Overview

The Business Control platform by Verestro enables digital card issuing and expense management for modern companies. By adapting to the changing needs of the current small, medium companies and big corporations and business customers digital, Business Controls enables companies to create and deliver instantly a temporary business Mastercard card to employee, simplify invoice collections and settlements of expenses.

If you are a bank or fintech you can offer a new product for your business customers and increase revenues.

The platform consists of web portal and mobile application or SDK. The simplest white label solution can be delivered in 3 months from start of the project.

Purpose and scope

This product guide provides a high-level overview of Business Control. This document covers the following topics:
- description of possible configurations,
- granting access,
- description of main processes as: login, reset password, cards import, redemption of card,
- additional and optional functionalities.

Terminology

This section explains a number of key terms used in this document.

Name	Description
Operator/portal user	The user working using web portal.
End-user/mobile user	A corporate employee who received a card and uses a mobile app.

Payment history	It's possible that transaction history will be stored on Verestro wallet server for infinite time (this setting can be specified during onboarding with Mastercard). If these options are enabled, MPA can retrieve transaction history for given card and payment instrument ID. Transactions are returned in corresponding parts for better user experience. Particular transaction may appear on the list with delay – depending on integrated external components.
Session token	Access to the system by a application user is secured using a session token to uniquely associate the session with the user. It is required to perform any action.
sFPANs (Subordinate Funding Pan)	Valid card numbers supplied by the Issuer. All payment messages will be delivered to the Issuer with this card number in Data Element 02.
Funding Card Alias	A name given to the ultimate funding account to which payments will flow. This name is assigned by the Issuer and should be recognisable to the Corporate who owns the account. E.g. "JoeCorp HR USDollar".
CSV	Comma Separated Values.
Digital Tokens	This is the surrogate card number that is inserted into the NFC chip in the Mobile phone. For tap payments, this is the number shared with the Point of sale device. On all message flows; it is mapped by Mastercard to its parent sFPAN. The Issuer will then map the sFPAN to the Funding Account.
Virtual Card	This is the optional card number for eCommerce payments - number entered at the eCommerce checkout page. On all message flows; it is mapped by Mastercard to its parent sFPAN. The Issuer will then map the sFPAN to the Funding Account.
Approval	In the context of Business Control, this is the assignment of a specific card for a certain period of time to a defined user.
Reapproval	By reapproval is meant the process of changing the data of a specific card assignment. Limits or date range can be changed.

Mobile reapproval	The process of changing a specific assignment initiated by the end user - which means through the use of a mobile application.
Group limit	This limit determines the maximum amount with which anyone in the group can assign a card to a user and the maximum amount on a card that can be accepted in a given group if an assignment confirmation request comes in from a group with a lower limit.

Key Use Cases

Below we present a list of key use cases enabled on Business Control platform. We are constantly working on new functionalities that are adding value to the product:

