✓ **Page 1: Signed by Seal Certificate #1 - clouddevs.com**

Signature is valid:

- Document has not been modified since this signature was applied
- Signature is valid, but revocation of the signer's identity could not be checked
- Signing time is from the clock on the signer's computer
- Signature is not CTR enabled and will expire after 2025/10/01 16:08:06 +02'00'

✓ **Signature Details**

Reason: Digitally verifiable PDF exported from clouddevs.com

Location: clouddevs.com

Certificate Details...

Last Checked: 2021/08/16 10:49:06 +02'00'

Field: Signature on page 3

[Click to view this version](#)

✓ **Annotations Modified**

✓ **Reason added on page 1**

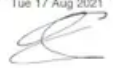
✓ **Signature added on page 2**

ETAT DES CHARGES DE COPROPRIETE

Immeuble : 007273

LIBELLE	DEPENSES TTC	DONT T V A	CHARGES LOCATIVES	FOURNISSEURS
TOTAL 621100 Rémunération du syndic	1958,40	326,40		
TOTAL CLE 9Z HONORAIRES SYNDIC	1958,40	326,40	0,00	
TOTAL Charges Courantes	6472,07	790,41	2905,37	
TOTAL POUR L'IMMEUBLE 007273	6472,07	790,41	2905,37	

Done at 4360 Esch-sur-Alzette, Luxembourg
Tue 17 Aug 2021



See proofs of signatures above.

If you want to involve multiple signatories for the same document, you can send the first signed PDF version to the next person who should sign it. His handwritten signature/paraphs will be added to the document and the cryptographic proof of the signature is added after the existing signature block. Found below, the example of the same document signed by 2 persons :

Signed and all signatures are valid. Document was updated after signing. Open Signature Panel to view the document change history.

Signatures

Validate All

Rev. 1: Signed by Seal Certificate #1 cca@rcdevs.com

Signature is valid:
This revision of the document has not been altered.
There have been subsequent changes to the document.
Signature is valid, but revocation of the signer's identity could not be checked.
Signing time is from the clock on the signer's computer.
Signature is not CTV enabled and will expire after 2025/10/31 18:08:28 +02'00'

Signature Details
Reason: Digitally verifiable PDF exported from cloud.rcdevs.com
Location: cloud.rcdevs.com
Certificate Details...
Last Checked: 2021/08/18 18:59:56 +02'00'
Field: Signature 1 on page 1
[Click to view this version](#)

Annotations Created
Square annot on page 1
Square annot on page 2

Rev. 2: Signed by Seal Certificate #2 cca@rcdevs.com

Signature is valid:
Document has not been modified since this signature was applied.
Signature is valid, but revocation of the signer's identity could not be checked.
Signing time is from the clock on the signer's computer.
Signature is not CTV enabled and will expire after 2025/10/31 18:10:27 +02'00'


Signature Details
Reason: Digitally verifiable PDF exported from cloud.rcdevs.com
Location: cloud.rcdevs.com
Certificate Details...
Last Checked: 2021/08/18 18:59:57 +02'00'
Field: Signature 2 on page 1
[Click to view this version](#)


Annotations Modified
Square annot on page 1
Square annot on page 2
Square annot on page 1
Square annot on page 2

Signature Panel

ETAT DES CHARGES DE COPROPRIETE

	LIBELLE	DEPENSES TTC	DONT T V A	CHARGES LOCATIVES	FOURNISSEURS
TOTAL	621100 Rémunération du syndic	1958,40	328,40		
TOTAL CLE 92 HONORAIRES SYNDIC		3956,40	328,40	0,00	
TOTAL Charges Courantes		6472,07	790,41	2905,37	
TOTAL POUR L'IMMEUBLE 907273		6472,07	790,41	2905,37	

Done at 4360 Esch-sur-Alzette, Luxembourg
Tue 17 Aug 2021


Done at 4360 Esch-sur-Alzette, Luxembourg
Wed 18 Aug 2021


Données exportées de 102 000 euros - 903 Mises à jour - 2021/08/18 18:59:57 - 18:59:57 - 18:59:57 - 18:59:57
Révisé par: cloud.rcdevs.com - 18:59:57 - 18:59:57 - 18:59:57 - 18:59:57

Signatures status are displayed in green in Adobe Reader because I trusted the RCDevs CA certificate in Adobe Reader :

Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.






