Secure Banking System

Group 14

-- User Guide--

VM - https://192.168.2.235:443

Requirements -

- Please download the Google Authenticator App from the PlayStore / App Store. We use this app for OTP in several functions of SBS.
- We require the JavaScript to be enabled in the browser at all times because of various verifications and setups involving Virtual Keyboards or PKI.

Admin credentials -

- We'll be providing one admin's credentials (Username, Password and OTP) for all the testers. They are required to create their own admins using the common account and are required to create other internal and external users using their own admin account.
- Please do not use the default admin provided. This will only cause confusion among the testers since we employ a few security measures involving user sessions.
- Moreover, we provide such a structure to avoid this confusion for testers. In a real world scenario, there will be only one admin for the system with other types of users under them.
- Do not use the default admin as there might be issues for different people trying to access the system simultaneously with the OTP. Once used, the OTP cannot be used by any user again.

Username - admin
Password - thisisadmin@password1
OTP device -

QR Code

or use the URL below:

otpauth://totp/admin?digits=6&secret=CPTOCGB6PLC6RDJ2E2DPZX7GCWQIQX37&algorithm=SHA1&period=30

Scan this QR Code on your Google Authenticator App.

Note - Please do not change the password for the default admin that we provide to you. Also, do not delete or interfere with activity related to accounts of other testers not created by you to avoid inconvenience and misunderstandings for other tester.

Assumptions -

- Admins are highly trustworthy people, followed by the other internal users. We assume they behave like admins and not misuse the authority provided to them.
- We tested the app on Google Chrome.
- We use the same form for all sorts of transactions.
    - To credit funds to an account, the user must leave the 'from' field empty and select his account in the 'to' field.
    - To debit funds from an account, the user must leave the 'to' field empty and select his account in the 'from' field.
    - To transfer funds from one account to another, both the to and from fields must be specified.
- For Security Reasons some forms may not be clickable if you go back on browser (try refreshing it or press home button).
- **We assume that different users use different devices like in a real world scenario.**

