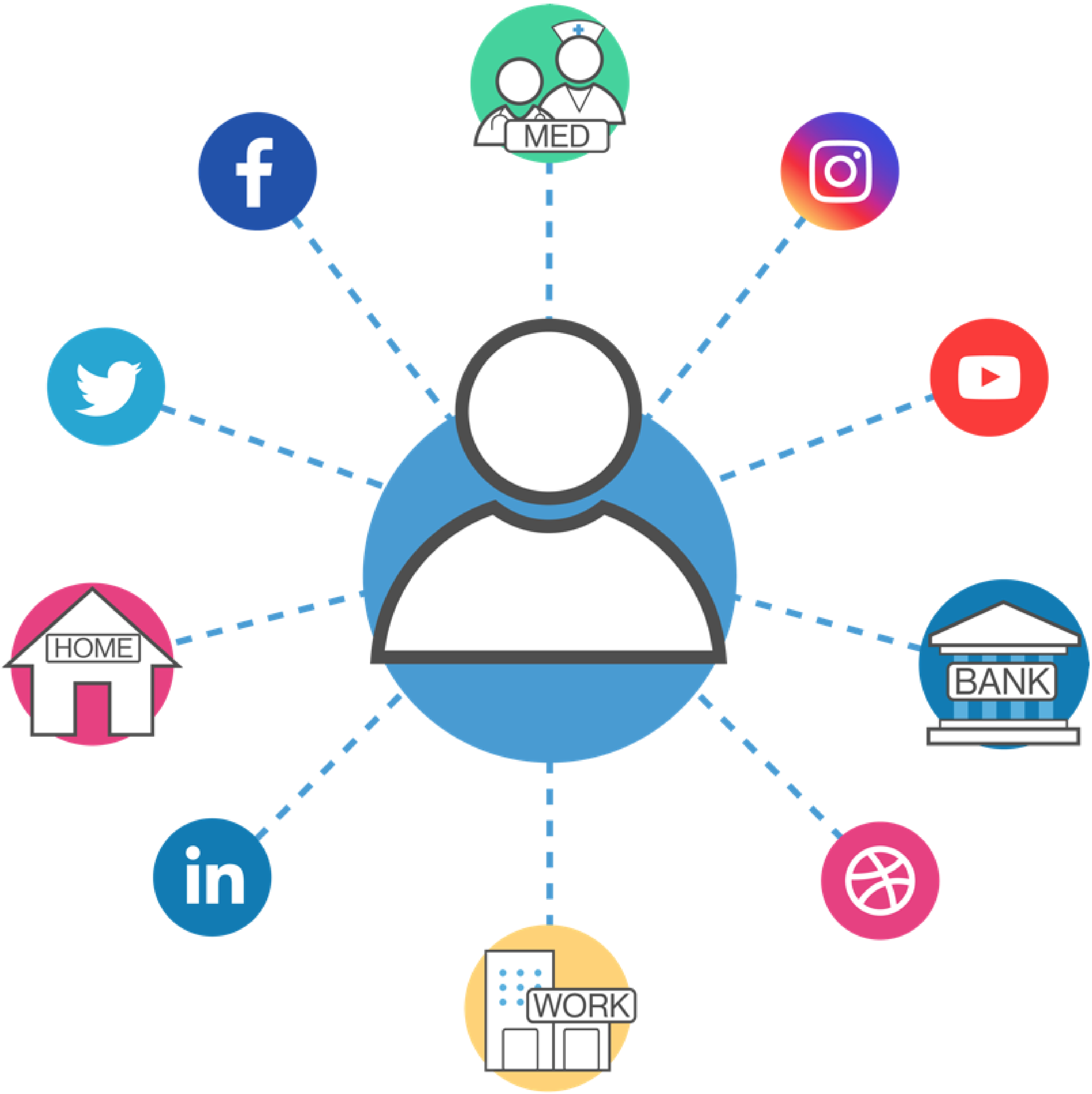
Decentralized Identifiers



User Guide

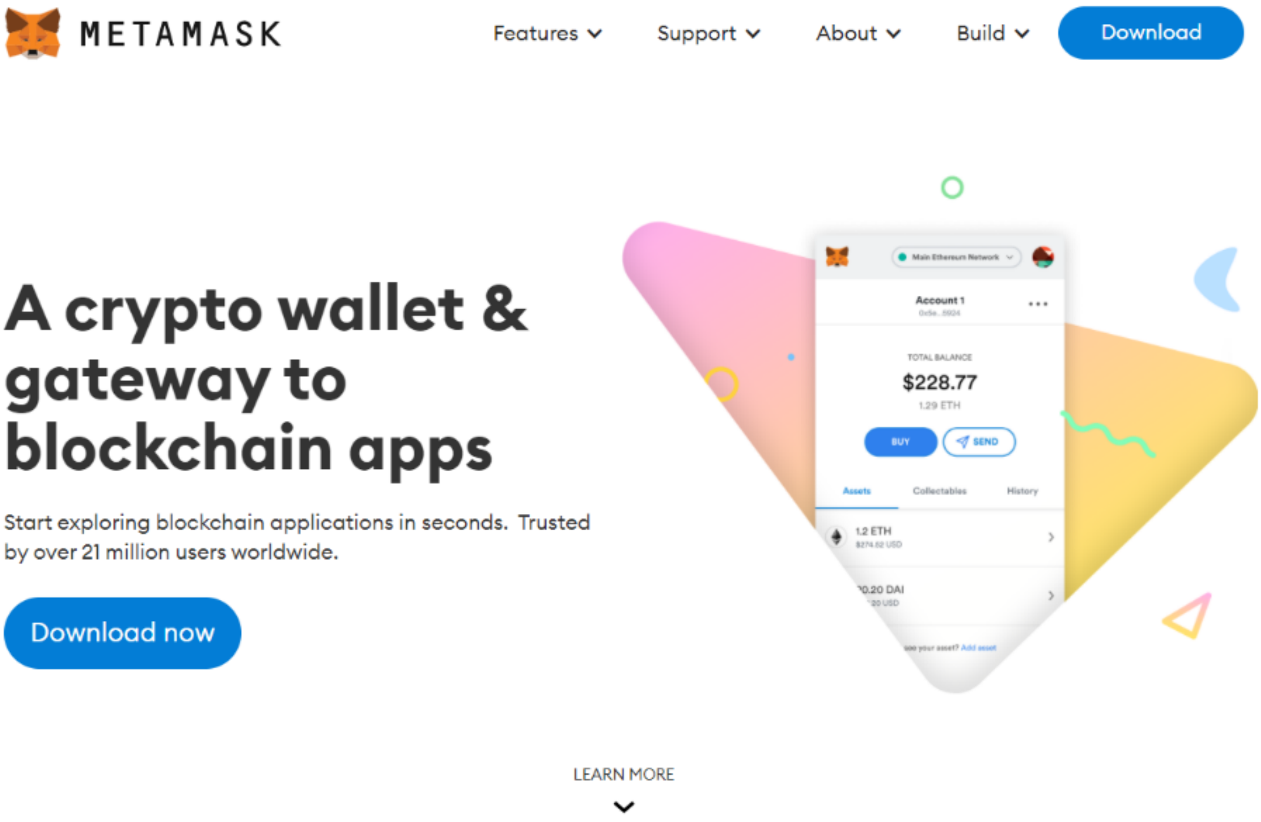
MetaMask Wallet

Each person should have a unique address in order to have an identity. To reach that address we create an account in Ethereum Network, which has a public key and a private key. The public and private keys show our address (e.g. home address) and a private password, respectively.

To create and manage our accounts we use MetaMask, an extension on browser. Instead of having centralized database, that stores our private and public keys, we store our keys there in a decentralized order, which is safer.

In MetaMask we have a master key, which is the unique password of our wallet and holds all of our accounts. If anyone has that master key he/she has access to all of our public and private keys.

Here is the MetaMask website where you can install MetaMask for the platform you are using.

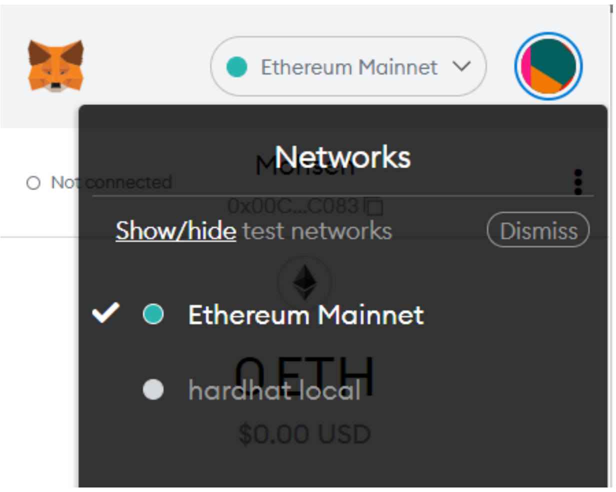


A crypto wallet & gateway to blockchain apps

Start exploring blockchain applications in seconds. Trusted by over 21 million users worldwide.

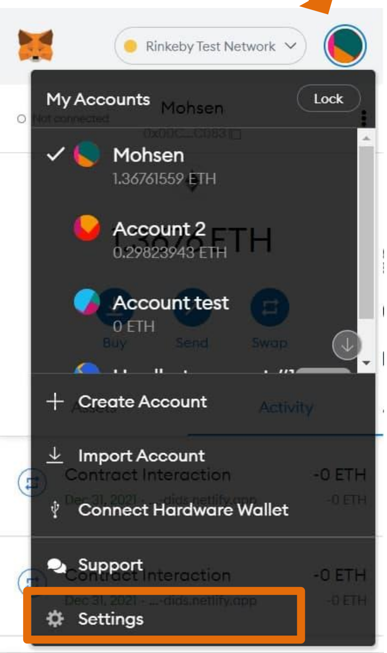
We have different networks. One of which is main net, and all of the coins have a real value, and you have to pay real money to earn coins. Another network is test net, and it is used for testing, where the coins do not have real value, and there are some websites where you can buy these coins freely. Some famous test names are Rinkeby, Kovan, Ropsten.

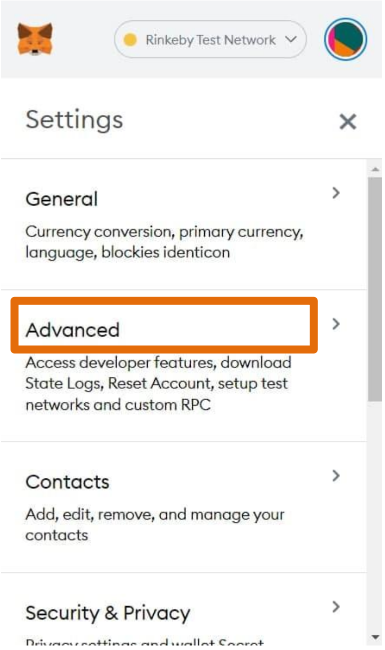
In this project we chose Rinkeby as our test net. MetaMask shows main nets as default.



In order to make test nets visible, you have to go to setting, then head to advanced section, and activate show test networks. These steps are shown below :

Click Here



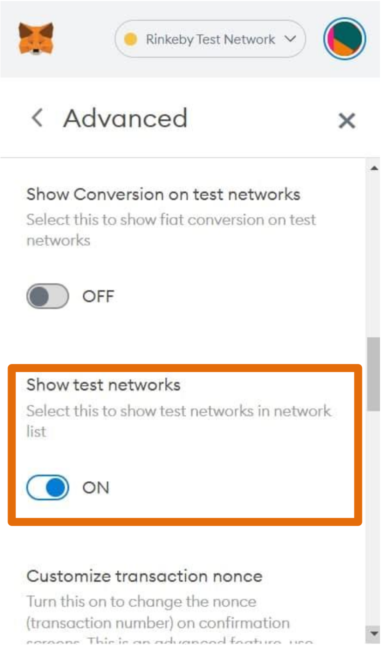


General
Currency conversion, primary currency, language, blockies identicon

Advanced
Access developer features, download State Logs, Reset Account, setup test networks and custom RPC

Contacts
Add, edit, remove, and manage your contacts

Security & Privacy

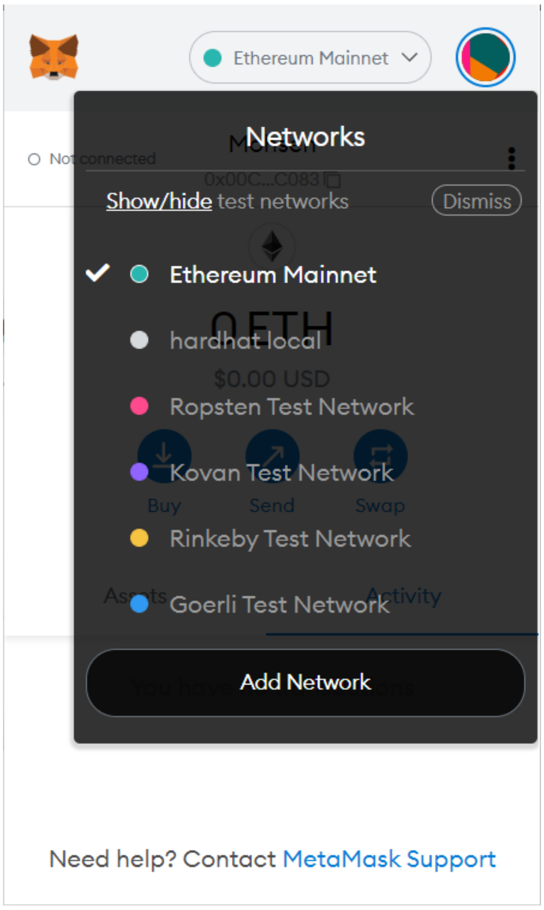


Show Conversion on test networks
Select this to show fiat conversion on test networks
OFF

Show test networks
Select this to show test networks in network list
ON

Customize transaction nonce
Turn this on to change the nonce (transaction number) on confirmation

Then MetaMask shows all the test nets.