- issue virtual card for employee,
- setup card limits (time, date, transaction limits etc.),
- manage groups in companies (departments or teams),
- scan invoices,
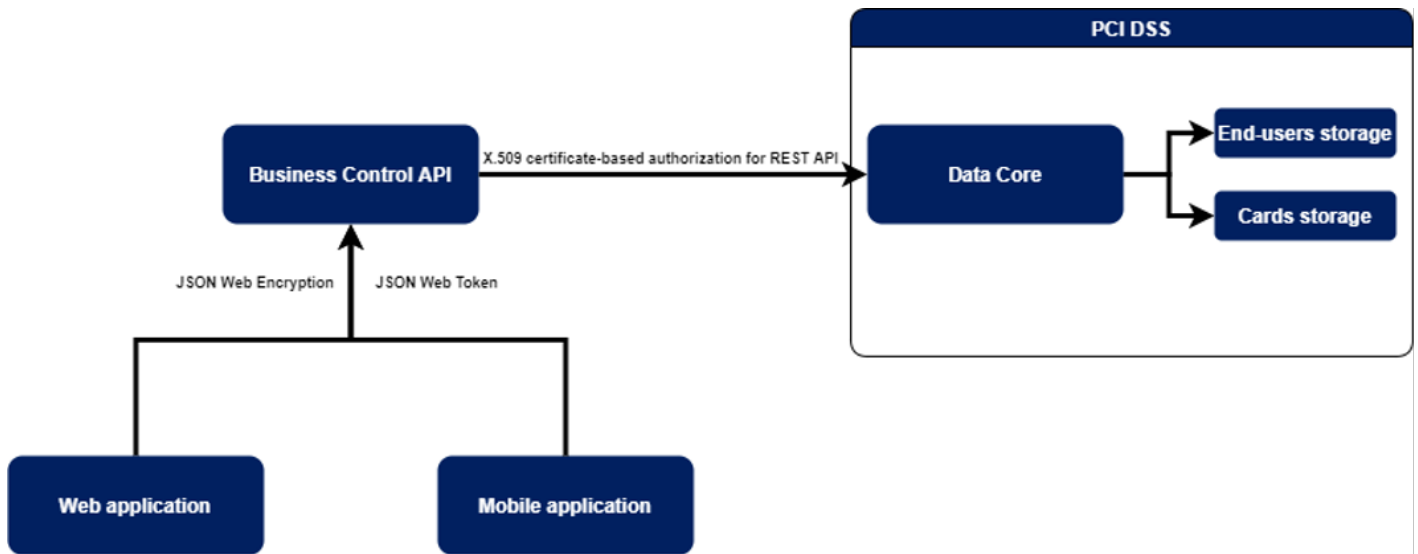- present reports for accounting purposes,
- and many more.

Security

The systems offered by Verestro are fully secure, which is confirmed by current third-party certificates. As we store card and payment data we are obliged to comply with strict legal requirements. Card data are stored in a specially designed environment - Data Core. This environment is PCI DSS certified. The PCI-DSS standard guarantees the security of payment card data. It ensures that sensitive information is properly guarded and provides maximum security in the payment process.

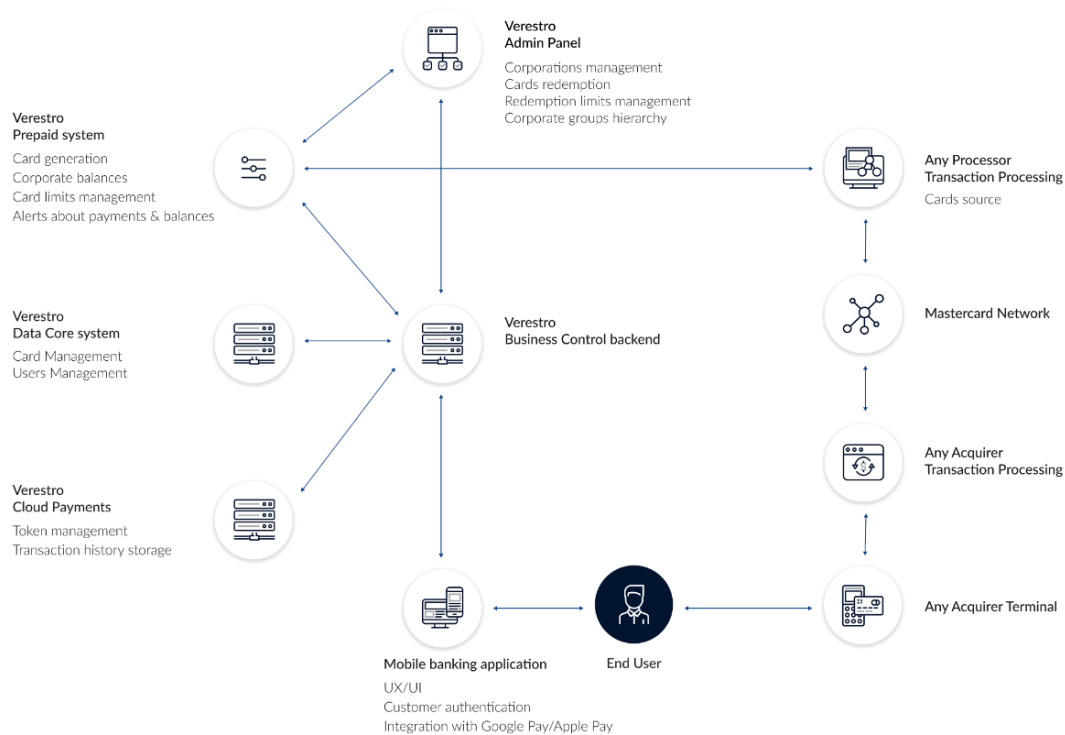We achieve high security standards by, among other things :

