D. I System

Decentralized Identity Verification Platform By Police

Documentation

➢Transaction Processors (TP)

- KnowYourCustomer 1.0

This TP provides 3 business logics in the chain.

◆ Add User Data

addUserData() function provides to create a record of user KYC details.
The recorded Data contains Encrypted KYC Data and Mini Data.

◆ Change Encryption Key

changeEncKey() function provides to update the record to corresponding state address.
The new recorded Data contains New Encrypted KYC Data and Mini Data.

◆ Verify User

verifyUser() function provides to update the record to corresponding state address.
In the new record ,The Mini Data update with Verify Tag.

➢Client

This project assumes that each portal has a unique view and access to the network with capabilities limited to their functionality. Hence this project has 3 different client views, each of which can be accessed via its individual URL as follows:

◆ User

http://localhost:3000/user

In this client , the transactions are done using a private key. Here it is not hard-coded with the client , in a working environment it should be given externally from a read only device.

It should include Name ,Email , Date of birth ,Address, Phone Number , Pin-code and Encryption Key are given as the inputs. User has an option to change encryption key and view data from the interface

If the user is verified then user can only edit the Data after having a limited time and reapply for verification.

◆ Police

http://localhost:3000/police

In this client , the transactions are done using a private key. Here it is hard-coded with the client , the key is secured by public key matching method.

In this part inside police UI we can see the transaction details i,e user details send by user. Only details allowed by user to share to police should be able to display ,all other details like voter id no , aadhar no and other kinds

of details are encrypted .Mainly the data are fetched from state to display .If user shares decryption key, police should be able to view all details using decryption key.

Here police can accept or reject user data . If rejection occurs users are not permitted to get verified public key and they cant even login to client part .Here rejection means that the user data is deleted from state .Accept data pass the user details to the validator and should be added to block .If police accept user should get a public key and they can login into client portal and check their data using this public key and decryption key so user should able to share public key in case of identification purposes for various activities .

◆ User Client

http://localhost:3000/client

It doesn’t make any transaction.Only a verified user can log to the user client.In there the client can check the users by their public key.