Ethereum Mainnet

Networks

Show/hide test networks Dismiss

✓ ● Ethereum Mainnet

● hardhat local

● Ropsten Test Network

● Kovan Test Network

● Rinkeby Test Network

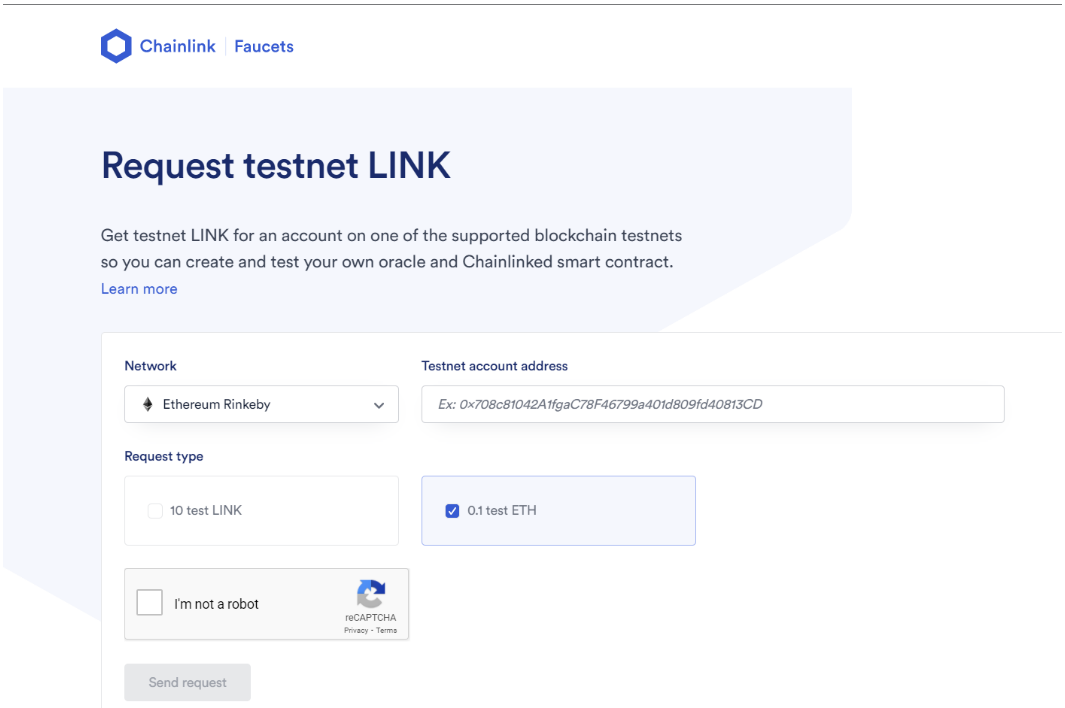
● Goerli Test Network

Add Network

Need help? Contact MetaMask Support

And then for charging your account you can go to some sites which are called faucets and buy coins without paying money.

https://faucets.chain.link/rinkeby is one of those sites. By getting there and entering your account's address you can get free test coins.



Chainlink | Faucets

Request testnet LINK

Get testnet LINK for an account on one of the supported blockchain testnets so you can create and test your own oracle and Chainlinked smart contract.
Learn more

Network: Ethereum Rinkeby

Testnet account address: Ex: 0x708c81042A1fgaC78F46799a401d809fd40813CD

Request type

□ 10 test LINK

☑ 0.1 test ETH

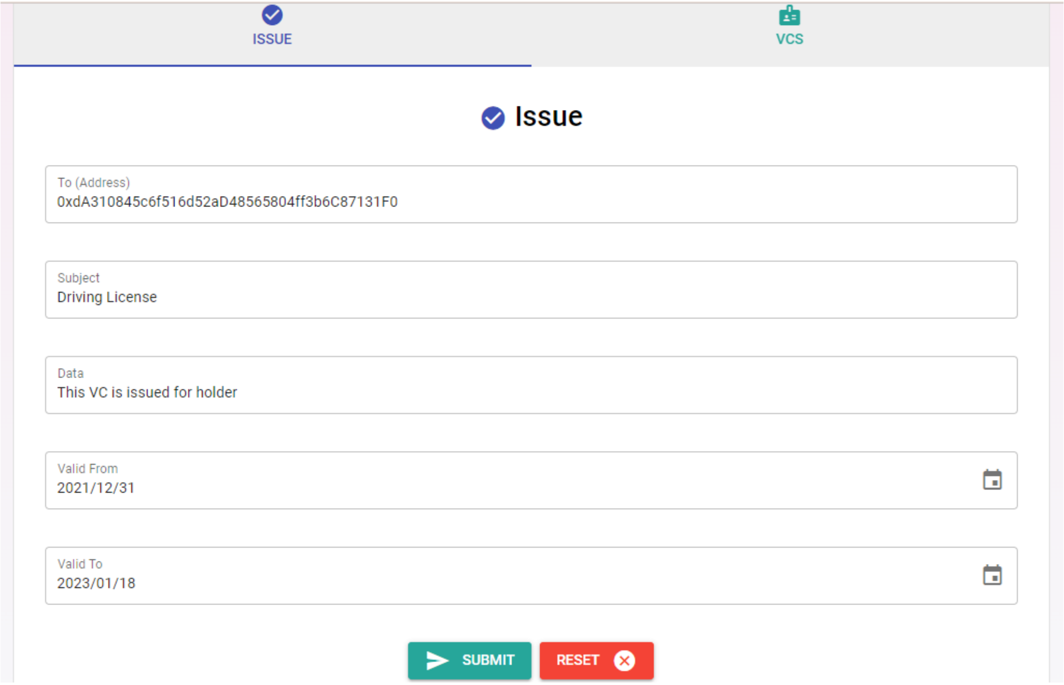
□ I'm not a robot

Send request

Issuer

- Issuer is an entity creating a verifiable credential, associating it with a specific subject and transmitting it to a holder. Examples of these are corporations, governments or non-profit organizations.

With having the address of a holder, the issuer can issue a verifiable credential (VC) for that specific holder. The VC has subject, data, issuance date and expiration date.



To (Address)
0xdA310845c6f516d52aD48565804ff3b6C87131F0

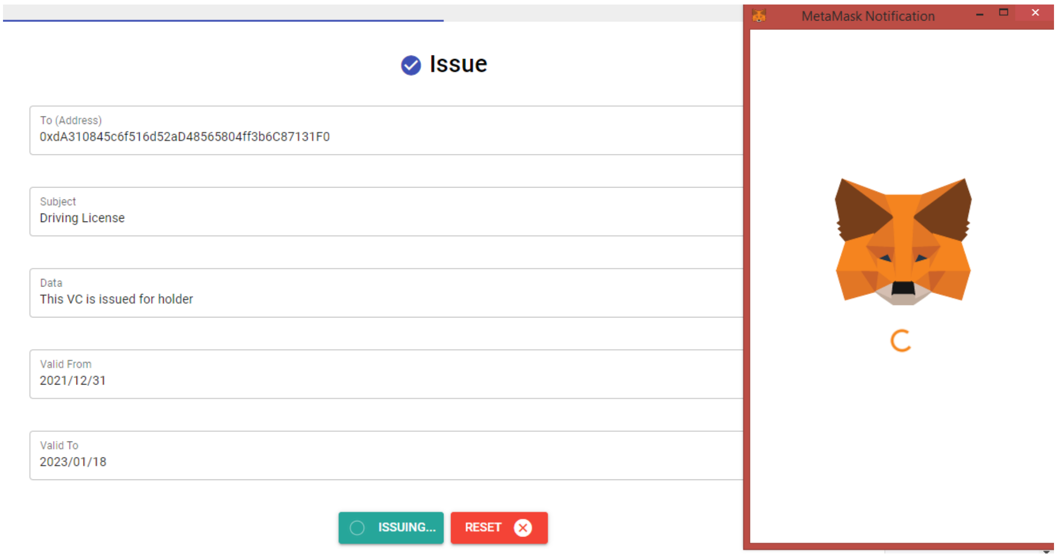
Subject
Driving License

Data
This VC is issued for holder

Valid From
2021/12/31

Valid To
2023/01/18

After submitting a VC for the specific holder, issuer must confirm the transaction (issuing a VC) in MetaMask to end up issuing successfully.



To (Address)
0xdA310845c6f516d52aD48565804ff3b6C87131F0

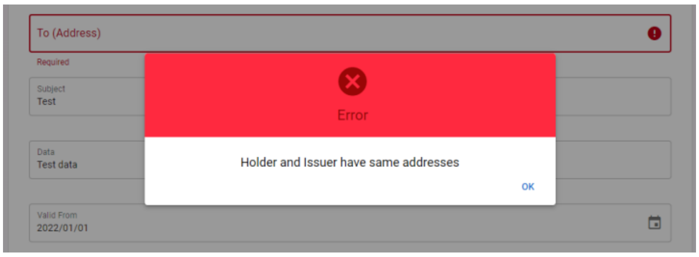
Subject
Driving License

Data
This VC is issued for holder

Valid From
2021/12/31

Valid To
2023/01/18

Caution : if the issuer and the holder have the same addresses or expiration date is earlier or equal to the issuance date, the following error dialogs would apper.



To (Address)

Required

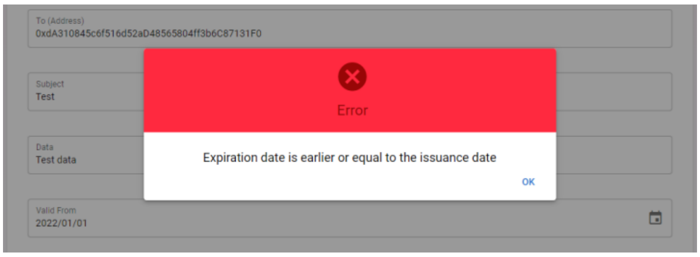
Subject
Test

Data
Test data

Valid From
2022/01/01

Error

Holder and Issuer have same addresses



To (Address)
0xdA310845c6f516d52aD48565804ff3b6C87131F0

Subject
Test

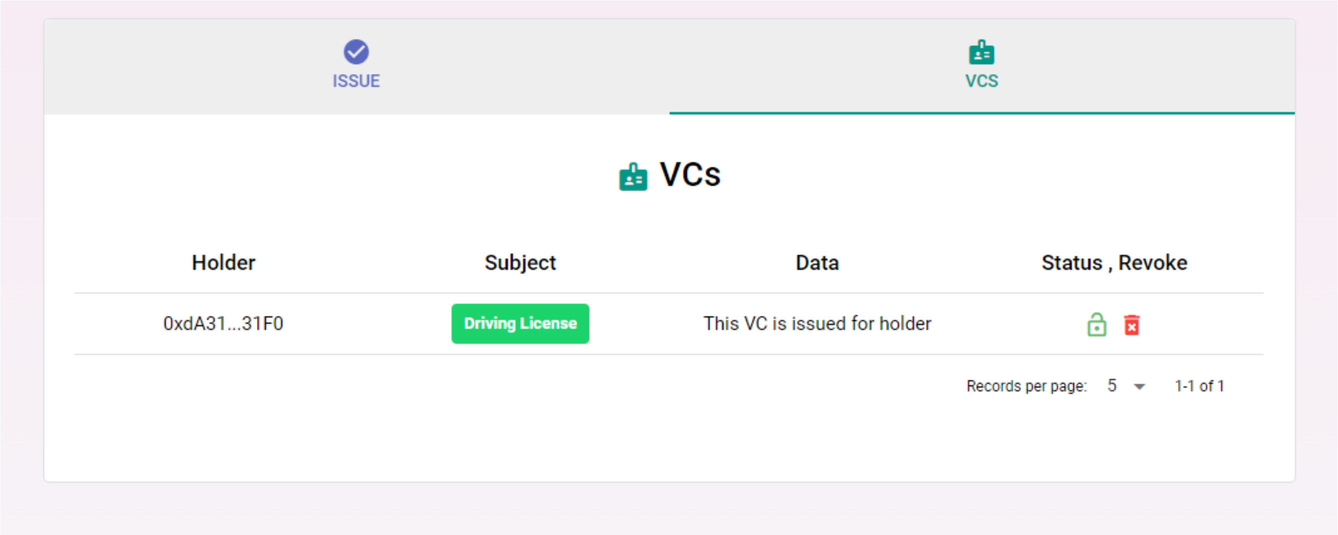
Data
Test data

Valid From
2022/01/01

Error

Expiration date is earlier or equal to the issuance date

When the transaction is confirmed, issuer can see the issued VC in "VCS" tab. All issued VCs are shown in that tab.