1.   Building and maintaining network security - the need to build and maintain a firewall configuration that protects cardholder data, not using manufacturers' default passwords and settings.

2.   Protecting cardholder data - protecting stored cardholder data, encrypting data transmissions when using public networks.

3.   Maintaining a payment management program - using regularly updated anti-virus systems, developing secure systems and applications.

4.   Implementing strong access control methods - limiting access to cardholder data to only those with a business need, assigning each user a unique ID, limiting physical access to cardholder data.

5. Regular network monitoring and testing - testing security systems and processes, controlling access to network resources and cardholder data.
6. Maintaining information security policies - relying on security policies for employees and vendors.

Architecture

Business Control uses Verestro's distributed systems to provide the highest quality of service. It is practically the best architectural solution these days. As mentioned in the previous chapter, the communication between services is completely secure, maintaining the highest security standards. This kind of system guarantees not only high efficiency, due to the division of responsibilities between the components, but also allows for easy and fast scaling of the system according to the customer's requirements.

Verestro Admin Panel

Corporations management
Cards redemption
Redemption limits management
Corporate groups hierarchy

Verestro Prepaid system

Card generation
Corporate balances
Card limits management
Alerts about payments & balances

Any Processor Transaction Processing

Cards source

Verestro Data Core system

Card Management
Users Management

Verestro Business Control backend

Mastercard Network

Verestro Cloud Payments

Token management
Transaction history storage

Any Acquirer Transaction Processing

Mobile banking application

UX/UI
Customer authentication
Integration with Google Pay/Apple Pay

End User

Any Acquirer Terminal

Access and Configuration

Access solutions

The access to Admin Portal in available in 3 ways:

- direct traffic through VPN - requires VPN reconfiguration on both sides,
- block access to the domain and allow access from a particular IP address (specific IP addresses or a range of addresses) - configuration required on Verestro side,
- free access for everyone, who have an account in Admin Portal (no matter if VPN configuration or IP address are set.

Admin Portal is available on two environments:

- test environment (dev/UAT environment),
- production environment.

    Sample of test environment (URL): https://corporate-panel-nameofclient.verestro.dev/
    Sample of production environment (URL): https:// corporate-panel-nameofclient.verestro.com/

Configuration

Time settings for individual functionalities

Business Control has a several default parameters related to the time of each action. Table below describes particular action and time related to the action.

Functionality	Description	Default time on beta environment	Default time on production environment
Operator session time.	Session after successful login to the panel.	60 minutes	15 minutes
Session reminder popup.	Time after which a popup appears asking to extend or end the session.	55 minutes	10 minutes
Mobile session time.	Session after successful login to the beta mobile application.	15 minutes	15 minutes
SMS lock time.	Determines the time after sms count will be erased and sms resend will be available.	24h	24h
Reset password OTP.	Validity of OTP during password reset process.	900s	900s

Automatic job configuration of Business Control

Functionality	Description	Default start time
Expiring outdated approvals.	The time when cards whose assignment has expired are removed from enduser.	Every full hour
Generating transaction reports.	Time when mechanism of generating reports for pending reports is starting.	Every 15th minute

Requirements for password

Functionality	Description
Mobile password length.	8-250 chars.
Portal password length.	8-30 chars.
Password (both mobile & portal) requirements .	upper-case letter, lower-case letter, special character and digit.