☐ Show all certification paths found

RCDevs Root CA <ca@
Seal Certificate #1

Summary | Details | Revocation | **Trust** | Policies | Legal Notice

This certificate is not trusted.

Trust Settings

-  Sign documents or data
-  Certify documents
-  Execute dynamic content that is embedded in a certified document
-  Execute high privilege JavaScripts that are embedded in a certified document
-  Perform privileged system operations (networking, printing, file access, etc.)

Add to Trusted Certificates...



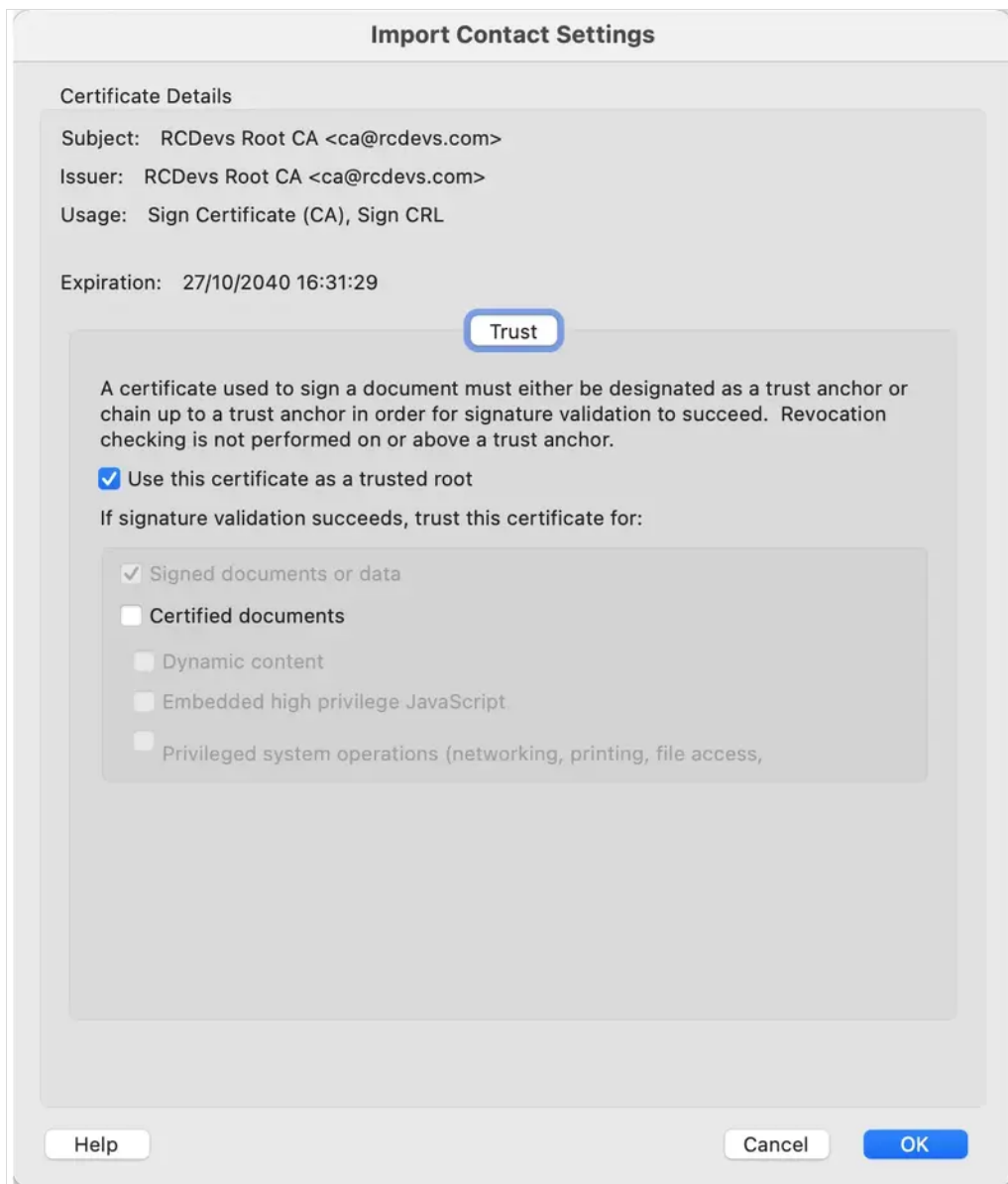
The selected certificate path is valid.