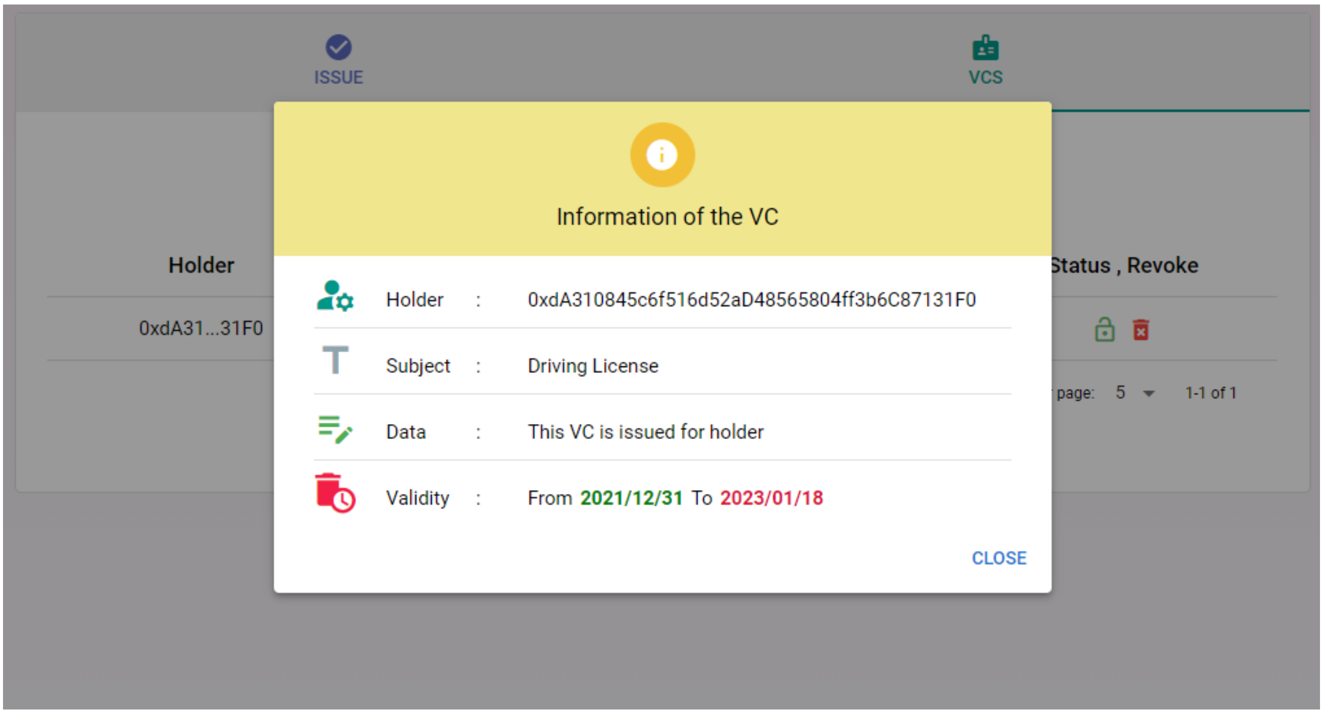


VCs

Holder	Subject	Data	Status , Revoke
0xdA31...31F0	Driving License	This VC is issued for holder	🔓 🗑

Records per page: 5 1-1 of 1

In each row, general information of each VC is shown briefly. However, by clicking on each row full information of that VC would be displayed in a dialog



Information of the VC

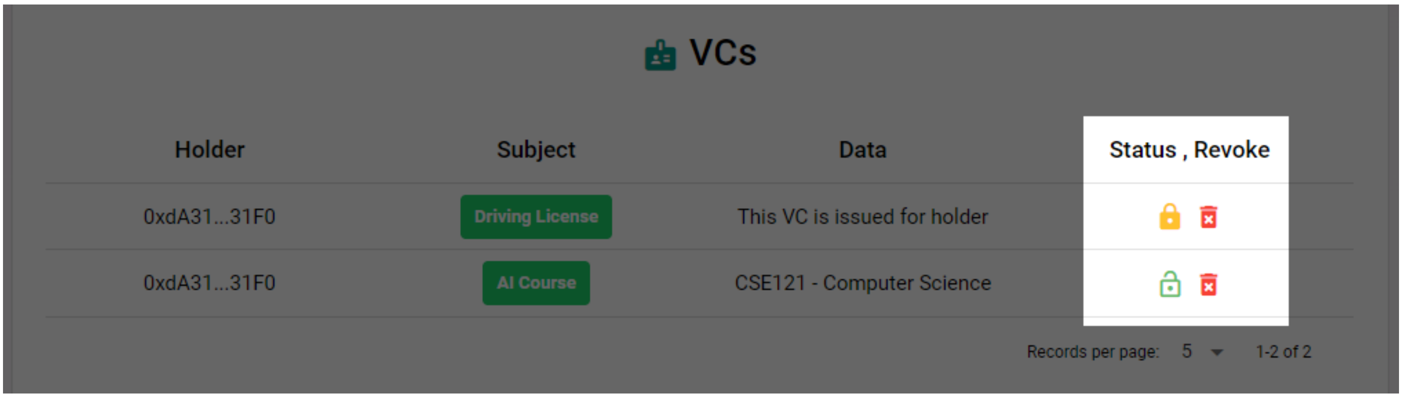
Holder : 0xdA310845c6f516d52aD48565804ff3b6C87131F0

Subject : Driving License

Data : This VC is issued for holder

Validity : From 2021/12/31 To 2023/01/18

In each row, you can see a column named "Status, Revoke".

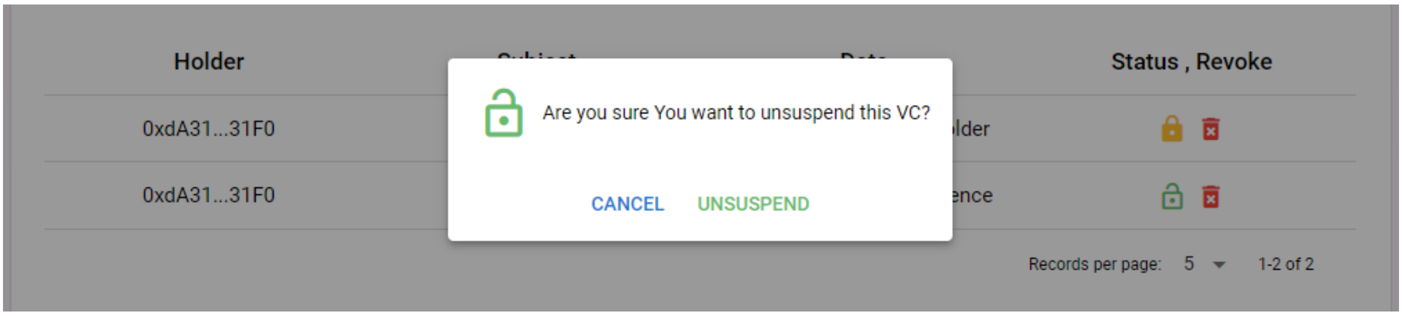


VCs

Holder	Subject	Data	Status , Revoke
0xdA31...31F0	Driving License	This VC is issued for holder	🔒 🗑
0xdA31...31F0	AI Course	CSE121 - Computer Science	🔓 🗑

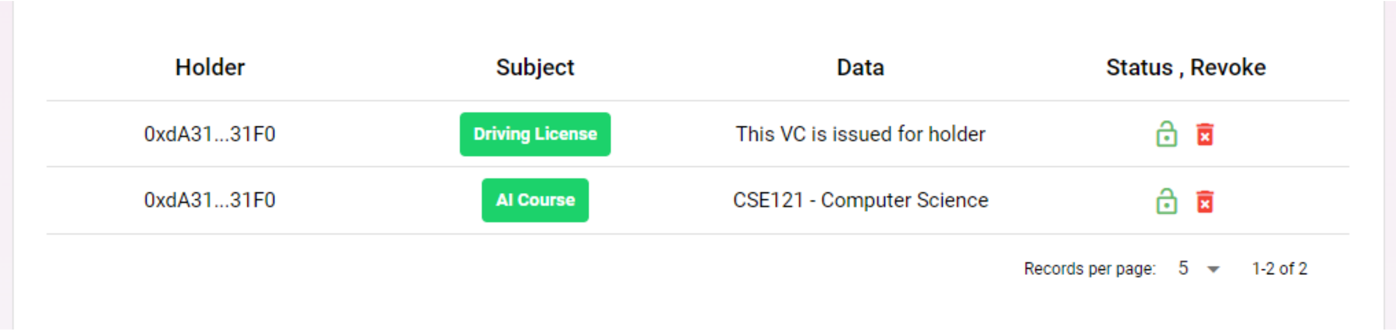
If a VC is suspended, its status is shown like 🔒, although if a VC is unsuspended, its status is shown like 🔓.

By clicking on the "lock" icon in a suspended VC, a dialog like below would be turned up and you can unsuspend that VC.



Are you sure You want to unsuspend this VC?

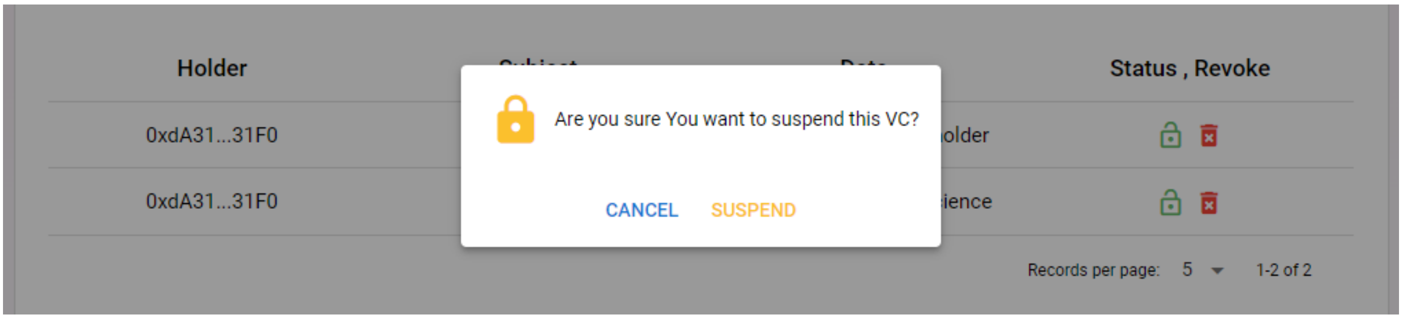
Result :



Holder	Subject	Data	Status , Revoke
0xdA31...31F0	Driving License	This VC is issued for holder	🔓 🗑
0xdA31...31F0	AI Course	CSE121 - Computer Science	🔓 🗑

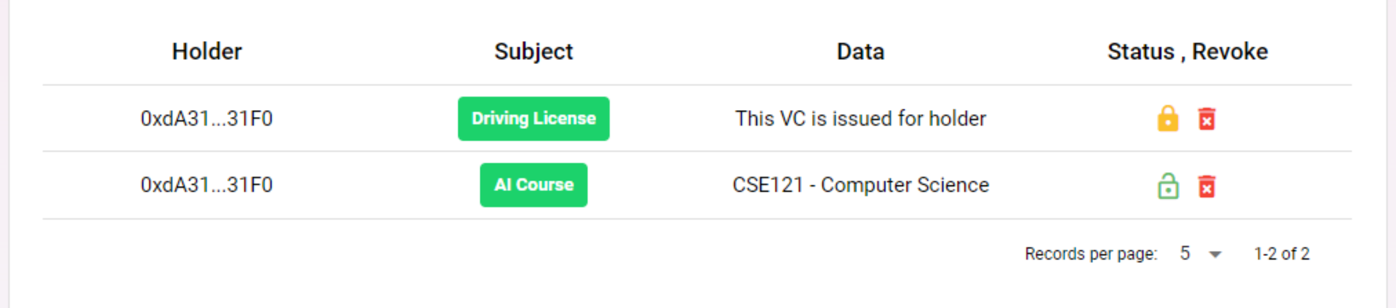
Note that you have to confirm the transaction in MetaMask to suspend or unsuspend a VC.

By clicking on the "opened lock" icon in a unsuspended VC, a dialog like below would be turned up and you can suspend that VC.



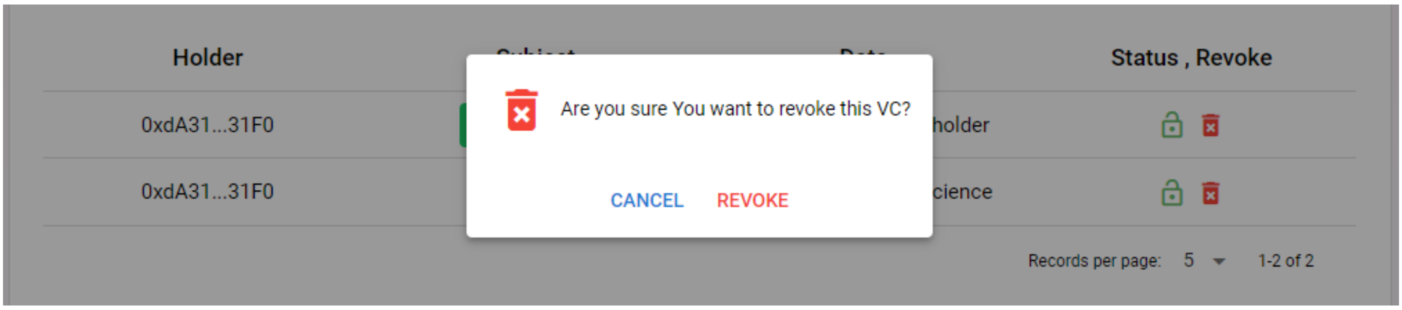
Are you sure You want to suspend this VC?