Mobile apps configuration

Completion of product configuration (T&C regulations, imported cards, created limits and user structures) is required to test mobile applications.

For beta environment testing, it is necessary to provide the project manager with information about the type of device and the data for which test cards are to be assigned. This is related to separate app delivery solutions for each platform.

In the case of a production environment, the application is provided by authorized and official application stores dedicated to that environment.

Beta environment

In the initial stages of the project, the mobile application can be delivered as an APK file to be installed manually on the device. It is also possible to set up an automatic distribution center for test versions, in which case it is enough to provide Verestro with a list of email addresses to which invitations to the test system will be sent. Each user will receive an individual registration link and AppTester software (a fully secure component of the Google Firebase system) or TestFlight software (Apple's standard way to distribute test applications that meet the latest functional and security requirements). Both of the distribution ways allow to download each version of the application and deliver new versions in real time to testers.
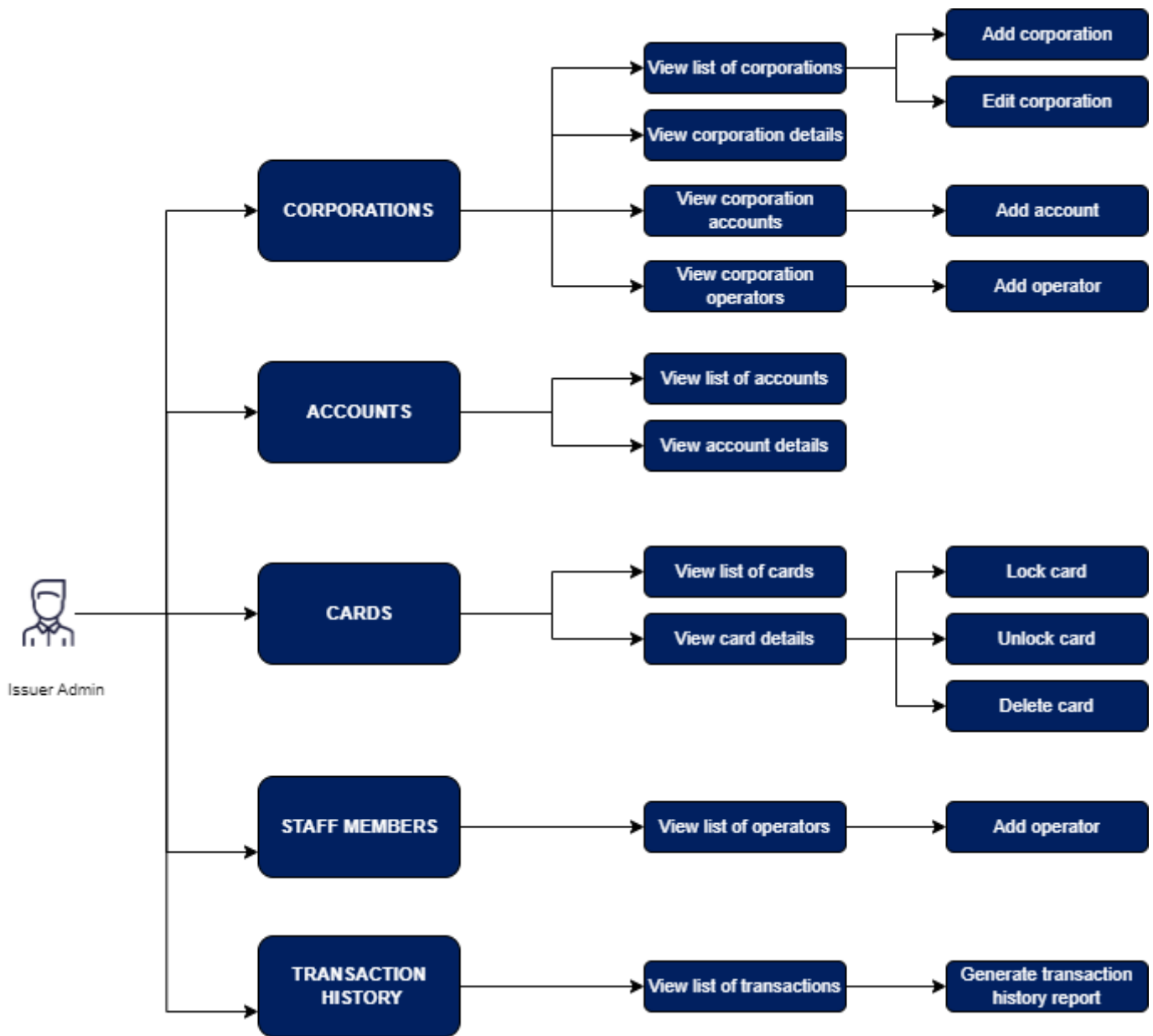
Production environment