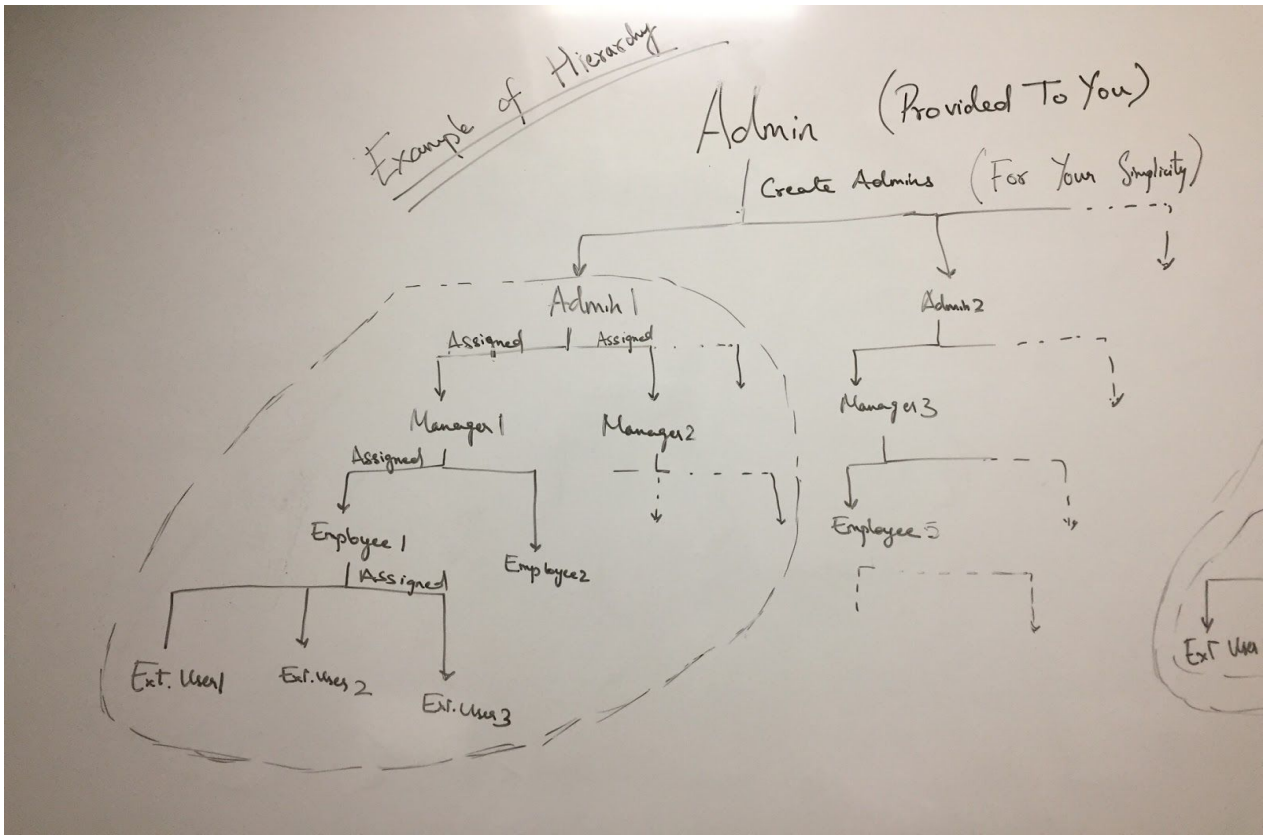
Common points -

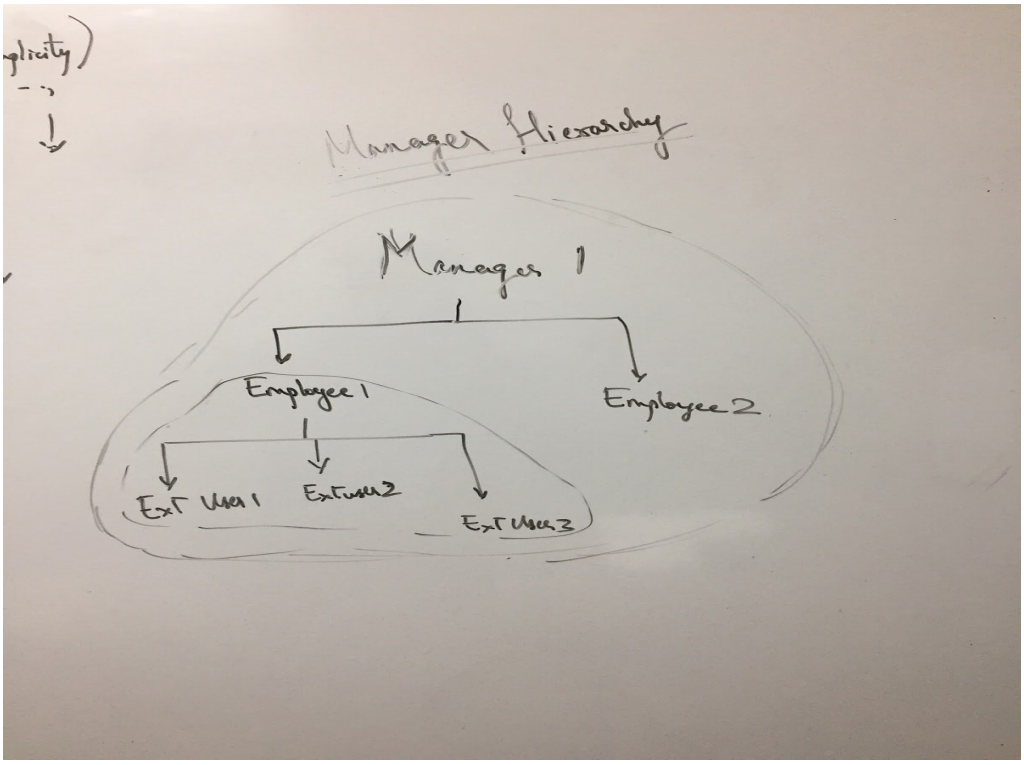
- When a user request is approved / declined, mail is sent to the user who requested it.
- For All the Transaction related work the PKI should be Setup. If you Logged in from a different browser or device kindly reset the PKI.
- **Once the tester sets up the password for a user using the one-time link on his mail during signup or password reset, if the admin page is logged into his browser, he might get redirected to the admin page. This does not imply that the current user has been given admin rights. In a real scenario, the admin and the current user will be on different systems.**
- At the time of logging in as another user, pressing the Back button may create problems due to session security. You may see an error message, just press home and retry.

Hierarchy of Users -

- The System Administrator is the highest authority.
- There are some managers assigned to each admin and some employees assigned to each manager.
- The bank cannot have any external users unless there is a minimum of one admin, one manager assigned to that admin and one employee assigned to that manager. So, for an admin to have an external user under him, he must first have created internal users.
- The testers are required to create an admin, followed by a manager and then an employee initially. After this, any number of external or internal users may be created.
- Each external user (merchant and individual user) is assigned to an employee, who is assigned to a manager and a manager being assigned to some admin.

The Bubbles in the image below are to represent the Particular Hierarchy.





Login -

- The following details are required to be entered on the login page:
    - Username
    - Password
    - OTP(from Google Authenticator)

Different Types of Users and their functionality

Admin

- **Create User -**
    - Assumption - The user gives his details to the admin physically and there is some behind the scene verification of the details. And only then, the admin creates the user's account on the web-based system.

    - Only the admin can create internal and external users on the SBS. The important details to be entered include - a correct email address, a unique username and the type of user. For simplicity, we allow duplicate email address so that testers can assume identity of multiple users and all the emails are sent to that address only. But, in a real world scenario, email address would be unique too.
    - The admin must create a manager before any other user. The manager is assigned to the admin who created him. Basically, whichever user and admin creates comes under him.
    - After this, he can add an employee which will be assigned to a manager randomly. Though, the manager will be someone assigned to the same admin.
    - An external user can be created only if all the three types of internal users are present in the system. The external user is then, randomly assigned to an employee. Again, the employee will be someone created by the same admin.
    - After the admin signs up a user, the user receives an e-mail on the registered email address with a one-time link to setup his password. The password must contain a minimum of 10 characters, a letter, a digit and a special character.
    - After setting up his password, the user receives a mail with a one-time link to a QR code. The users are required to scan this code with the Google Authenticator app to save OTP in their phones. This is a required set up for them to be able to log into their accounts.
    - Only after completing the above mentioned procedures, the user account is activated.

- **View/ Edit User Information -**
    - An admin can view the user information for all users (internal and external) except other admins.
    - The admin can modify the details (name, email address, phone number, date of birth) of all the internal and external users except other admins.
- **Login as Another User -**
    - The admin can login as any other external or internal user except another admin. This is done to provide the admin a platform to perform maintenance operations and troubleshooting.

- **View User PII with permission from Government -**
    - The admin can select a user whose PII he wants to access.

    - He can view the PII only when his request is approved by the government authority.
    - When he sends a request, the government authority receives a mail with a one-time link through which it can approve the admin's request.
    - The credentials for the government ID are -
        - Email - govt.sbs2018@gmail.com
        - Password - thisissbs2018

- **Views Account Details of External Users -**
    - The admin can view the account details (account number, balance) for all the external users.

- **View User Requests Pending for Approval -**
    - This view contains all the requests sent to the admin by internal and external users pending for approval. The requests can be for viewing/ editing user information, viewing transactions, deleting external user account etc.
    - The admin might approve or decline these requests.

- **View All Pending Risky Transactions-**
    - The admin can view all the pending risky transactions requests (amount > 100000) created by/ to or from all the active users in the system.
    - He is also authorised to approve or decline these requests. The admin is required to enter his OTP from Google Authenticator for the same. PKI verification will take place here.
    - The account balance is updated only after successful approval or rejection of the requests.

- **View All Pending Transactions -**
    - The admin can view all the pending transactions requests created by/ to or from all the active users in the system.
    - He is also authorised to approve or decline these requests. The admin is required to enter his OTP from Google Authenticator for the same. PKI verification will take place here.
    - The account balance is updated only after successful approval or rejection of the requests.

- **View All Completed Transactions -**
    - The admin can view the transaction history of the successful transactions of all the users sorted in descending order of the time they were completed.
    - This includes the details of all the transactions including from account, to account, time completed, internal user who approved the transaction and the amount.
    - The admin is authorised to view the details of these transactions by clicking on the links.

- **Transaction Locator -**
    - This can help the admin filter the required transactions from all the transactions based on certain search criteria.
    - He can filter using one or more of the fields (transaction id, from account, to account, amount, completed or pending).
    - If no search criteria is entered, the default list consists of all the pending transactions of active users and all the completed transactions of the currently active and inactive users.
    - The admin is authorised to view the details of these transactions by clicking on the links.

- **Initiate User Password Reset -**
    - Assumption - If an internal or external user loses access to his account, he contacts the admin physically to reset his credentials. And only after some behind the scene verification, the request is initiated. This follows the same procedure used during the Signup process.
    - The admin choses the user whose account he wishes to reset.
    - The user receives an e-mail on the registered email address with a one-time link to setup his password. The password must contain a minimum of 10 characters, a letter, a digit and a special character.
    - After setting up his password, the user receives a mail with a one-time link to a QR code. The users are required to scan this code with the Google Authenticator app to save OTP in their phones. This is a required set up for them to be able to log into their accounts.
    - The public and private key of the user is also reset automatically through this process.

- **Reset PKI -**
    - The admin can reset his public and private keys using this feature. This is required when he wishes to perform a transaction from a new browser or a new device.

- **View System Logs**
    - The admin can view the system log files according to the date on which the logs were created.
    - The logs include all the system usage information such as adding of accounts, user requests sent, approved and declined, request for PII, transaction requests sent, approved and declined etc.
    - The logs of the current date are added to Current Log File.

- **View Transaction Logs**
    - The admin can view the transaction log files according to the date on which the logs were created.
    - The logs include transaction related information such as requests sent, approved and declined etc.
    - The logs of the current date are added to Current Transaction Log File.
    - If the logs are from None to a user, it implies a credit request. If they are from a user to None, it implies a debit request. If they are from one user to another, it is a request for transferring funds.

- **Delete User**
    - The admin can delete any manager or employee's account using this option.
    - The account for an employee cannot be deleted if he is the only employee in the system under that particular admin and has external users assigned to him.
      When an employee is deleted, and there exist other employees under the same admin, all the external users assigned to him are assigned randomly to some of these employees.
    - The account for a manager cannot be deleted if he is the only manager in the system under that particular admin and has employees assigned to him.
      When a manager is deleted, and there exist other managers under the

same admin, all the employees assigned to him are assigned randomly to some other manager.
    - The account cannot be deleted in case the user has some transactions pending. Particularly, we don't let a user account be deleted if there is an unresolved transaction where the from account is owned by that user. Meaning, when his transaction is supposed to transfer money to some other account or maybe debit. In all other cases, we decline all pending transactions.
    - When an employee or a manager is deleted, the requests pending to him for approval are either deleted or redirected to the new assigned employee or manager. The requests created by him are deleted.

Manager

Each manager is assigned to an admin. The tester can check the assigned admin to that manager on the home view of the manager ("Assigned To: ")

- **View/ Edit Information for all External Users -**
    - He can view all the external users that are present in the system and can click on them to view their profiles.
    - To view the user information of any user, he needs to send a request to the assigned admin. After the admin approves his request, he can view the details only once.
    - For Editing - He sends a request to the assigned admin by clicking submit in the "Request For Access Page" after getting viewing rights.
    - If he wishes to edit the user details he'll send another request to the assigned admin for getting one time edit rights.
    - After that the manager can edit the details and after making changes, another request is sent to the assigned admin for verification. If the request is approved the changes are reflected.

- **View Accounts Details of Users Assigned to You -**
    - The manager can view the account details (account number, balance) of the external users that are assigned to an employee who is assigned to him.

- **View User Requests Pending for Approval**
    - This view contains all the requests sent to the manager by employees assigned to him and external users pending for approval. The requests can be for viewing/ editing user information, viewing transactions etc.
    - The manager might approve or decline these requests.

- **View Pending Transactions Assigned to You -**
    - The manager can view all the pending transaction requests (risky or not) created by an employee assigned to him.
    - The manager can also view the pending risky transactions (amount > 100000) created by external users assigned to an employee who is assigned to him.
    - He is also authorised to approve or decline these requests. The manager is required to enter his OTP from Google Authenticator for the same. PKI verification will take place here.
    - The account balance is updated only after successful approval or rejection of the requests.

- **View Pending Risky Transactions Assigned to You**
    - The manager can view all the pending transactions requests (amount > 100000) created by an employee assigned to him.
    - The manager can also view the pending risky transactions (amount > 100000) created by external users assigned to an employee who is assigned to him.
    - He is also authorised to approve or decline these requests. The manager is required to enter his OTP from Google Authenticator for the same. PKI verification will take place here.
    - The account balance is updated only after successful approval or rejection of the requests.

- **View Completed Transactions**
    - The manager can view the transaction history of the successful transactions of all the users sorted in descending order of the time they were completed.
    - The manager can view the details of the transaction approved by him without permission. For all other transactions details he has to send a request.

    - For one-time viewing the details of the transaction, the manager can either request the user who created the transaction by clicking the Submit button or can request the assigned Admin by clicking Request Admin button
    - Once the request is approved, the manager can view the details once after which he has to request again.

- **Transaction Locator**
    - This can help the manager filter the required transactions from all the transactions based on certain search criteria.
    - He can filter using one or more of the fields (transaction id, from account, to account, amount, completed or pending).
    - If no search criteria is entered, the default list consists of all the pending transactions of active users and all the completed transactions of the currently active and inactive users.
    - The manager can view the details of the transaction approved by him without permission. For all other transactions details he has to send a request.
    - For one-time viewing the details of the transaction, the manager can either request the user who created the transaction by clicking the Submit button or can request the Admin by clicking Request Admin button
    - Once the request is approved the Manager can view the details once then after he has to request again.

- **Reset PKI**
    - The manager can reset his public and private keys using this feature. This is required when he wishes to perform a transaction from a new browser or a new device.

Employee

Each employee is assigned to a manager. The tester can check the assigned manager to that employee on the home view of the employee (“Assigned To: ”)

- **View/ Edit Information for External Users**

    - He can view all the external users that are present in the system and can click on them to view their profile.
    - To view the user information of any user, he needs to send a request to the assigned manager. After the manager approves his request, he can view the details only once.
    - For Editing - He sends a request to the assigned manager by clicking submit in the “Request For Access Page” after getting viewing rights.
    - If he wishes to edit the user details he’ll send another request to the assigned manager for getting one time edit rights.
    - After that the employee can edit the details and after making changes, another request is sent to the assigned admin for verification. If the request is approved the changes are reflected.

- **View Account Details of Users Assigned to You**
    - The employee can view the account details (account number, balance) of the external users that are assigned to him.

- **View User Requests Pending for Approval**
    - This view contains all the requests sent to the employee by external users assigned to him pending for approval. The requests can be for editing profile, creating a new account etc.
    - The employee might approve or decline these requests.

- **Create Transaction for External Users**
    - Assumption - The external user contacts the employee physically to create the required transaction. Thus, the employee is authorised to create the request on behalf of the external user.
    - The employee can credit and debit funds to and from any external user’s account.
    - He can transfer funds from any of external user’s account if the user has enough balance.
    - The amount entered must be less than or equal to the balance of the account selected in the ‘from’ field.
    - The employee also needs to enter his OTP to complete the request.
    - This request is sent to the manager to which he is assigned.
    - PKI verification takes place here.

- **View Pending Transactions Assigned to You**
    - The employee can view all the pending transaction requests created by external users assigned to him.
    - He is also authorised to approve or decline these requests. The employee is required to enter his OTP from Google Authenticator for the same. PKI verification will take place here.
    - The account balance is updated only after successful approval or rejection of the requests.
    - The risky transactions of the external users assigned to him are also present in the list but he does not have the authorization to approve them. Only the system manager he is assigned to or an admin can approve them.

- **View Completed Transactions**
    - The employee can view the transaction history of the successful transactions of all the users sorted in descending order of the time they were completed.
    - The employee can view the details of the transaction created by him or approved by him without permission. For all other transactions details he has to send a request.
    - For one-time viewing the details of the transaction, the employee can either send a request to the user who created the transaction by clicking the Submit button or can request to Admin by clicking Request Admin button.
    - Once the request is approved, the employee can view the details once after which he has to request again.

- **Transaction Locator**
    - This can help the employee filter the required transactions from all the transactions based on certain search criteria.
    - He can filter using one or more of the fields (transaction id, from account, to account, amount, completed or pending).
    - If no search criteria is entered, the default list consists of all the pending transactions of active users and all the completed transactions of the currently active and inactive users.

    - The employee can view the details of the transaction created by him or approved by him without permission. For all other transactions details he has to send a request.
    - For one-time viewing the details of the transaction, the employee can either request to user who created the transaction by clicking the Submit button or can request to Admin by clicking Request Admin button.
    - Once the request is approved the Employee can view the details once then after he has to request again.

- **Reset PKI**
    - The employee can reset his public and private keys using this feature. This is required when he wishes to perform a transaction from a new browser or a new device.

Individual User

Each Individual User is assigned to an employee. The tester can check the assigned employee to that user on the home view of the user (“Assigned To: ”). The manager who the employee is assigned to can also be visible on the home view of the user. This is needed in case of risky transactions.

- **View/ Edit Profile -**
    - The individual user can view his own profile details.
    - If he wishes to edit these details (name, email, phone number and DOB), he can click on Edit and make the necessary changes.
    - After this, a request to approve these changes are sent to the assigned admin.
    - Individual User ----assigned to---> Employee ----assigned to---> Manager ----assigned to---> Admin (assigned admin for individual user)
    - The changes are reflected only when the admin approves this request.

- **Credit/ Debit/ Transfer Funds**
    - The individual can credit and debit funds to and from his own accounts. He does not have permissions to debit funds from other users accounts. He also does not have permissions to credit funds to other users accounts.

    - He can transfer funds from any of his accounts if they have enough balance.
    - He can only transfer funds to his own accounts or the accounts he adds as known accounts.
    - The amount entered must be less than or equal to the balance of the account selected in the ‘from’ field.
    - The user also needs to enter his OTP to complete the request.
    - This request is sent to the employee to which he is assigned. However, in case of a risky transaction, it is sent to the assigned manager.
    - PKI verification takes place here.

- **Pending Transaction Requests**
    - The individual user can view the pending transaction requests which have been created by him.
    - He can also view the requests created by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **View Completed Transactions**
    - The individual user can view the completed (approved) transactions which have been created by him.
    - He can also view the completed (approved) transactions created by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **Transaction Locator**
    - This can help the individual user filter the required transactions from all the transactions visible to him based on certain search criteria.
    - He can filter using one or more of the fields (transaction id, from account, to account, amount, completed or pending).
    - If no search criteria is entered, the default list consists of all the pending and completed transactions created by him or by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **View User Requests Received**

    - This view contains all the requests sent to the individual user by internal and external users pending for approval. The requests can be for viewing transactions by internal users, adding their accounts to client accounts by a merchant etc.
    - The individual user might approve or decline these requests.

- **View Your Accounts/ Balance**
    - The user can view all of his accounts along with the balance of each account.

- **Request New Account**
    - If the individual user wishes to create another account, he can use this view to send a request to the employee assigned to him.
    - The account is created initially with zero balance only if the employee approves this request.

- **View PII**
    - If the user has not entered his PII (Aadhar Number), he can enter it using this form.
    - Once he has entered his PII, he can view it whenever he wants by entering his OTP.

- **Enter Known Account**
    - The individual user can enter the account numbers of his known accounts using this view.
    - He can only transfer funds to the accounts he adds in this view.
    - He is not allowed to add his own accounts in this view.

- **View Known Accounts**
    - The individual user can view all his known accounts along with his own accounts in this view.

- **Remove Merchant User Permissions**
    - If a merchant has obtained the permission to enter an account of the individual user as one of his clients, the individual user can revoke that permission at any time using this view. This removes the individual user as one of the merchant's clients.

    - If a client removes permissions for a merchant but before that the merchant has already sent a request for a transaction, the transaction can be approved by an internal user. This is because the transaction was created before the permissions were revoked.

- **Reset PKI**
    - The individual user can reset his public and private keys using this feature. This is required when he wishes to perform a transaction from a new browser or a new device.

- **Delete User**
    - If a user wishes to delete his profile, he can send a request to the employee he is assigned to by entering his OTP.
    - The employee may approve or decline this request.
    - If the request has been approved by the employee, it is sent to the assigned admin. Individual User ----assigned to---> Employee ----assigned to---> Manager ----assigned to---> Admin (assigned admin for manager)
    - The user delete request cannot be approved if the user has pending transactions.
    - When the request is approved, the user becomes inactive and cannot log into SBS. All his pending requests are deleted.

Merchant

Each merchant is assigned to an employee. The tester can check the assigned employee to that user on the home view of the user (“Assigned To: ”). The manager who the employee is assigned to can also be visible on the home view of the user. This is needed in case of risky transactions.

- **View/ Edit Profile**
    - The merchant can view his own profile details.
    - If he wishes to edit these details (name, email, phone number and DOB), he can click on Edit and make the necessary changes.
    - After this, a request to approve these changes are sent to the assigned admin.

    - Merchant ----assigned to---> Employee ----assigned to---> Manager ----assigned to---> Admin (assigned admin for manager)
    - The changes are reflected only when the admin approves this request.

- **Credit/ Debit/ Transfer Funds**
    - The merchant can credit and debit funds to and from his own accounts and his client accounts. He does not have permissions to debit funds from any other accounts. He also does not have permissions to credit funds to other accounts.
    - He can transfer funds from any of his accounts or his client accounts if they have enough balance.
    - He can only transfer funds to his own accounts, his client accounts or the accounts he adds as known accounts.
    - The amount entered must be less than or equal to the balance of the account selected in the 'from' field.
    - The user also needs to enter his OTP to complete the request.
    - This request is sent to the employee to which he is assigned. However, in case of a risky transaction, it is sent to the assigned manager.
    - PKI verification takes place here.

- **Pending Transaction Requests**
    - The merchant can view the pending transaction requests which have been created by him.
    - He can also view the requests created by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **View Completed Transactions**
    - The merchant can view the completed (approved) transactions which have been created by him.
    - He can also view the completed (approved) transactions created by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **Transaction Locator**
    - This can help the merchant filter the required transactions from all the transactions visible to him based on certain search criteria.

    - He can filter using one or more of the fields (transaction id, from account, to account, amount, completed or pending).
    - If no search criteria is entered, the default list consists of all the pending and completed transactions created by him or by other external or internal users to or from his account.
    - He can also view the details of these transactions.

- **View User Requests Received**
    - This view contains all the requests sent to the merchant by internal and external users pending for approval. The requests can be for viewing transactions by internal users, adding their accounts to client accounts by a merchant etc.
    - The merchant might approve or decline these requests.

- **View Your Accounts/ Balance**
    - The merchant can view all of his accounts along with the balance of each account.

- **Request New Account**
    - If the merchant wishes to create another account, he can use this view to send a request to the employee assigned to him.
    - The account is created initially with zero balance only if the employee approves this request.

- **Enter Known Account**
    - The merchant can enter the account numbers of his known accounts using this view.
    - For him to be able to transfer funds to accounts other than his own accounts or his client accounts, he needs to add the accounts in this view.
    - He is not allowed to add his own accounts in this view.

- **View Known Accounts**
    - The merchant can view all his known accounts along with his own accounts in this view.

- **Enter Client Account**

    - The merchant can enter the account number of an individual user or a merchant and sends a request to the respective user for becoming a client.
    - After the request is approved, he can make transactions on the client's behalf.

- **View Client Accounts**
    - The merchant can view all the clients that he has added and have been approved by the client.

- **Remove Merchant User Permissions**
    - If a merchant has obtained the permission to enter an account of this merchant as one of his clients, this merchant can revoke that permission at any time using this view. This removes him as one of the merchant's clients.
    - If a client removes permissions for a merchant but before that the merchant has already sent a request for a transaction, the transaction can be approved by an internal user. This is because the transaction was created before the permissions were revoked.

- **Reset PKI**
    - The merchant can reset his public and private keys using this feature. This is required when he wishes to perform a transaction from a new browser or a new device.

- **Delete User**
    - If a merchant wishes to delete his profile, he can send a request to the employee he is assigned to by entering his OTP.
    - The employee may approve or decline this request.
    - If the request has been approved by the employee, it is sent to the assigned admin. Merchant ----assigned to---> Employee ----assigned to---> Manager ----assigned to---> Admin (assigned admin for manager)
    - The user delete request cannot be approved if the user has pending transactions.
    - When the request is approved, the user becomes inactive and cannot log into SBS. All his pending requests are deleted.