Result :



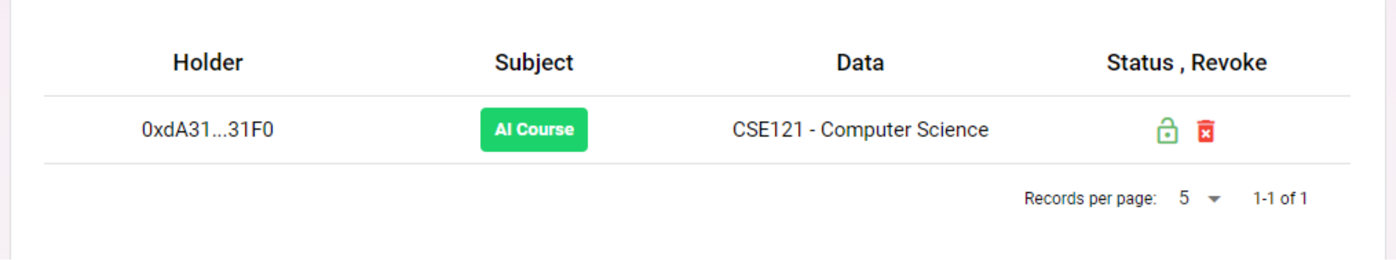
Holder	Subject	Data	Status , Revoke
0xdA31...31F0	Driving License	This VC is issued for holder	🔒 🗑
0xdA31...31F0	AI Course	CSE121 - Computer Science	🔓 🗑

Apart from "Status", you can see "Revoke" which means that you can revoke any issued VC as an issuer. By clicking on the "Trash Can" icon in each row, the following dialog would be shown and issuer can revoke the specified VC.



Are you sure You want to revoke this VC?

Result :



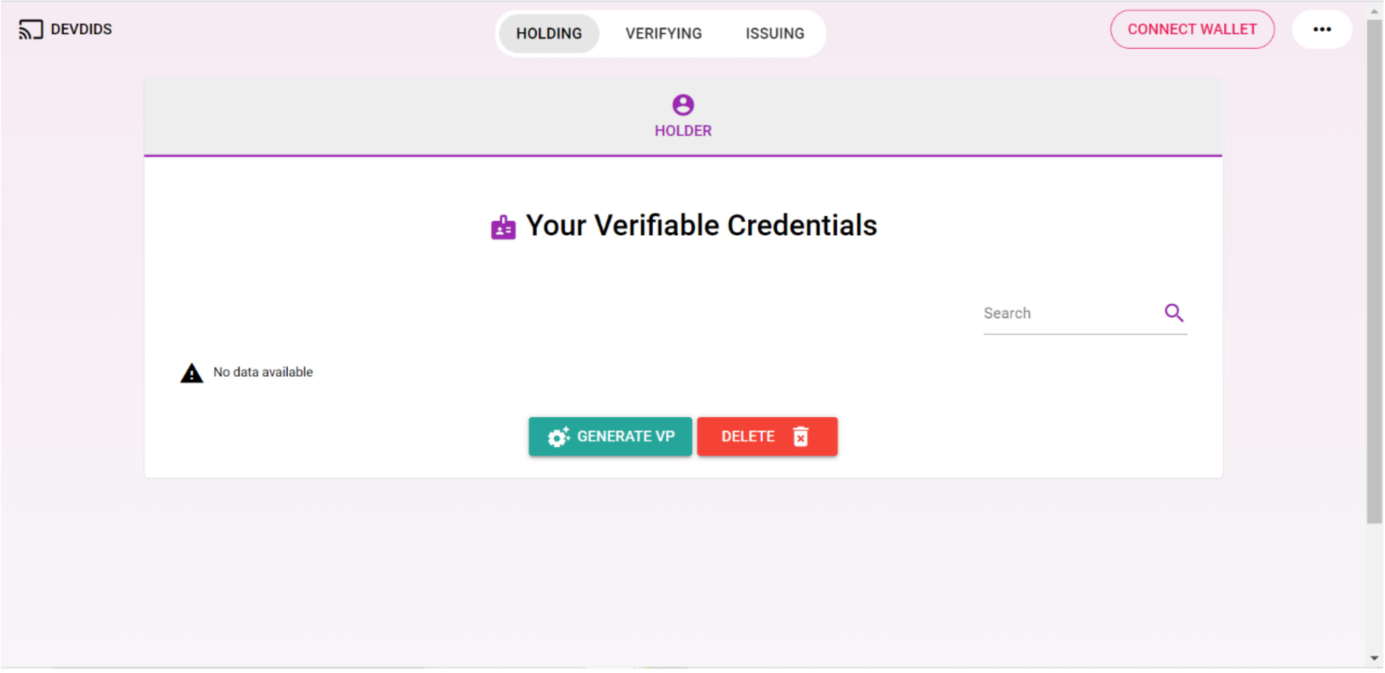
Holder	Subject	Data	Status , Revoke
0xdA31...31F0	AI Course	CSE121 - Computer Science	🔓 🗑

Note that you have to confirm the transaction in MetaMask to revoke a VC.

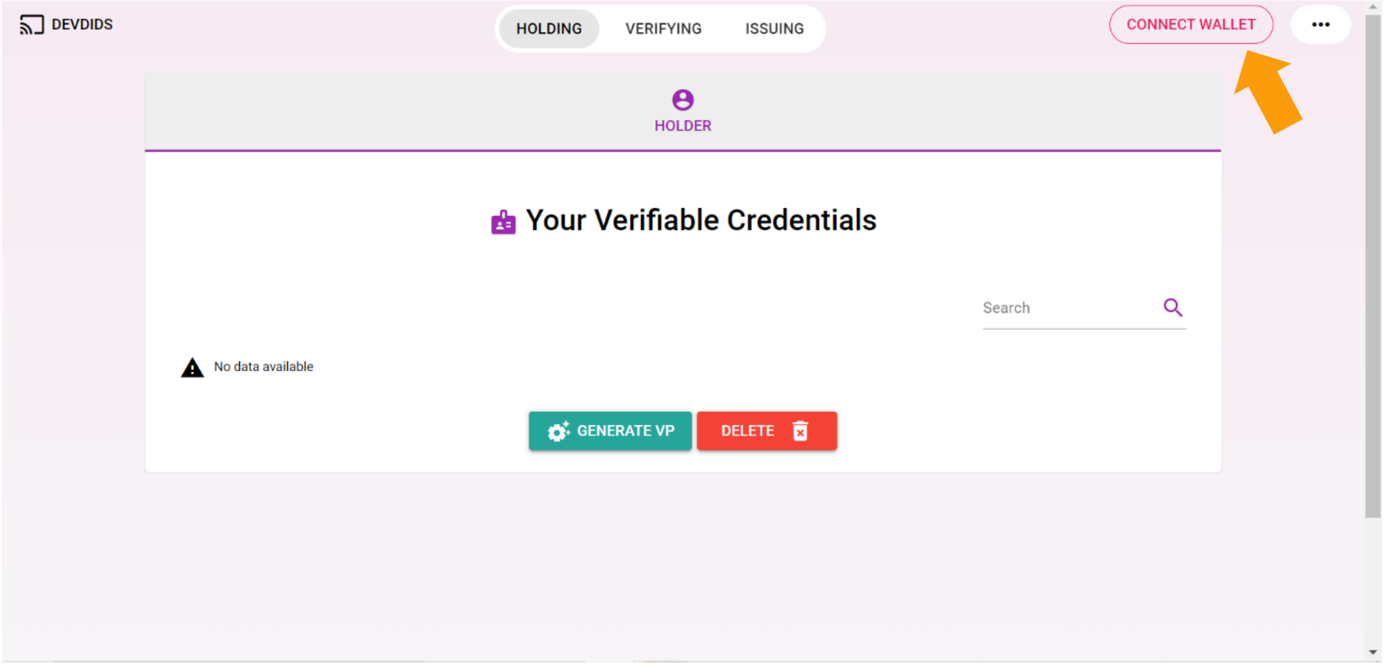
Holder

- Holder is an entity possessing one or more verifiable credentials and generating presentations from them. Like students, customers, and employees

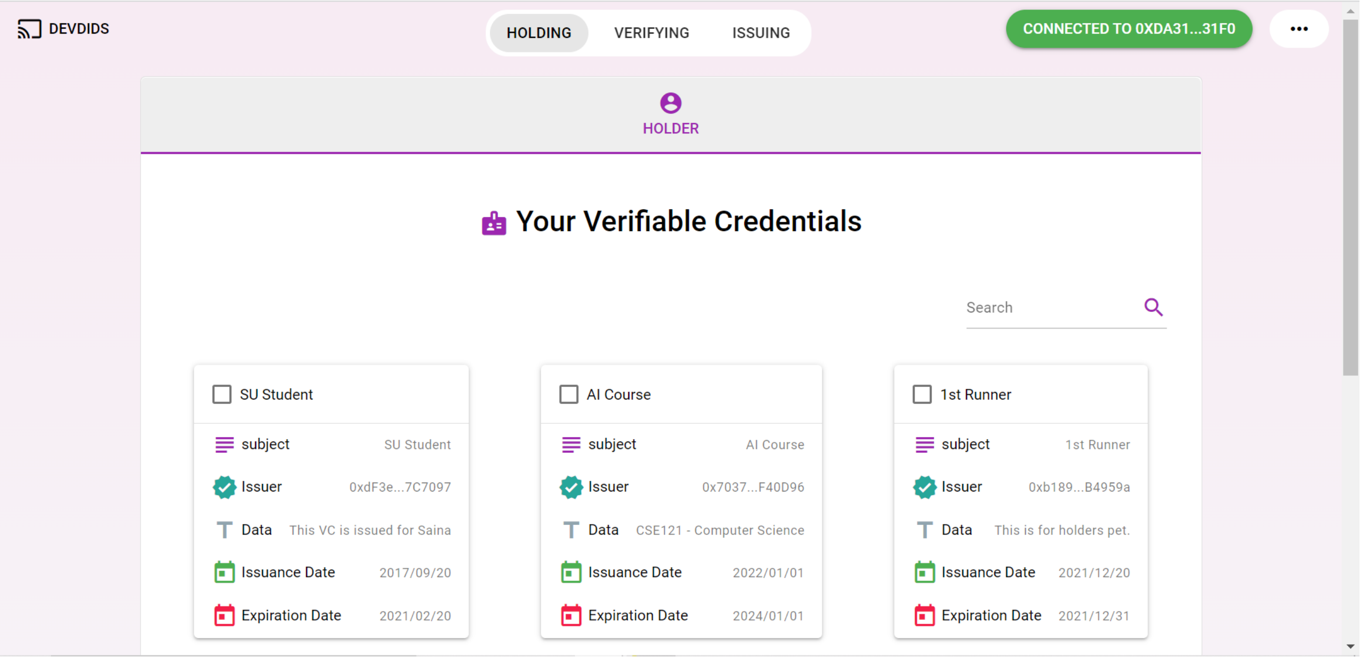
To access the holder page you have to head to https://dev-dids.netlify.app/holder. Firstly, this page looks like this :



Then you have to click on CONNECT WALLET to connect to your wallet.



And then you can see your verifiable credentials (VCs) :



Your Verifiable Credentials

□ SU Student

subject	SU Student
Issuer	0xdF3e...7C7097
Data	This VC is issued for Saina
Issuance Date	2017/09/20
Expiration Date	2021/02/20

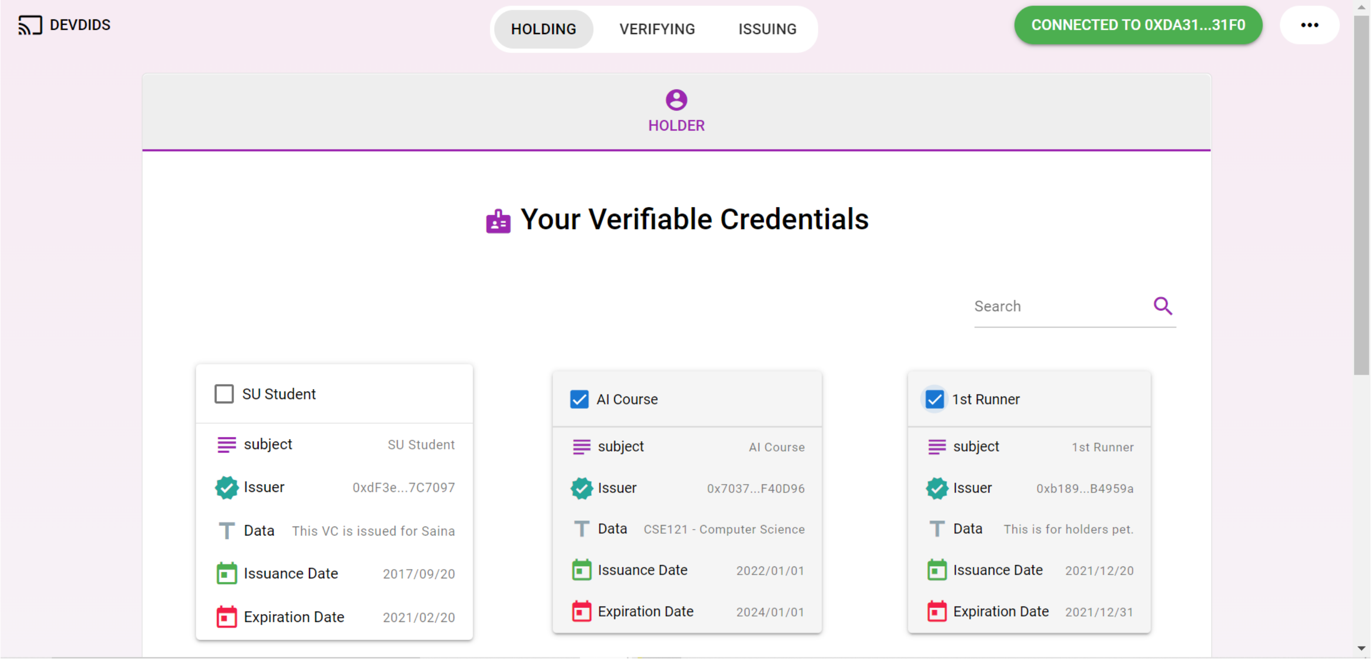
□ AI Course

subject	AI Course
Issuer	0x7037...F40D96
Data	CSE121 - Computer Science
Issuance Date	2022/01/01
Expiration Date	2024/01/01

□ 1st Runner

subject	1st Runner
Issuer	0xb189...B4959a
Data	This is for holders pet.
Issuance Date	2021/12/20
Expiration Date	2021/12/31

You can select as many verifiable credentials as you want by clicking on them :



Your Verifiable Credentials

□ SU Student

subject	SU Student
Issuer	0xdF3e...7C7097
Data	This VC is issued for Saina
Issuance Date	2017/09/20
Expiration Date	2021/02/20

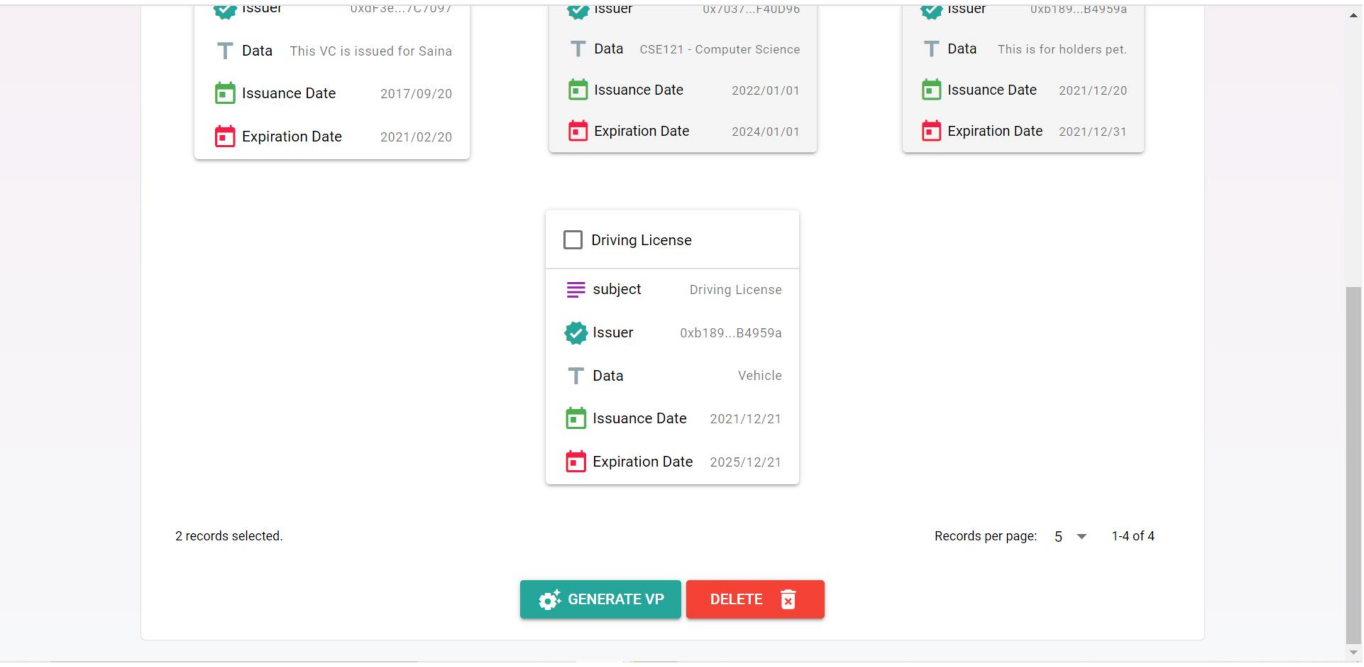
☑ AI Course

subject	AI Course
Issuer	0x7037...F40D96
Data	CSE121 - Computer Science
Issuance Date	2022/01/01
Expiration Date	2024/01/01

☑ 1st Runner

subject	1st Runner
Issuer	0xb189...B4959a
Data	This is for holders pet.
Issuance Date	2021/12/20
Expiration Date	2021/12/31

Then you can delete them by clicking on delete button :



Issuer 0xdF3e...7C7097

Data This VC is issued for Saina

Issuance Date 2017/09/20

Expiration Date 2021/02/20

Issuer 0x7037...F40D96

Data CSE121 - Computer Science

Issuance Date 2022/01/01

Expiration Date 2024/01/01

Issuer 0xb189...B4959a

Data This is for holders pet.

Issuance Date 2021/12/20

Expiration Date 2021/12/31

☐ Driving License

subject Driving License

Issuer 0xb189...B4959a

Data Vehicle

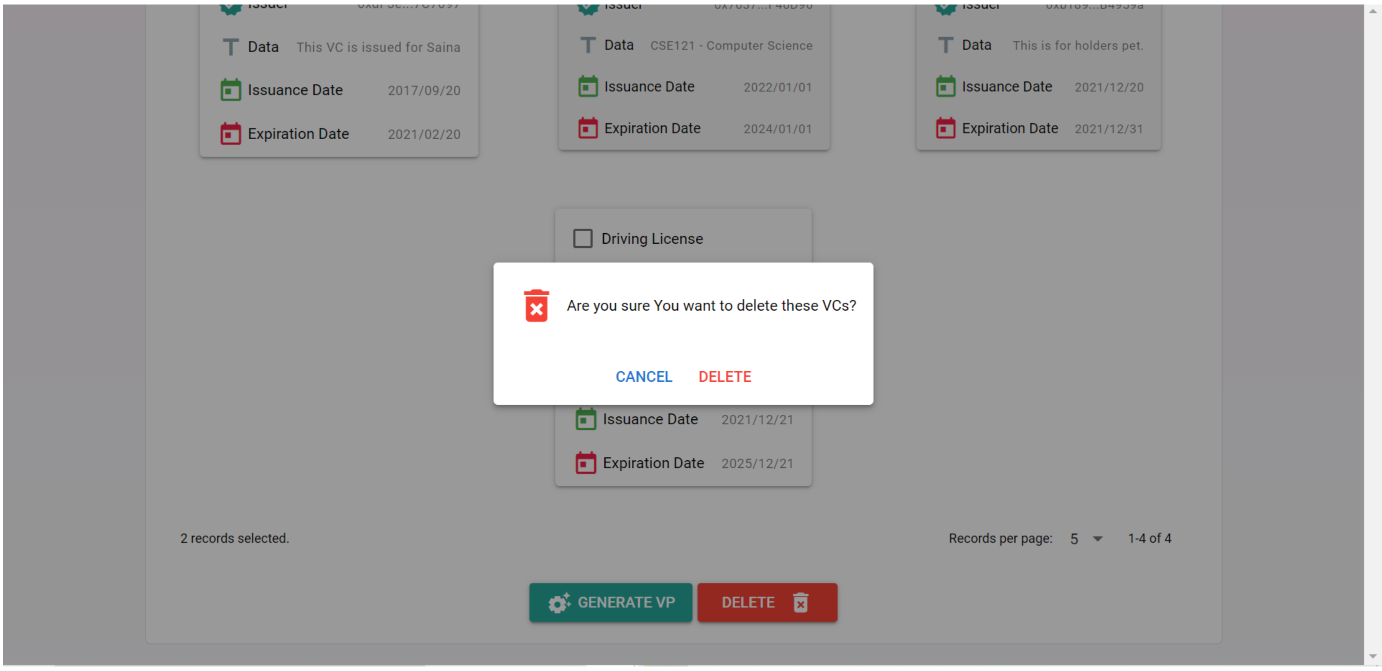
Issuance Date 2021/12/21

Expiration Date 2025/12/21

2 records selected.

Records per page: 5 1-4 of 4

Then a dialog appears on the page asking if you want to delete or cancel the process of deleting those VCs :



Issuer 0xdF3e...7C7097

Data This VC is issued for Saina

Issuance Date 2017/09/20

Expiration Date 2021/02/20

Issuer 0x7037...F40D96

Data CSE121 - Computer Science

Issuance Date 2022/01/01

Expiration Date 2024/01/01

Issuer 0xb189...B4959a

Data This is for holders pet.

Issuance Date 2021/12/20

Expiration Date 2021/12/31

☐ Driving License

Are you sure You want to delete these VCs?

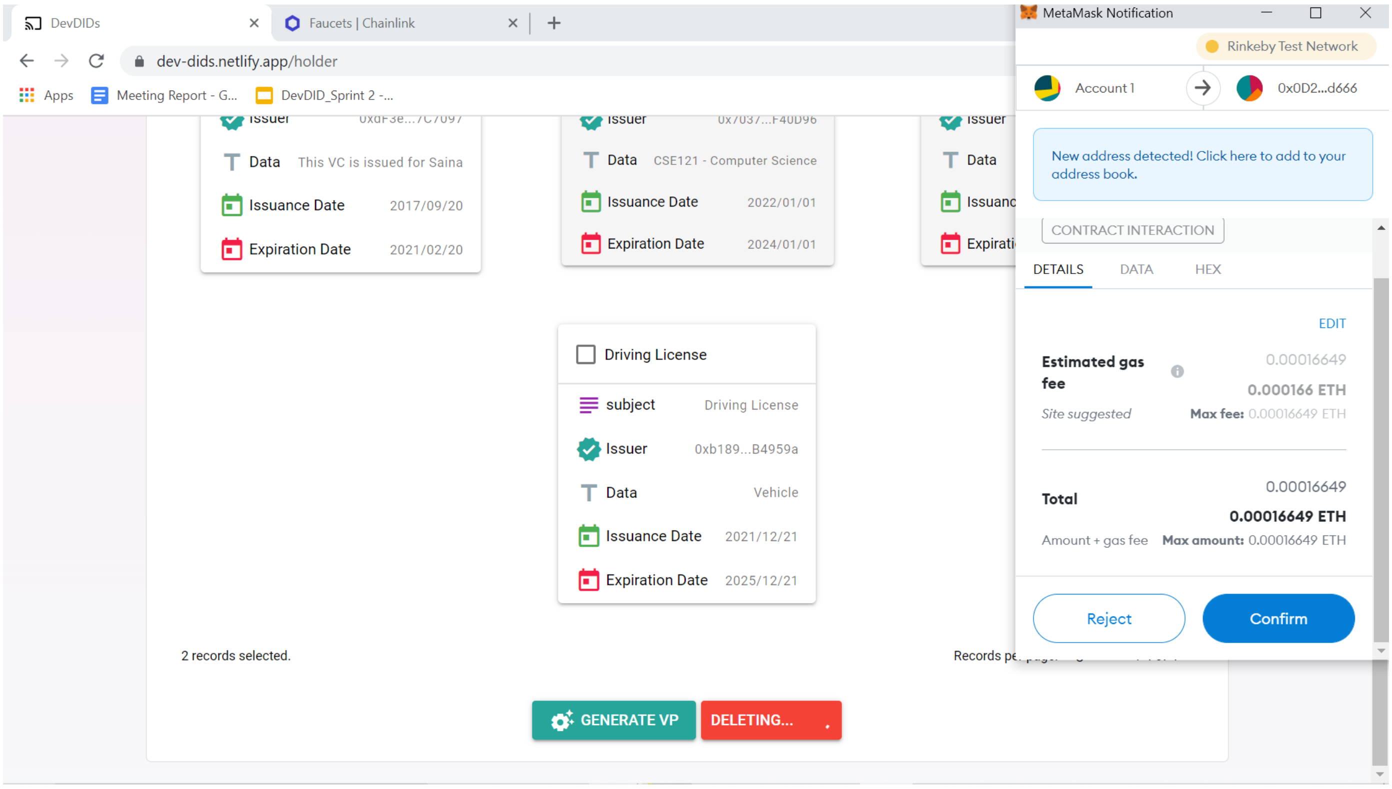
Issuance Date 2021/12/21

Expiration Date 2025/12/21

2 records selected.

Records per page: 5 1-4 of 4

If you click on CANCEL the process will be canceled and the selected VCs remain, but if you click on DELETE, MetaMask wants you to confirm the process :



Issuer	0xaF3e...7C7097
Data	This VC is issued for Saina
Issuance Date	2017/09/20
Expiration Date	2021/02/20

Issuer	0x7037...F40D96
Data	CSE121 - Computer Science
Issuance Date	2022/01/01
Expiration Date	2024/01/01

☐ Driving License

subject	Driving License
Issuer	0xb189...B4959a
Data	Vehicle
Issuance Date	2021/12/21
Expiration Date	2025/12/21

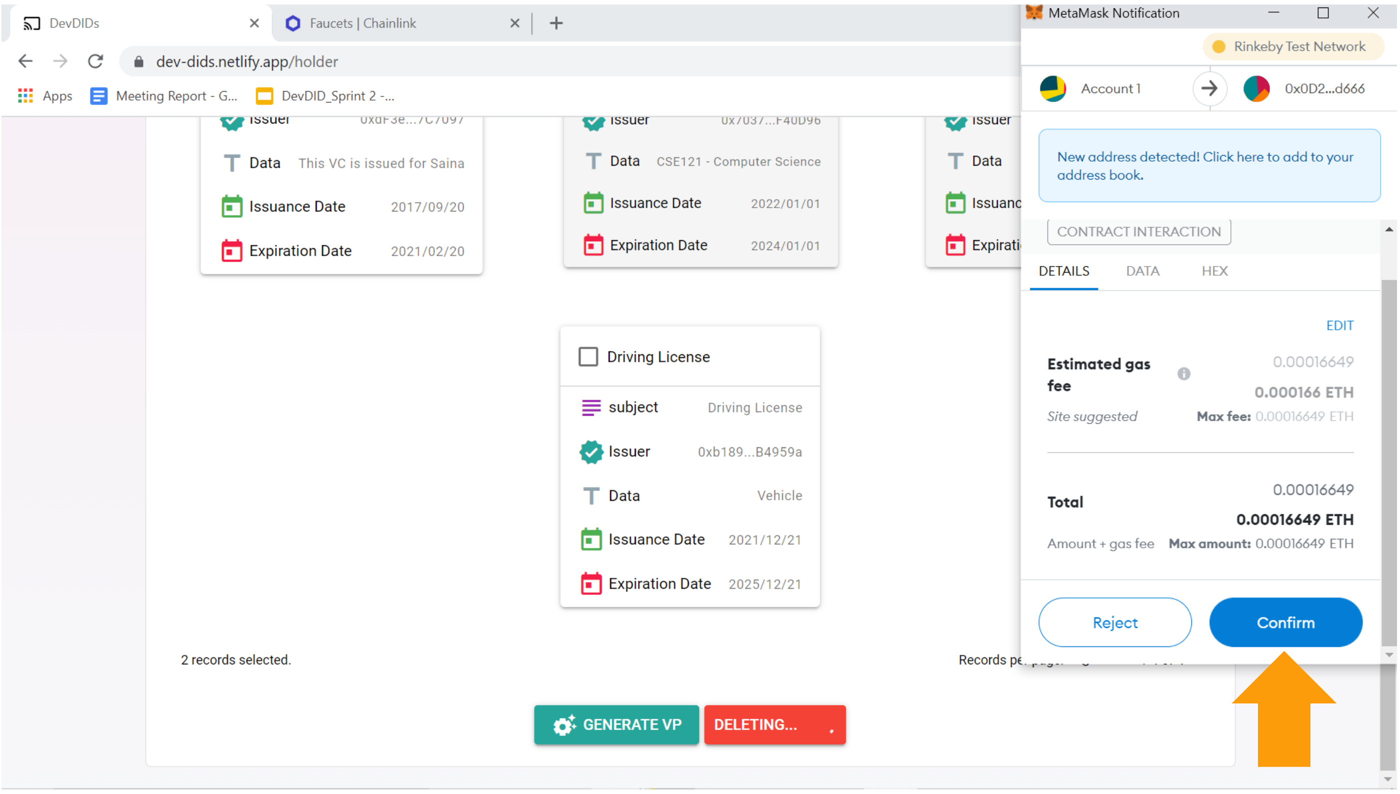
2 records selected.

New address detected! Click here to add to your address book.

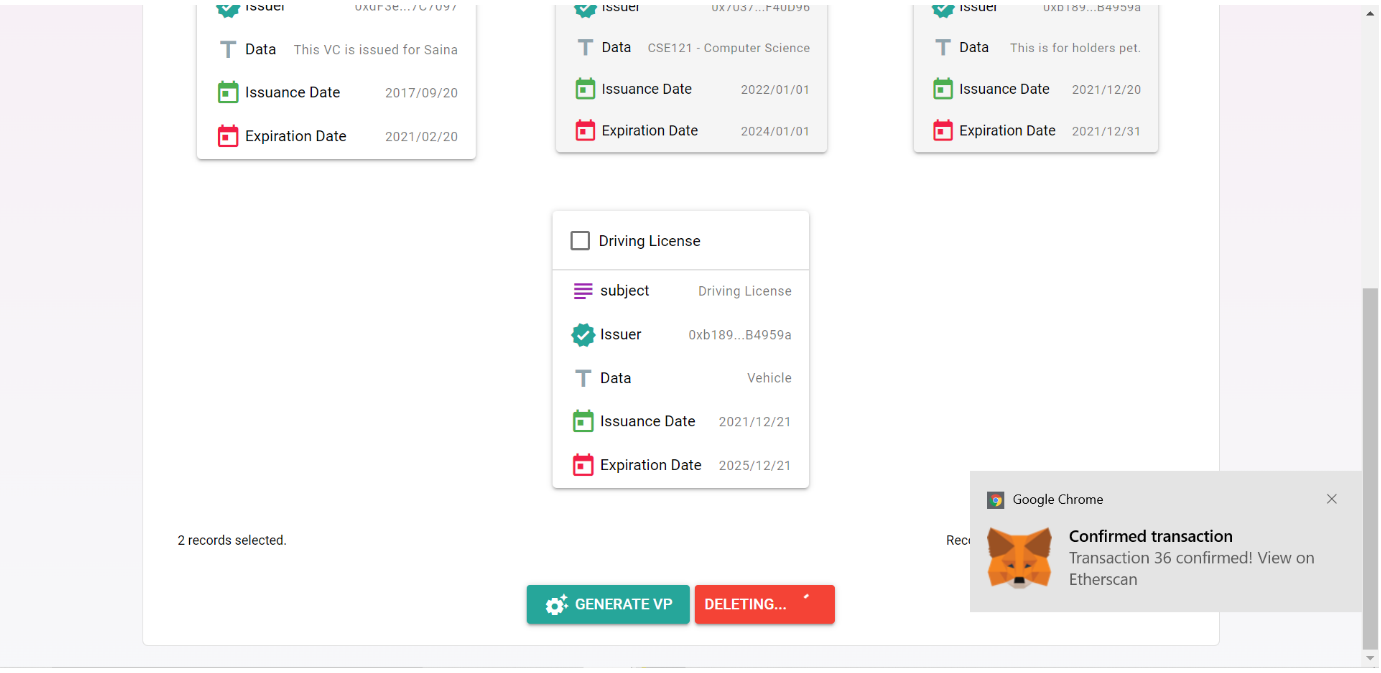
Estimated gas fee	0.00016649 0.000166 ETH
Site suggested	**Max fee:** 0.00016649 ETH
Total	0.00016649 **0.00016649 ETH**
Amount + gas fee	**Max amount:** 0.00016649 ETH

By clicking on Reject Button the process will be canceled.

But if you click on Confirm Button as below, the selected VCs will be deleted.


DevDIDs
Faucets | Chainlink
dev-dids.netlify.app/holder
Apps
Meeting Report - G...
DevDID_Sprint 2 -...
Issuer 0xaF3e...7C7097
Data This VC is issued for Saina
Issuance Date 2017/09/20
Expiration Date 2021/02/20
Issuer 0x7037...F40D96
Data CSE121 - Computer Science
Issuance Date 2022/01/01
Expiration Date 2024/01/01
☐ Driving License
subject Driving License
Issuer 0xb189...B4959a
Data Vehicle
Issuance Date 2021/12/21
Expiration Date 2025/12/21
2 records selected.
GENERATE VP
DELETING...
MetaMask Notification
Rinkeby Test Network
Account 1
0x0D2...d666
New address detected! Click here to add to your address book.
CONTRACT INTERACTION
DETAILS DATA HEX
EDIT
Estimated gas fee 0.00016649 0.000166 ETH
Site suggested Max fee: 0.00016649 ETH
Total 0.00016649 0.00016649 ETH
Amount + gas fee Max amount: 0.00016649 ETH
Reject
Confirm

As soon as the notification of the confirmed process appears and the loading of the delete button stops, the selected VCs will be deleted:



Issuer 0xdF3e...7C7097
Data This VC is issued for Saina
Issuance Date 2017/09/20
Expiration Date 2021/02/20

Issuer 0x7037...F40D96
Data CSE121 - Computer Science
Issuance Date 2022/01/01
Expiration Date 2024/01/01

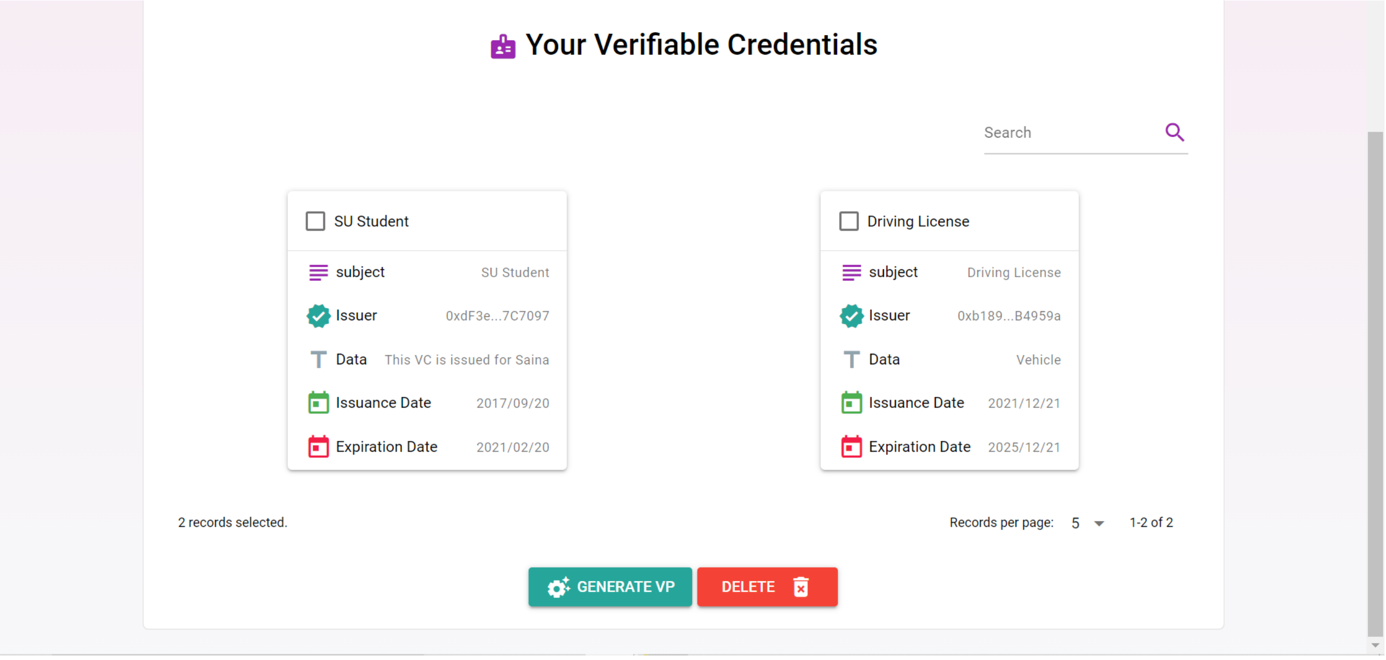
Issuer 0xb189...B4959a
Data This is for holders pet.
Issuance Date 2021/12/20
Expiration Date 2021/12/31

□ Driving License
subject Driving License
Issuer 0xb189...B4959a
Data Vehicle
Issuance Date 2021/12/21
Expiration Date 2025/12/21

2 records selected.

Google Chrome
Confirmed transaction
Transaction 36 confirmed! View on Etherscan

Result :



Your Verifiable Credentials

□ SU Student
subject SU Student
Issuer 0xdF3e...7C7097
Data This VC is issued for Saina
Issuance Date 2017/09/20
Expiration Date 2021/02/20

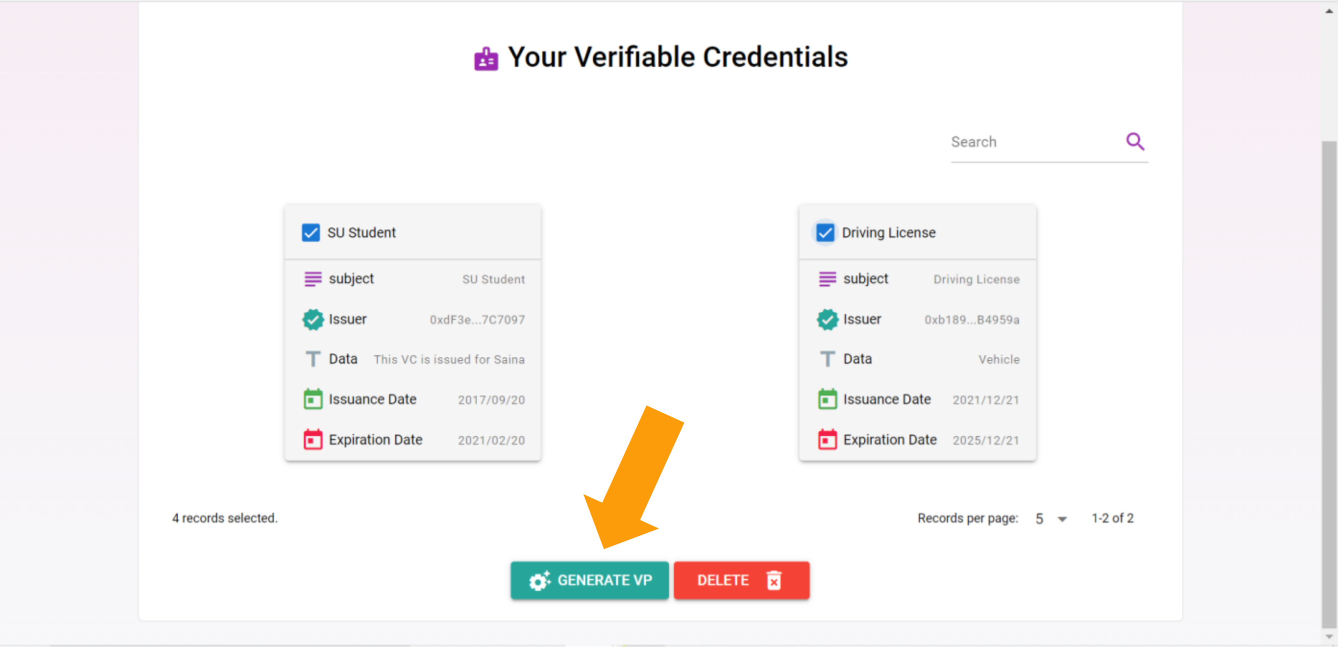
□ Driving License
subject Driving License
Issuer 0xb189...B4959a
Data Vehicle
Issuance Date 2021/12/21
Expiration Date 2025/12/21

2 records selected.

Records per page: 5 1-2 of 2

It is important to note that if you have selected more than one VC (n VCs) to be deleted, you have to confirm the transaction n times.

In order to give your VCs to verifier you can select some or all of them and then click on GENERATE VP:



Your Verifiable Credentials

Search

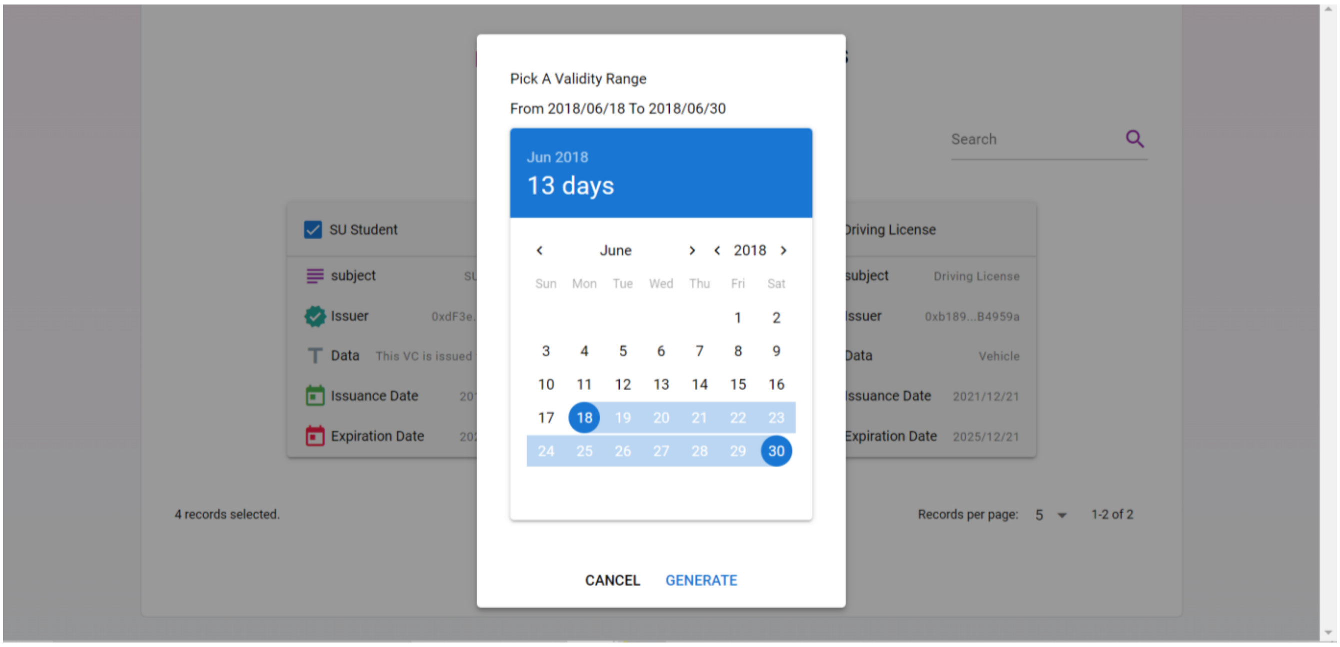
☑ SU Student	
subject	SU Student
Issuer	0xdF3e...7C7097
Data	This VC is issued for Saina
Issuance Date	2017/09/20
Expiration Date	2021/02/20

☑ Driving License	
subject	Driving License
Issuer	0xb189...B4959a
Data	Vehicle
Issuance Date	2021/12/21
Expiration Date	2025/12/21

4 records selected.

Records per page: 5 1-2 of 2

After that you have to pick a validity range for your new VP: (the start of this range should be more than the maximum of start date of all selected VCs and the end of that should be less than the minimum of end date of all selected VCs)



Pick A Validity Range

From 2018/06/18 To 2018/06/30

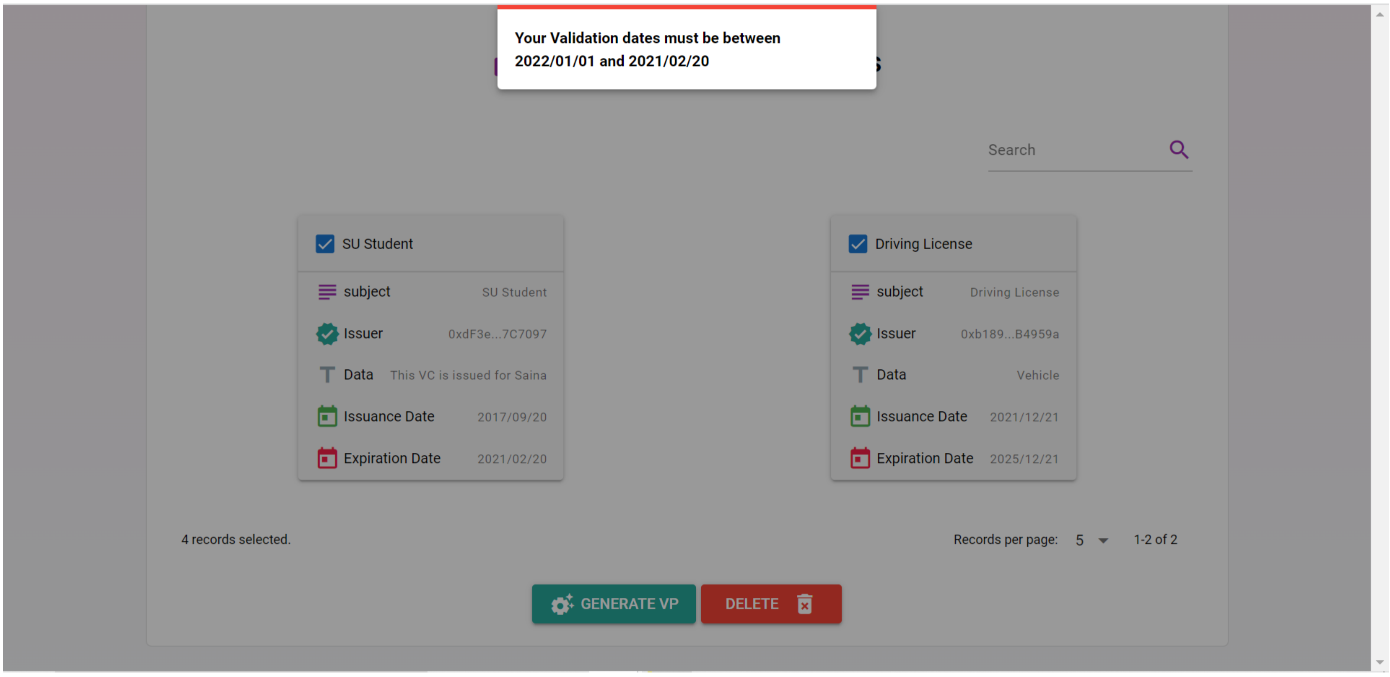
Jun 2018

13 days

June 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					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

If you do not follow the above rule you cannot generate VP:



Your Validation dates must be between 2022/01/01 and 2021/02/20

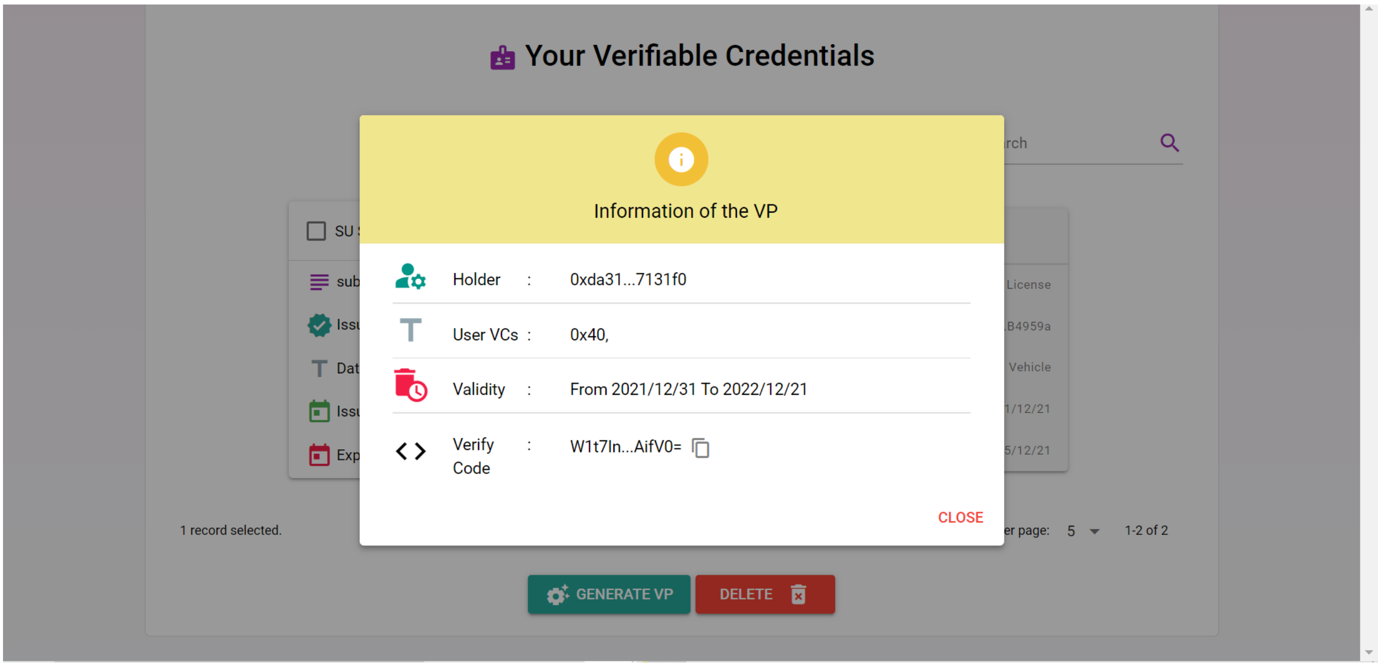
☑ SU Student	
subject	SU Student
Issuer	0xdF3e...7C7097
Data	This VC is issued for Saina
Issuance Date	2017/09/20
Expiration Date	2021/02/20

☑ Driving License	
subject	Driving License
Issuer	0xb189...B4959a
Data	Vehicle
Issuance Date	2021/12/21
Expiration Date	2025/12/21

4 records selected.

Records per page: 5 1-2 of 2

But if you follow it, the VP will be generated



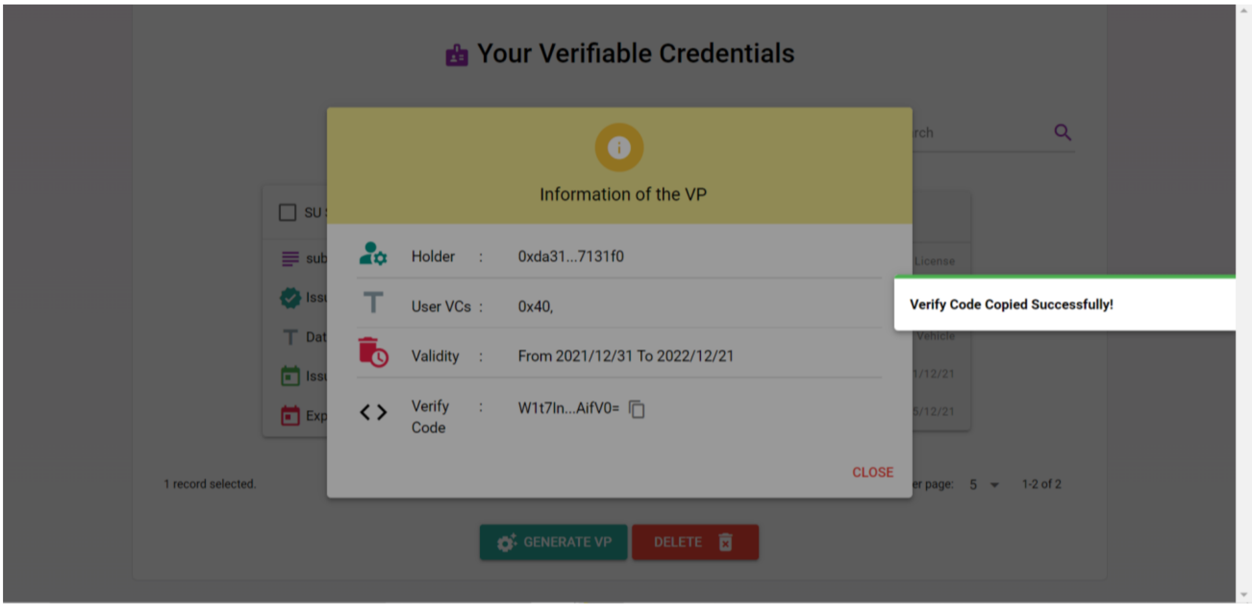
Your Verifiable Credentials

Information of the VP

Holder :	0xda31...7131f0
User VCs :	0x40,
Validity :	From 2021/12/31 To 2022/12/21
Verify Code :	W1t7In...AifV0=

1 record selected.

By copying the code and giving it to the verifier, he can verify whether your VP is valid or not.



Information of the VP

Holder : 0xda31...7131f0

User VCs : 0x40,

Validity : From 2021/12/31 To 2022/12/21

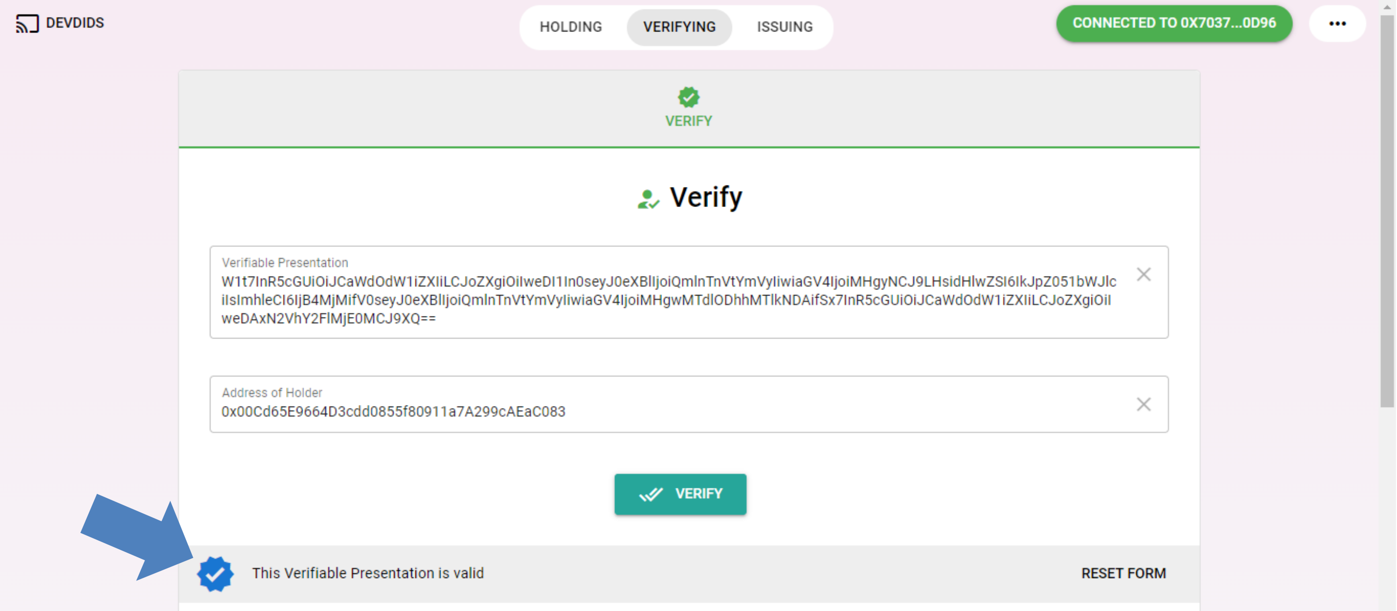
Verify Code : W1t7In...AifV0=

Verify Code Copied Successfully!

Verifier

- Verifier an entity requesting and receiving a verifiable presentation that proves the holder possesses the required verifiable credentials with certain characteristics.

In order to verify a VP, verifier has to get the VP code and holder's address from the holder. Then if the VP is verifiable this dialog will appear:



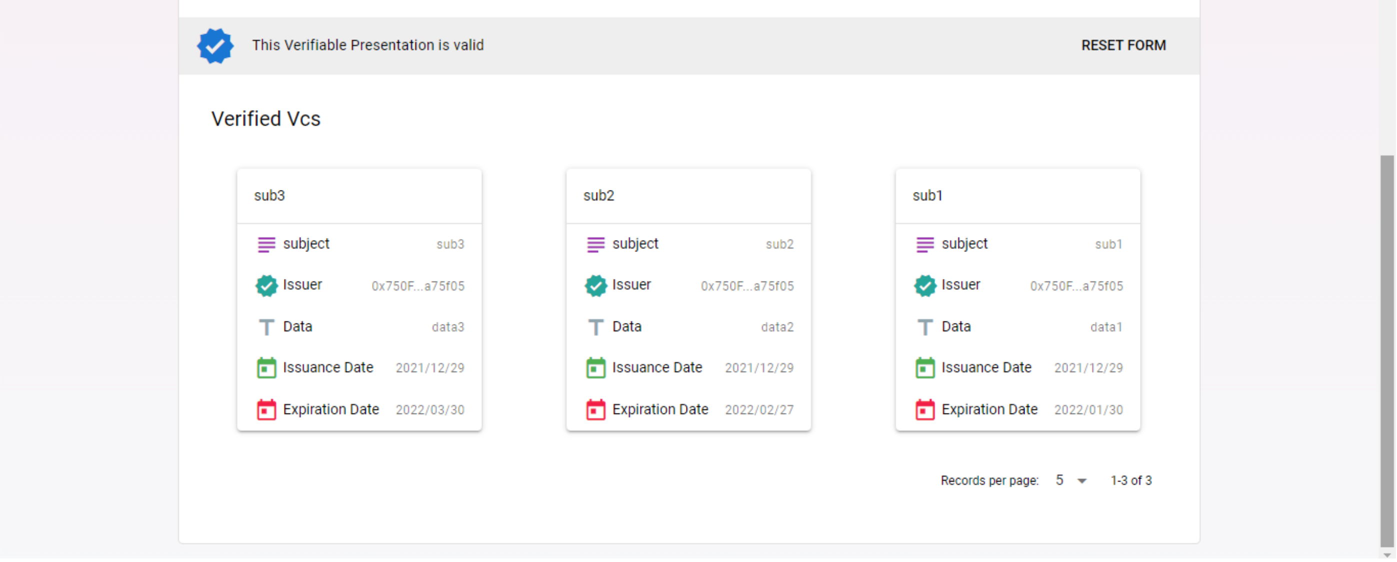
Verify

Verifiable Presentation
W1t7InR5cGUiOiJCaWdOdW1iZXIiLCJoZXgiOiIweDI1In0seyJ0eXBlIjoiQmlnTnVtYmVyIiwiaGV4IjoiMHgyNCJ9LHsidHlwZSI6IkJpZ051bWJlc
iIsImhleCI6IjB4MjMifV0seyJ0eXBlIjoiQmlnTnVtYmVyIiwiaGV4IjoiMHgwMTdlODhhMTlkNDAifSx7InR5cGUiOiJCaWdOdW1iZXIiLCJoZXgiOiI
weDAxN2VhY2FlMjE0MCJ9XQ==

Address of Holder
0x00Cd65E9664D3cdd0855f80911a7A299cAEaC083

This Verifiable Presentation is valid

In addition, verifier can see the list of verified credentials in that verified VP:



This Verifiable Presentation is valid

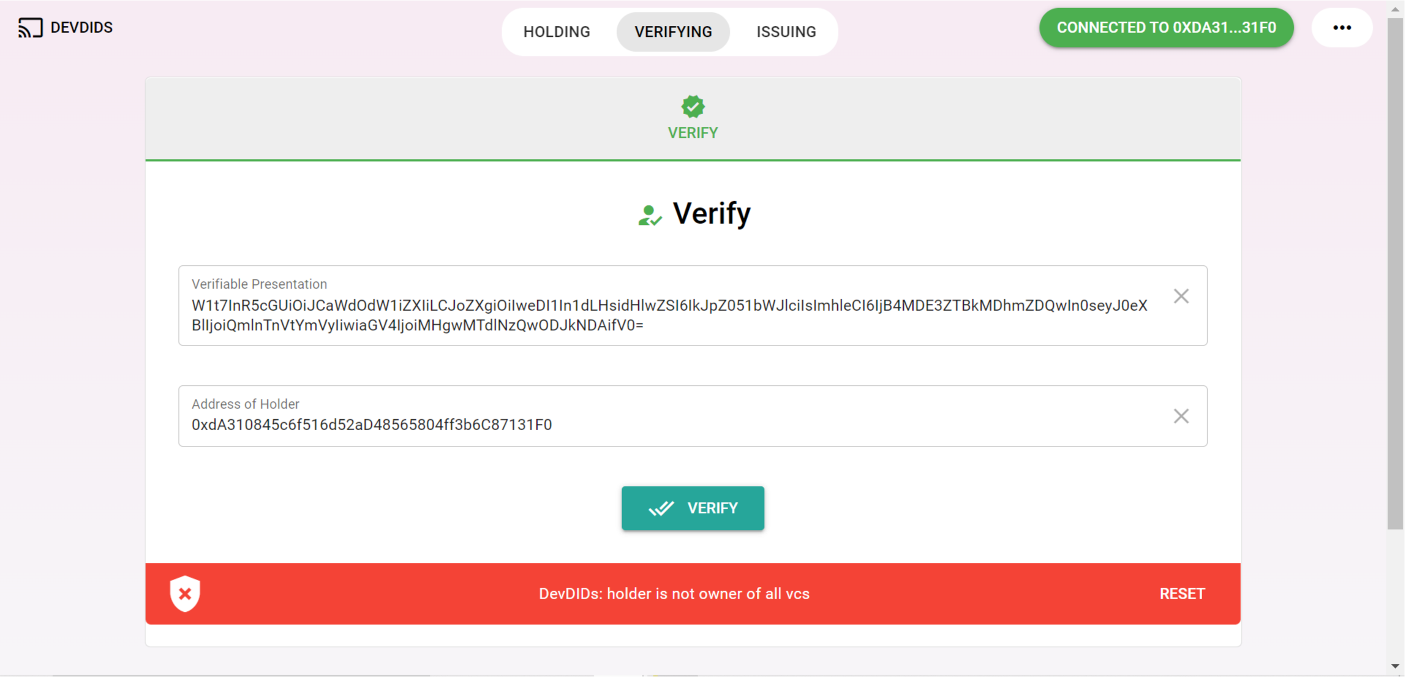
Verified Vcs

sub3	
subject	sub3
Issuer	0x750F...a75f05
Data	data3
Issuance Date	2021/12/29
Expiration Date	2022/03/30

sub2	
subject	sub2
Issuer	0x750F...a75f05
Data	data2
Issuance Date	2021/12/29
Expiration Date	2022/02/27

sub1	
subject	sub1
Issuer	0x750F...a75f05
Data	data1
Issuance Date	2021/12/29
Expiration Date	2022/01/30

Otherwise a red dialog with the reason of invalidity appears:



Verify

Verifiable Presentation
W1t7InR5cGUiOiJCaWdOdW1iZXIiLCJoZXgiOiIweDI1In1dLHsidHlwZSI6IkJpZ051bWJlciIsImhleCI6IjB4MDE3ZTBkMDhmZDQwIn0seyJ0eXBlIjoiQmlnTnVtYmVyIiwiaGV4IjoiMHgwMTdlNzQwODJkNDAifV0=

Address of Holder
0xdA310845c6f516d52aD48565804ff3b6C87131F0

DevDIDs: holder is not owner of all vcs