Once the testing phase is complete, Verestro generates applications that must be signed with the appropriate set of keys and then, using procedures appropriate to the specific distribution site (Apple AppStore or Google Play), added to the app stores. Once the application is in the store, any user can easily and quickly install the application and update it automatically.

Roles in the System

Issuer Administrator

Created in the new Issuer setup process after legal and contractual issues are completed. Associated with the flow of configuring corporations related to the Issuer. Could see the corporations associated in the system and their cards along with limits.

Corporate level

The following section provides information about the actions that vary according to the level of authority in the corporate structure and key capabilities common to the roles contained in the corporation.

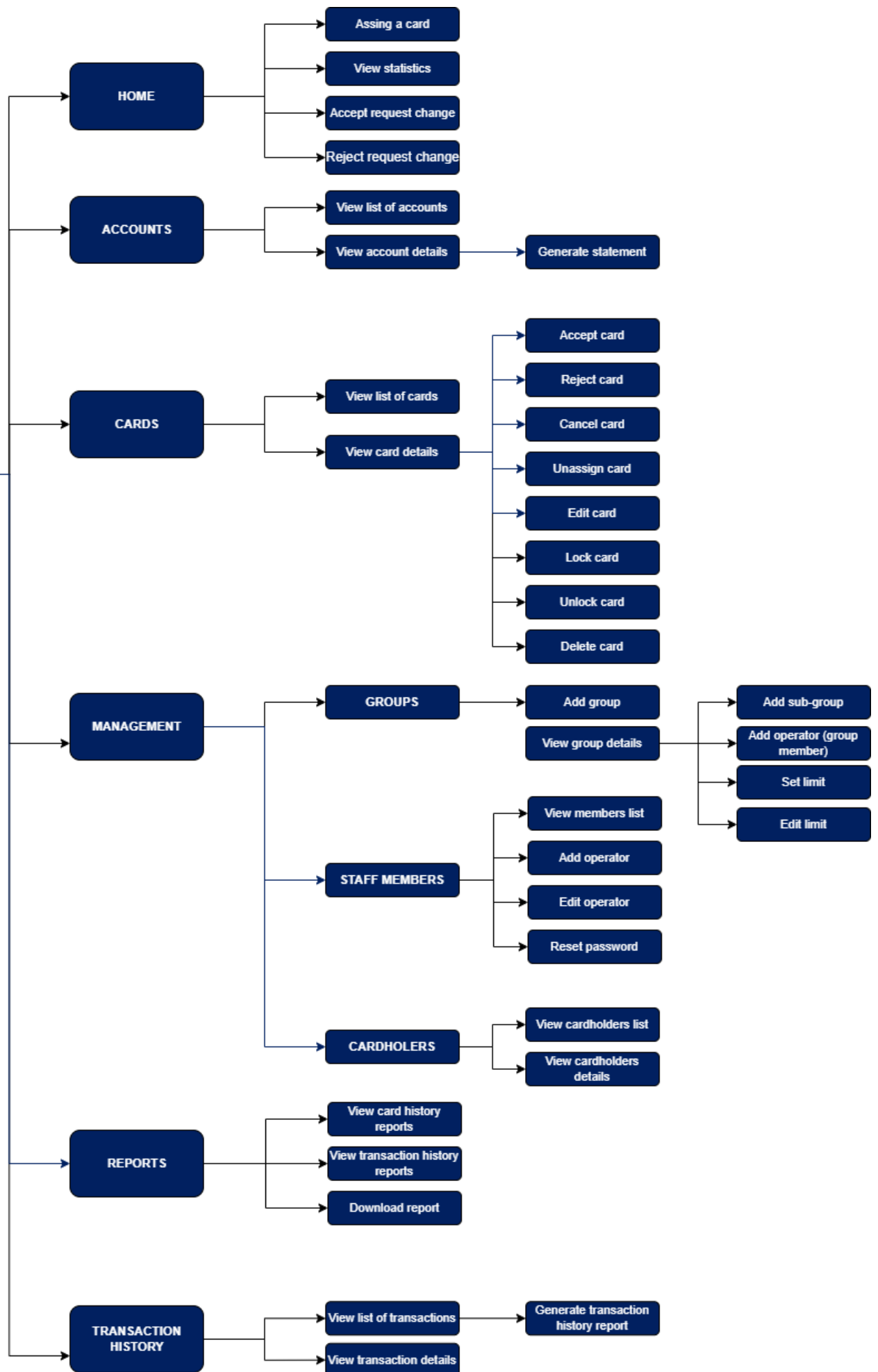| Functionality	Administrator	Manager	User
Add new corporate operator (administrator, manager, user).	Yes	X	X
Create new group.	Yes	Yes	X
View all groups.	Yes	Yes	X