The path validation checks were done as of the signing time:

2021/08/17 18:11:10 +02'00'

Validation Model: Shell

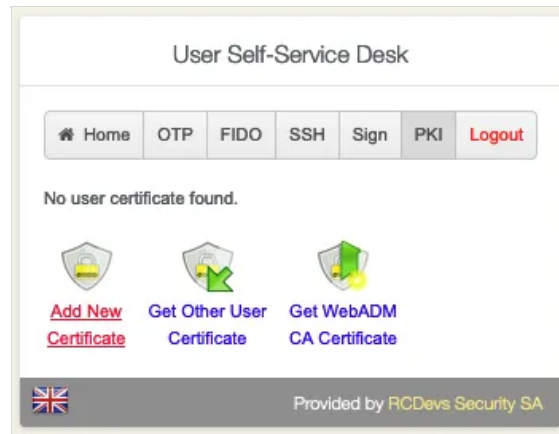
OK



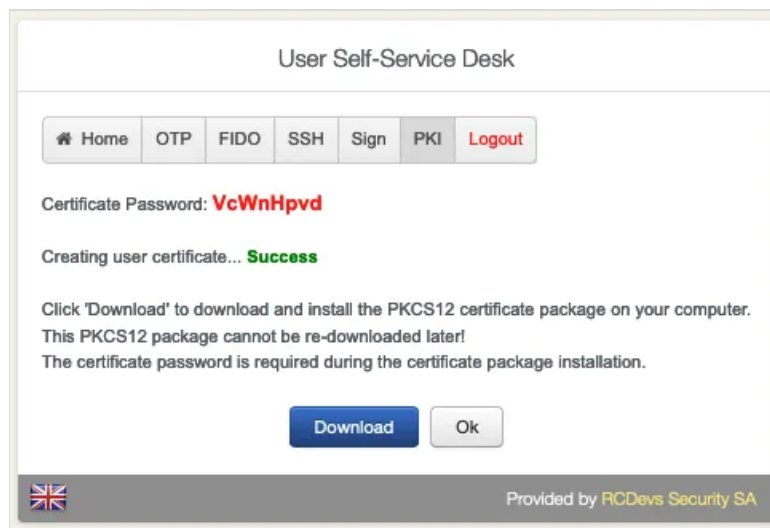
This is not needed when signatures are produced by qualified devices because Adobe Reader already trust the Certificate Authorities used to provide qualified devices.

5.6 User Certificate enrollment

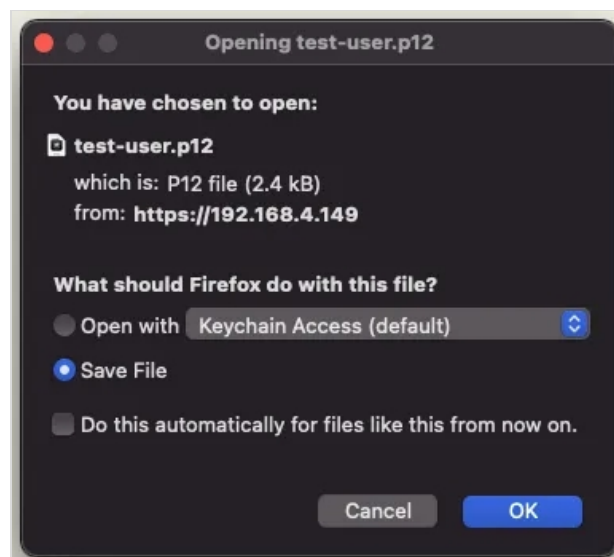
Go to the **PKI** tab. Choose if you would like to **Add New Certificate**, **Get Other User Certificate** or **Get WebADM CA Certificate**.



Click on **Add New Certificate**.



Download the **New Certificate**.



Overview of all the users' certificates. **Download**, **Renew** or **Delete** a certificate.

User Self-Service Desk

Home

OTP

FIDO


SSH


Sign

PKI


Logout


Click the actions in the table below to download, renew or delete your certificates.

Serial	Name	Valid From	Valid To	Status	Actions
2	Defaulttest-user	13/08/2021	13/08/2022	Valid	  


Add New
Certificate


Get Other User
Certificate


Get WebADM
CA Certificate

 Provided by RCDevs Security SA

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved