Riddle & Code

LIBRDDL SDK

Table of Contents

Table of Figures

1 DESCRIPTION

This document includes usage method, software architecture and test results of RDDL SDK.
< What is RDDL SDK? Purpose of RDDL SDK>
< Mention libRDDL repo >
< Mention Planetmint and Liquid>

2 SOFTWARE ARCHITECTURE

Figure 1 indicates library structure. The library consists of 3 layers:

- rddlSDKAPI: This layer includes user functions.
- rddlSDKAbst: This layer includes hardware specific functions
- libRddl: This layer includes common software function which are platform independent.

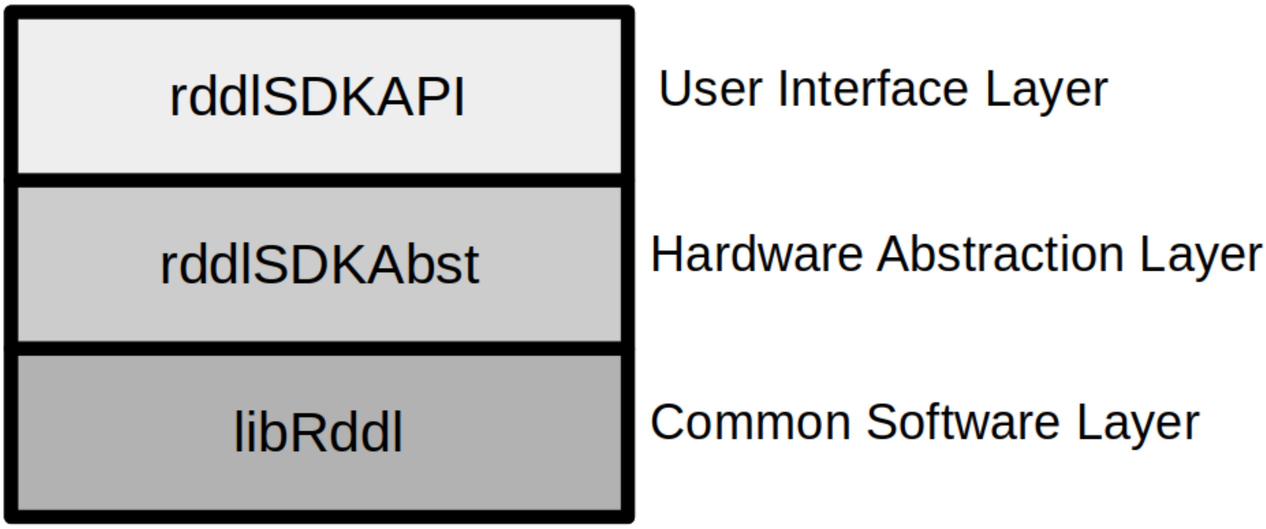


Figure 1: General System Overview

2.1 API FUNCTIONS

void runRDDLSDKNotarizationWorkflow(const char* data_str, size_t data_length): This function has two separate tasks. If the seed in the device is registered to the network, it creates a transaction using the given data and broadcasts it. If the seed in the device is not registered to the network, it creates a registration transaction and broadcasts it. Figure 2 gives flowchart of this function.

The getPlntmntKeys function prepares public and private keys to be used in other functions. It generates the master key from the seed stored in the device. It generates planetmint keys from masterkey with the following derivation path /44'/8680'/0'/0/0 and liquid keys from /44'/1776'/0'/0/0. It also derives the public key from the private key embedded in the machine.

The hasMachineBeenAttested function checks whether the device has been registered before by querying *https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key*. It uses the planetmint external public key for the query which is serialized of planetmint node with PLANETMINT_PMP version.

The registerMachine function creates a message in the google protobuf structure containing machine information. This machine information includes the generated public keys, the machine's domain and device information.

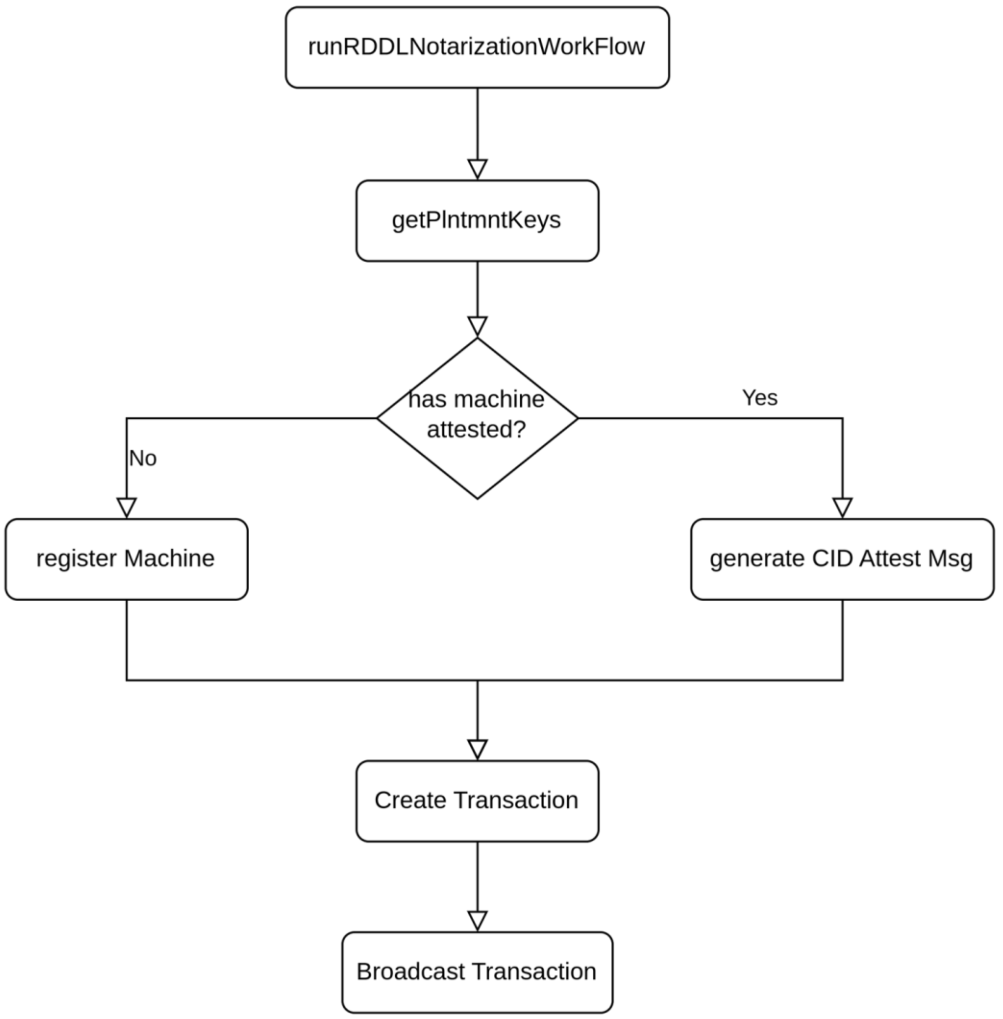


Figure 2: flowchart of runRDLLNotarizationWorkflow function

The create transaction function prepares the transaction using the generated message in the google protobuf structure, planetmint keys, denom, sequence, chain id and account id. Denom and chain-id information are retrieved from the device. If it is not saved in the device, default values are used which are plmnt and planetmint-testnet-1 respectively. Sequence and account id information is retrieved by querying *https://testnet-api.rddl.io/cosmos/auth/v1beta1/account_info/*. The hash160 version of the planetmint public key is used for this query. If the query returns negative, information is retrieved from the device. If it is not saved in the device, default values are used which are 0.

Finally, broadcast transaction function sends the created transaction to *https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs* address.

char* sdkSetSeed (**char*** pMnemonic, **size_t** len): Generates seed for the device from the given mnemonic. If a mnemonic is not given, it generates itself. Returns the used mnemonic.

void sdkStoreSeed **(char*** **new_seed)**: Writes the seed to the non-volatile memory of the device. If new_seed is NULL, it writes the seed produced by sdkSetSeed function. If it is not NULL, it writes the value in new_seed.

void sdkReadSeed **(char*** **seed_arr, int*** **seed_size)**: Returns embedded seed value and it’s size. The size of seed is currently 64 bytes.

3 TESTS

Before starting the test, you need to change the TEST_SEED in testRDDLSDK.c. Otherwise, you will use a previously registered seed.

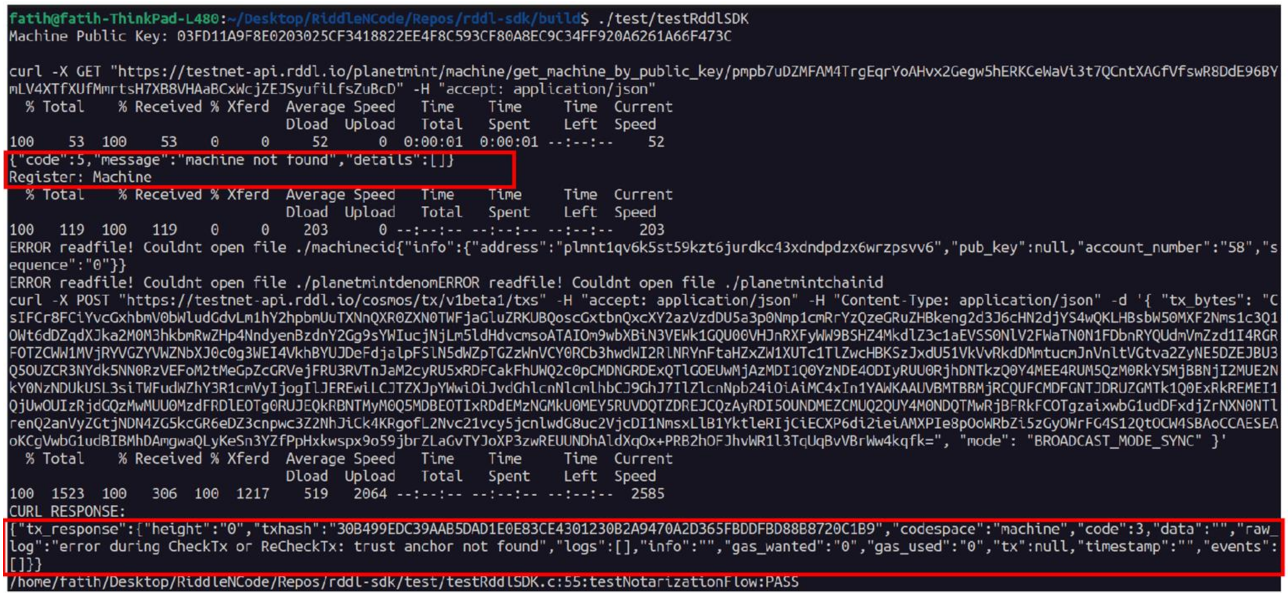
Compile library with following command on the project directory. It will also generate test executable.

```
bash build.sh
```

To run test code, use following command on the project directory:

```
bash runTest.sh
```

If the test device is not registered to the network, the following errors will be received when the test program is run.



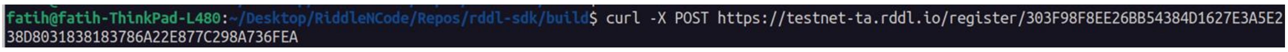
```
fatih@fatih-ThinkPad-L480:~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ ./test/testRddlSDK
Machine Public Key: 03FD11A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7uDZMFAM4TrgEqrYoAHvx2Gegw5hERKCeWaVi3t7QCntXAGfVfswR8DdE96BY
mLV4XTfXUfMmrtsH7XB8VHAaBCxWcjZEJSyufiLfsZuBcD" -H "accept: application/json"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    53  100    53    0     0     52      0  0:00:01  0:00:01 --:--:--    52
{"code":5,"message":"machine not found","details":[]}
Register: Machine
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   119  100   119    0     0    203      0 --:--:-- --:--:-- --:--:--   203
ERROR readfile! Couldnt open file ./machinecid{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":null,"account_number":"58","s
equence":"0"}}
ERROR readfile! Couldnt open file ./planetmintdenomERROR readfile! Couldnt open file ./planetmintchainid
curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{ "tx_bytes": "C
sIFCr8FCiYvcGxhbmV0bWludGdvLm1hY2hpbmUuTXNnQXR0ZXN0TWFjaGluZRKUBQoscGxtbnQxcXY2azVzdDU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2djYS4wQKLHBsbW50MXF2Nms1c3Q1
OWt6dDZqdXJka2M0M3hkbmRwZHp4NndyenBzdnY2Gg9sYWIucjNjLm5ldHdvcmsoATAIOm9wbXBiN3VEWk1GQU00VHJnRXFyWW9BSHZ4MkdlZ3c1aEVSS0NlV2FWaTN0N1FDbnRYQUdmVmZzd1I4RGR
FOTZCWW1MVjRYVGZYVWZNbXJ0c0g3WEI4VkhBYUJDeFdjalpFSlN5dWZpTGZzWnVCY0RCb3hwdWI2RlNRYnFtaHZxZW1XUTc1TlZwcHBKSzJxdU51VkVvRkdDMmtucmJnVnltVGtva2ZyNE5DZEJBU3
Q5OUZCR3NYdk5NN0RzVEFoM2tMeGpZcGRVejFRU3RVTnJaM2cyRU5xRDFCakFhUWQ2c0pCMDNGRDExQTlGOEUwMjAzMDI1Q0YzNDE4ODIyRUU0RjhDNTkzQ0Y4MEE4RUM5QzM0RkY5MjBBNjI2MUE2N
kY0NzNDUkUSL3siTWFudWZhY3R1cmVyIjogIlJEREwiLCJTZXJpYWwiOiJvdGhlcnNlcmlhbCJ9GhJ7IlZlcnNpb24iOiAiMC4xIn1YAWKAAUVBMTBBMjRCQUFCMDFGNTJDRUZGMTk1Q0ExRkREMEI1
QjUwOUIzRjdGQzMwMUU0MzdFRDlEOTg0RUJEQkRBNTMyM0Q5MDBEOTIxRDdEMzNGMkU0MEY5RUVDQTZDREJCQzAyRDI5OUNDMEZCMUQ2QUY4M0NDQTMwRjBFRkFCOTgzaixwbG1udDFxdjZrNXN0NTl
renQ2anVyZGtjNDN4ZG5kcGR6eDZ3cnpwc3Z2NhJiCk4KRgofL2Nvc21vcy5jcnlwdG8uc2VjcDI1NmsxLlB1YktleRIjCiECXP6di2ieiAMXPIe8pOoWRbZi5zGyOWrFG4S12QtOCW4SBAoCCAESEA
oKCgVwbG1udBIBMhDAmgwaQLyKeSn3YZfPpHxkwspx9o59jbrZLaGvTYJoXP3zwREUUNDhAldXqOx+PRB2hOFJhvWR1l3TqUqBvVBrWw4kqfk=", "mode": "BROADCAST_MODE_SYNC" }'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1523  100   306  100  1217    519   2064 --:--:-- --:--:-- --:--:--  2585
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"30B499EDC39AAB5DAD1E0E83CE4301230B2A9470A2D365FBDDFBD88B8720C1B9","codespace":"machine","code":3,"data":"","raw_
log":"error during CheckTx or ReCheckTx: trust anchor not found","logs":[],"info":"","gas_wanted":"0","gas_used":"0","tx":null,"timestamp":"","events":
[]}}
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:55:testNotarizationFlow:PASS
```

Figure 3: Message for Trusted Anchor that has not registered the network

The first message in the red frame indicates that the seed of device is not registered to the network. Second one indicates that the Trusted Anchor used is also not known by the network. Note that Trust Anchor's private key is embedded in the code. If it will be used as a different device, it must be changed. It is called private_key_machine_id under rddl.c file.

First, Trust Anchor needs to be registered to the network. To register the Trusted Anchor, we must send a request to the network using the 32-digit Hex number specified by the “Machine Public Key” in Figure 3. This number is public key of Trusted Anchor. To send registration request, we need to use the following message;

curl -X POST https://testnet-ta.rddl.io/register/<32DigitHexMachinePubKey>

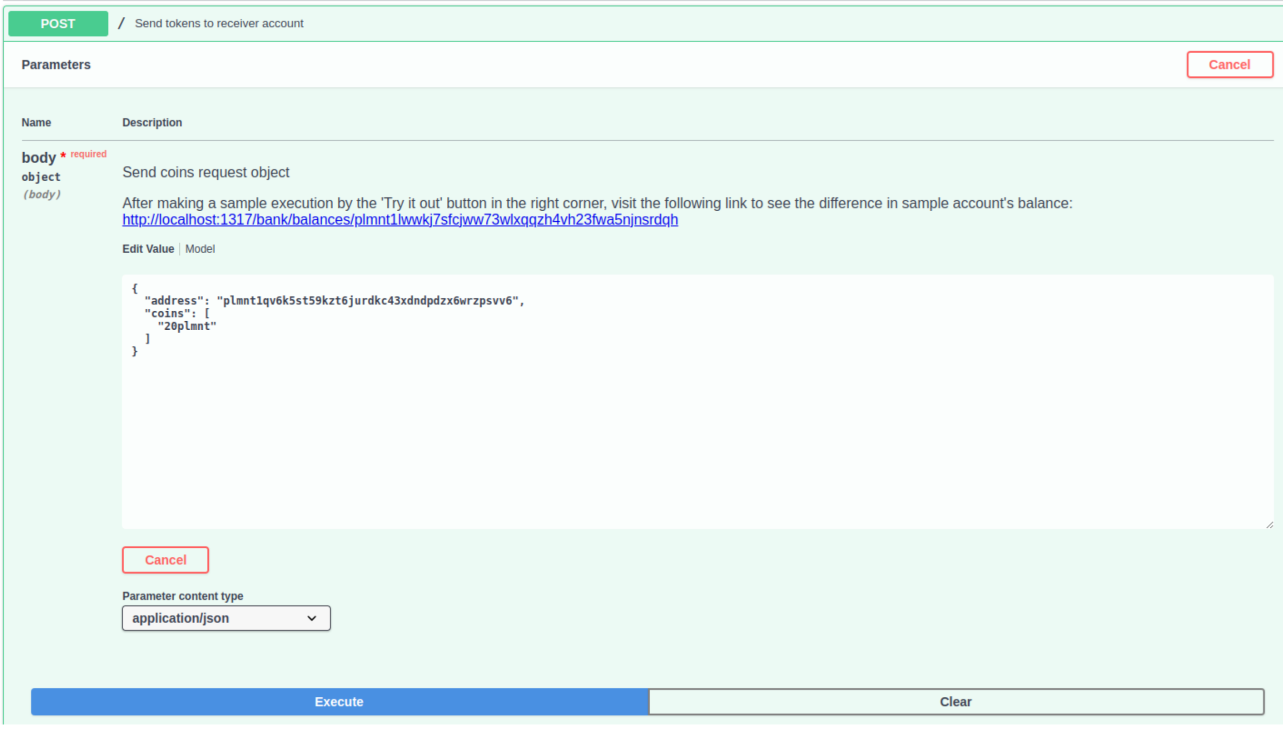


```
fatih@fatih-ThinkPad-L480:~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ curl -X POST https://testnet-ta.rddl.io/register/303F98F8EE26BB54384D1627E3A5E2
38D8031838183786A22E877C298A736FEA
```

Figure 4: Registration Request for Trusted Anchor

After registering the machine to the network, we will load some coins on it so that it can pay the transaction fees. Otherwise, transactions will be rejected due to insufficient coins.

To do this, open https://testnet-faucet.rddl.io/#/default/post_ . Then click POST and Try it out, respectively and upload money to the account ID. The Address is the value specified with “address:” and starting with plmnt as in Figure 3. After entering the address as shown in Figure 5 and writing down how much you will send to the coin section, you can click Execute and load the coin.



POST / Send tokens to receiver account

Parameters

Name | Description

body * required
object
(body)

Send coins request object

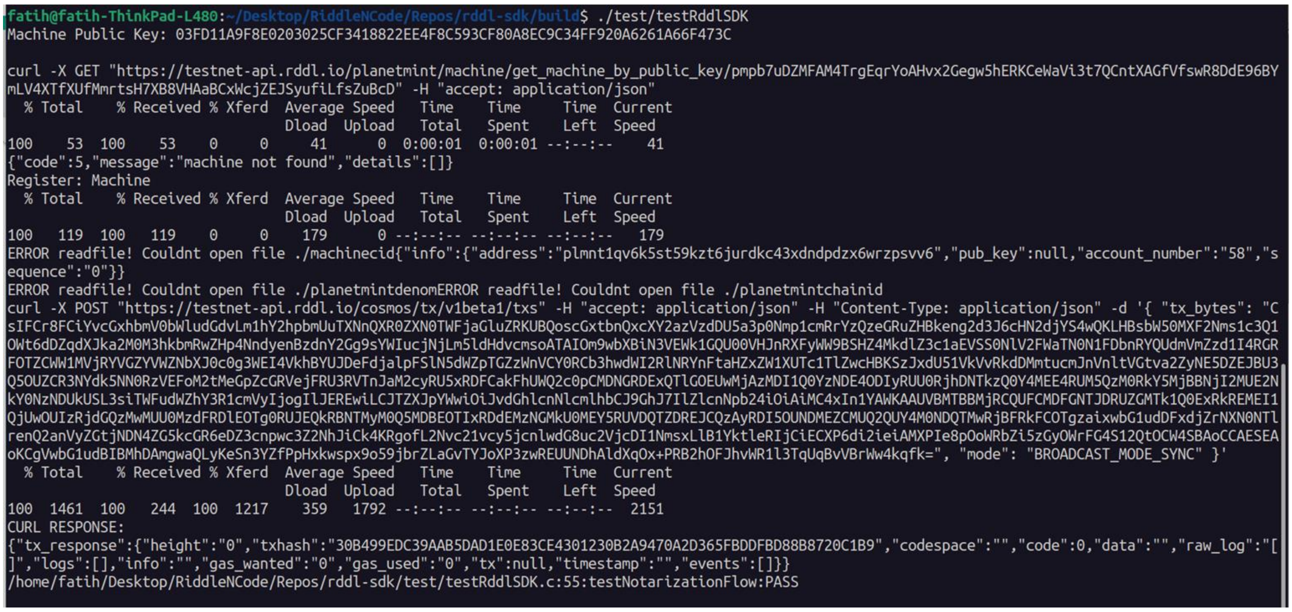
After making a sample execution by the 'Try it out' button in the right corner, visit the following link to see the difference in sample account's balance:
http://localhost:1317/bank/balances/plmnt1lwwkj7sfcjww73wlxqqzh4vh23fwa5njnsrdqh

```
{
  "address": "plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6",
  "coins": [
    "20plmnt"
  ]
}
```

Parameter content type: application/json

Figure 5: Sending coin to the device

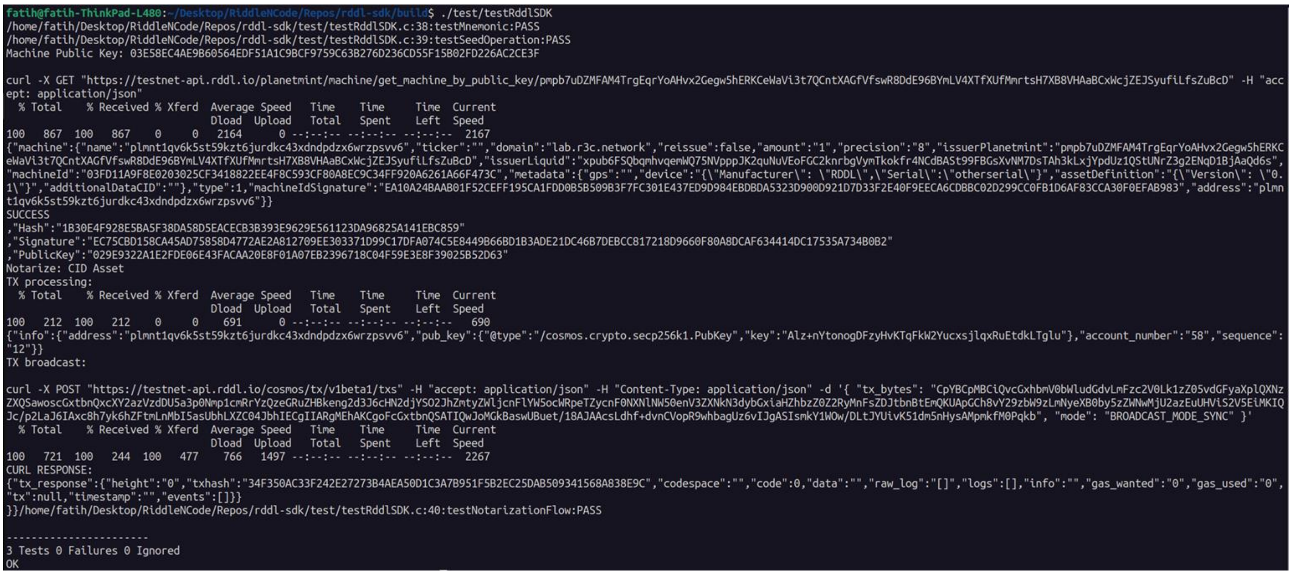
Now, when we run the same test code again, it will first perform the registration process as in Figure 6.



```
fatih@fatih-ThinkPad-L480:~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ ./test/testRddlSDK
Machine Public Key: 03FD11A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7uDZMFAM4TrgEqrYoAHvx2Gegw5hERKCeWaVi3t7QCntXAGfVfswR8DdE96BY
mLV4XTfXUfMmrtsH7XB8VHAaBCxWcjZEJSyufiLfsZuBcD" -H "accept: application/json"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    53  100    53    0     0     41      0  0:00:01  0:00:01 --:--:--    41
{"code":5,"message":"machine not found","details":[]}
Register: Machine
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   119  100   119    0     0    179      0 --:--:-- --:--:-- --:--:--   179
ERROR readfile! Couldnt open file ./machinecid{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":null,"account_number":"58","s
equence":"0"}}
ERROR readfile! Couldnt open file ./planetmintdenomERROR readfile! Couldnt open file ./planetmintchainid
curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{ "tx_bytes": "C
sIFCr8FCiYvcGxhbmV0bWludGdvLm1hY2hpbmUuTXNnQXR0ZXN0TWFjaGluZRKUBQoscGxtbnQxcXY2azVzdDU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2djYS4wQKLHBsbW50MXF2Nms1c3Q1
OWt6dDZqdXJka2M0M3hkbmRwZHp4NndyenBzdnY2Gg9sYWIucjNjLm5ldHdvcmsoATAIOm9wbXBiN3VEWk1GQU00VHJnRXFyWW9BSHZ4MkdlZ3c1aEVSS0NlV2FWaTN0N1FDbnRYQUdmVmZzd1I4RGR
FOTZCWW1MVjRYVGZYVWZNbXJ0c0g3WEI4VkhBYUJDeFdjalpFSlN5dWZpTGZzWnVCY0RCb3hwdWI2RlNRYnFtaHZxZW1XUTc1TlZwcHBKSzJxdU51VkVvRkdDMmtucmJnVnltVGtva2ZyNE5DZEJBU3
Q5OUZCR3NYdk5NN0RzVEFoM2tMeGpZcGRVejFRU3RVTnJaM2cyRU5xRDFCakFhUWQ2c0pCMDNGRDExQTlGOEUwMjAzMDI1Q0YzNDE4ODIyRUU0RjhDNTkzQ0Y4MEE4RUM5QzM0RkY5MjBBNjI2MUE2N
kY0NzNDUkUSL3siTWFudWZhY3R1cmVyIjogIlJEREwiLCJTZXJpYWwiOiJvdGhlcnNlcmlhbCJ9GhJ7IlZlcnNpb24iOiAiMC4xIn1YAWKAAUVBMTBBMjRCQUFCMDFGNTJDRUZGMTk1Q0ExRkREMEI1
QjUwOUIzRjdGQzMwMUU0MzdFRDlEOTg0RUJEQkRBNTMyM0Q5MDBEOTIxRDdEMzNGMkU0MEY5RUVDQTZDREJDMDJEMjk5Q0MwRkIxRDZBRjgzQ0NBMzBGMEVGQUI5ODNQMwRjBFRkFCOTgzaixwbG1udDFxdjZrNXN0NTl
renQ2anVyZGtjNDN4ZG5kcGR6eDZ3cnpwc3Z2NhJiCk4KRgofL2Nvc21vcy5jcnlwdG8uc2VjcDI1NmsxLlB1YktleRIjCiECXP6di2ieiAMXPIe8pOoWRbZi5zGyOWrFG4S12QtOCW4SBAoCCAESEA
oKCgVwbG1udBIBMhDAmgwaQLyKeSn3YZfPpHxkwspx9o59jbrZLaGvTYJoXP3zwREUUNDhAldXqOx+PRB2hOFJhvWR1l3TqUqBvVBrWw4kqfk=", "mode": "BROADCAST_MODE_SYNC" }'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1461  100   244  100  1217    359   1792 --:--:-- --:--:-- --:--:--  2151
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"30B499EDC39AAB5DAD1E0E83CE4301230B2A9470A2D365FBDDFBD88B8720C1B9","codespace":"","code":0,"data":"","raw_log":"[
]","logs":[],"info":"","gas_wanted":"0","gas_used":"0","tx":null,"timestamp":"","events":[]}}
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:55:testNotarizationFlow:PASS
```

Figure 6: Registiration of Seed

After the seed is registered, every time we call the test code, it will perform a transaction that contains the data as in Figure 7.



```
fatih@fatih-ThinkPad-L480:~/Desktop/RiddleNCode/Repos/rddl-sdk/build$ ./test/testRddlSDK
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:38:testMnemonic:PASS
/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:39:testSeedOperation:PASS
Machine Public Key: 03E58EC4AE9B60564EDF51A1C9BCF9759C63B276D236CD55F15B02FD226AC2CE3F

curl -X GET "https://testnet-api.rddl.io/planetmint/machine/get_machine_by_public_key/pmpb7uDZMFAM4TrgEqrYoAHvx2Gegw5hERKCeWaVi3t7QCntXAGfVfswR8DdE96BYmLV4XTfXUfMmrtsH7XB8VHAaBCxWcjZEJSyufiLfsZuBcD" -H "acc
ept: application/json"
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   867  100   867    0     0   2164      0 --:--:-- --:--:-- --:--:--  2167
{"machine":{"name":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","ticker":"","domain":"lab.r3c.network","reissue":false,"amount":"1","precision":"8","issuerPlanetmint":"pmpb7uDZMFAM4TrgEqrYoAHvx2Gegw5hERKC
eWaVi3t7QCntXAGfVfswR8DdE96BYmLV4XTfXUfMmrtsH7XB8VHAaBCxWcjZEJSyufiLfsZuBcD","issuerLiquid":"xpub6FSQbqmhvqemWQ75NVpppJK2quNuVEoFGC2knrbgVymTkokfr4NCdBASt99FBGsXvNM7DsTAh3kLxjYpdUz1QStUNrZ3g2ENqD1BjAaQd6s",
"machineId":"03FD11A9F8E0203025CF3418822EE4F8C593CF80A8EC9C34FF920A6261A66F473C","metadata":{"gps":"","device":"{\"Manufacturer\": \"RDDL\",\"Serial\":\"otherserial\"}","assetDefinition":"{\"Version\": \"0.
1\"}","additionalDataCID":""},"type":1,"machineIdSignature":"EA10A24BAAB01F52CEFF195CA1FDD0B5B509B3F7FC301E437ED9D984EBDBDA5323D900D921D7D33F2E40F9EECA6CDBBC02D299CC0FB1D6AF83CCA30F0EFAB983","address":"plmn
t1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6"}}
SUCCESS
,"Hash":"1B30E4F928E5BA5F38DA58D5EACECB3B393E9629E561123DA96825A141EBC859"
,"Signature":"EC75CBD158CA45AD75858D4772AE2A812709EE303371D99C17DFA074C5E8449B66BD1B3ADE21DC46B7DEBCC817218D9660F80A8DCAF634414DC17535A734B0B2"
,"PublicKey":"029E9322A1E2FDE06E43FACAA20E8F01A07EB2396718C04F59E3E8F39025B52D63"
Notarize: CID Asset
TX processing:
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   212  100   212    0     0    691      0 --:--:-- --:--:-- --:--:--   690
{"info":{"address":"plmnt1qv6k5st59kzt6jurdkc43xdndpdzx6wrzpsvv6","pub_key":{"@type":"/cosmos.crypto.secp256k1.PubKey","key":"Alz+nYtonogDFzyHvKTqFkW2YucxsjlqxRuEtdkLTglu"},"account_number":"58","sequence":
"12"}}
TX broadcast:

curl -X POST "https://testnet-api.rddl.io/cosmos/tx/v1beta1/txs" -H "accept: application/json" -H "Content-Type: application/json" -d '{ "tx_bytes": "CpYBCpMBCiQvcGxhbmV0bWludGdvLmFzc2V0Lk1zZ05vdGFyaXplQXNz
ZXQSawoscGxtbnQxcXY2azVzdDU5a3p0Nmp1cmRrYzQzeGRuZHBkeng2d3J6cHN2djYSO2JhZmtyZWljcnFlYW5ocWRpeTZycnF0NXNlNW50enV3ZXNkN3dybGxiaHZhbzZ0Z2RyMnFsZDJtbnBtEmQKUApGCh8vY29zbW9zLmNyeXB0by5zZWNwMjU2azEuUHViS2V5EiMKIQ
Jc/p2LaJ6IAxc8h7yk6hZFtmLnMbI5asUbhLXZC04JbhIECgIIARgMEhAKCgoFcGxtbnQSATIQwJoMGkBaswUBuet/18AJAAcsLdhf+dvnCVopR9whbagUz6vIJgASIsmkY1WOw/DLtJYUivK51dm5nHysAMpmkfM0Pqkb", "mode": "BROADCAST_MODE_SYNC" }'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   721  100   244  100   477    766   1497 --:--:-- --:--:-- --:--:--  2267
CURL RESPONSE:
{"tx_response":{"height":"0","txhash":"34F350AC33F242E27273B4AEA50D1C3A7B951F5B2EC25DAB509341568A838E9C","codespace":"","code":0,"data":"","raw_log":"[]","logs":[],"info":"","gas_wanted":"0","gas_used":"0",
"tx":null,"timestamp":"","events":[]}}
}}/home/fatih/Desktop/RiddleNCode/Repos/rddl-sdk/test/testRddlSDK.c:40:testNotarizationFlow:PASS

-----------------------
3 Tests 0 Failures 0 Ignored
OK
```

Figure 7: Data Transaction into RDDL Network