

Step-1 : Go to this URL and register yourself.

Url :- http://202.51.70.18/register/

The screenshot shows a web browser window with the URL <http://202.51.70.18/register/>. The page title is "Welcome to RCertVault". A sub-instruction says "Please fill the below form to register." The form contains six input fields: "Username*", "Password*", "Confirm Password*", "Full Name*", "Email*", and "Contact*". Below the form is a blue "Submit" button. At the bottom of the page, a copyright notice reads "© 2025 RCertVault. All rights reserved."

Welcome to RCertVault

Please fill the below form to register.

Username*

Password*

Confirm Password*

Full Name*

Email*

Contact*

Submit

© 2025 RCertVault. All rights reserved.

Step-2 : After the registration is completed, go to the login section.

Url :- http://202.51.70.18/admin/

The screenshot shows a web browser window with the URL <http://202.51.70.18/admin/login/?next=/admin/>. The page title is "RCertVault Admin". It features a login form with two input fields: "Username:" and "Password:", each with its own input box. Below the password field is a "Log in" button.

RCertVault Admin

Username:

Password:

Log in

Step-3 : Use your username and password to log in to the dashboard.

Welcome to the RCertVault Dashboard

ACCOUNTS

	+ Add	Change
Api tokens	+ Add	Change
Key Holders	+ Add	Change
Organization memberships	+ Add	Change
Users	+ Add	Change
Vault	+ Add	Change

API ACCESS LOGS

	View
Api Access Log (s)	View

AUTHENTICATION AND AUTHORIZATION

	+ Add	Change
Groups	+ Add	Change

Recent actions

My actions

- [Dev \(pending\)
Key Holder](#)
- [test - ef167ae3-2bce-4677-9a3a-b113f2863387 \(Org: Nepal Insurance Authority\)
Api token](#)
- [Dev \(pending\)
Vault](#)

Step-4: Go to the Key Holders section and click on your name (in my case, Test) to edit it.

RCertVault Admin

Home > Accounts > Key Holders

Select Key Holder to change

Action:	NAME	EMAIL	STATUS	SUBMITTED AT	CONTACT
<input type="checkbox"/>	Test	tes@g.com	Pending	Dec 29, 2025, 3:10 p.m.	+9779811111111

1 Key Holder

FILTER

- Show counts
- By status

- All
- Pending
- Maker Approved
- Checker Approved
- Rejected

Step-5 :- Upload your public key file (.p7b), choose the organization, and save.

The screenshot shows the RCertVault Admin interface. On the left, there's a sidebar with sections like 'ACCOUNTS', 'API ACCESS LOGS', and 'AUTHENTICATION AND AUTHORIZATION'. The main area is titled 'Change Key Holder' for 'Test (pending)'. It has fields for 'Serial number' (empty), 'Public key file' (with a 'Choose File' button and 'No file chosen' message), 'Certificate Details' (empty), 'Contact' (+9779811111111), and 'Organization' (set to 'Nepal Insurance Authority'). Below these is a note about selecting multiple organizations. At the bottom are 'SAVE', 'Save and continue editing', and 'Delete' buttons.

Step-6 :- Go to the Vault section in the admin sidebar. Upload your .p12 private key and its PIN. If you want to enable auto-signing features, check the box. (*If auto-signing is not enabled, your vault will not be accessible without your permission.*)

The screenshot shows the RCertVault Admin interface. The sidebar includes 'ACCOUNTS', 'API ACCESS LOGS', and 'AUTHENTICATION AND AUTHORIZATION' sections. The main area is titled 'Change Vault' for 'Test (pending)'. It has a checkbox for 'Auto signing enabled' (unchecked), a field for '.p12 Private Key' with a 'Choose File' button and 'No file chosen' message, and a field for 'Private Key PIN'. At the bottom are 'SAVE', 'Save and continue editing', and 'Delete' buttons.

Step-7 :- Go to API Tokens and add a new API token. Choose your organization, select all permissions or only the ones you need, set an expiry date, add a description for reference, and click Save.

The screenshot shows the 'Add api token' page. On the left, there's a sidebar with 'ACCOUNTS' selected, showing 'Api tokens' (highlighted in yellow), 'Key Holders', 'Organization memberships', 'Users', and 'Vault'. The main area has tabs for 'Available groups', 'Chosen groups', 'Available user permissions', and 'Chosen user permissions'. It includes fields for 'Expires at' (Date: 2025-12-30, Time: Now), a 'Description' input, and a 'Save' button.

Step-8: Copy the token that is created and use it in your application to sign and verify PDFs from this platform.

The screenshot shows the 'Select api token to change' page. The left sidebar shows 'API ACCESS LOGS' with 'Api Access Log (s)' selected. The main area displays a table with one row of data:

Action:	TOKEN	USER	ORGANIZATION	CREATED AT	EXPIRES AT
<input type="checkbox"/>	0f5a5ec9-f0dd-4fdf-a097-8d4d3be4ae70	test1	Nepal Insurance Authority	Dec. 29, 2025, 3:24 p.m.	Dec. 30, 2025, 3:24 p.m.

Below the table, it says '1 api token'.

Step-8: Before your API works, your organization's Maker and Checker must approve your request.

- Look at the Status in Key Holders; it should be Checker Approved.

Home > Accounts > Key Holders

Start typing to filter...

ACCOUNTS

		+ Add
Api tokens		
Key Holders		
Organization memberships		+ Add
Users		
Vault		

Select Key Holder to change

Action: ----- Go 0 of 1 selected

<input type="checkbox"/>	NAME	EMAIL	STATUS	SUBMITTED AT	CONTACT
<input type="checkbox"/>	Test	tes@g.com	Pending	Dec. 29, 2025, 3:10 p.m.	+9779811111111

1 Key Holder

API ACCESS LOGS