View own group and groups below.	Yes	Yes	Yes
View group details, view groups members, reset password group members.	Yes	Yes	Yes
View, lock/unlock, remove from the EndUser, assigned cards from own and group below.	Yes	Yes	Yes
Assign cards.	Yes	Yes	Yes
View approvals history from own group or group below.	Yes	Yes	Yes
View awaiting card assignment from group below.	Yes	Yes	Yes
Accept/decline approval from group below.	Yes	Yes	Yes
Edit existing approval from own group.	Yes	Yes	Yes
View all assigned cards and approvals.	Yes	Yes	X
View assigned cards and approvals for own group and groups below.	Yes	Yes	Yes

As may be seen from the table above, the main differences between admin and manager concern adding new operators to the corporation. In contrast, the context of a user is usually narrowed down to its own group or actions directly related to particular user-level operator.

The manager and user roles are fully configurable. It can contain decreasing privileges in comparison to Admin or completely different functionalities.

Corporate Administrator

This is a role that guarantees full authority in the corporate context. It has access to manage the hierarchy of groups and portal operators. Corporate Administrator has a privilege to assign cards and has access to all the details of the corporation.

Corporation Admin

HOME
- Assing a card
- View statistics
- Accept request change
- Reject request change

ACCOUNTS
- View list of accounts
- View account details
  - Generate statement

CARDS
- View list of cards
- View card details
  - Accept card
  - Reject card
  - Cancel card
  - Unassign card
  - Edit card
  - Lock card
  - Unlock card
  - Delete card

MANAGEMENT
- GROUPS
  - Add group
  - View group details
    - Add sub-group
    - Add operator (group member)
    - Set limit
    - Edit limit
- STAFF MEMBERS
  - View members list
  - Add operator
  - Edit operator
  - Reset password
- CARDHOLERS
  - View cardholders list
  - View cardholders details

REPORTS
- View card history reports
- View transaction history reports
- Download report

TRANSACTION HISTORY
- View list of transactions
  - Generate transaction history report
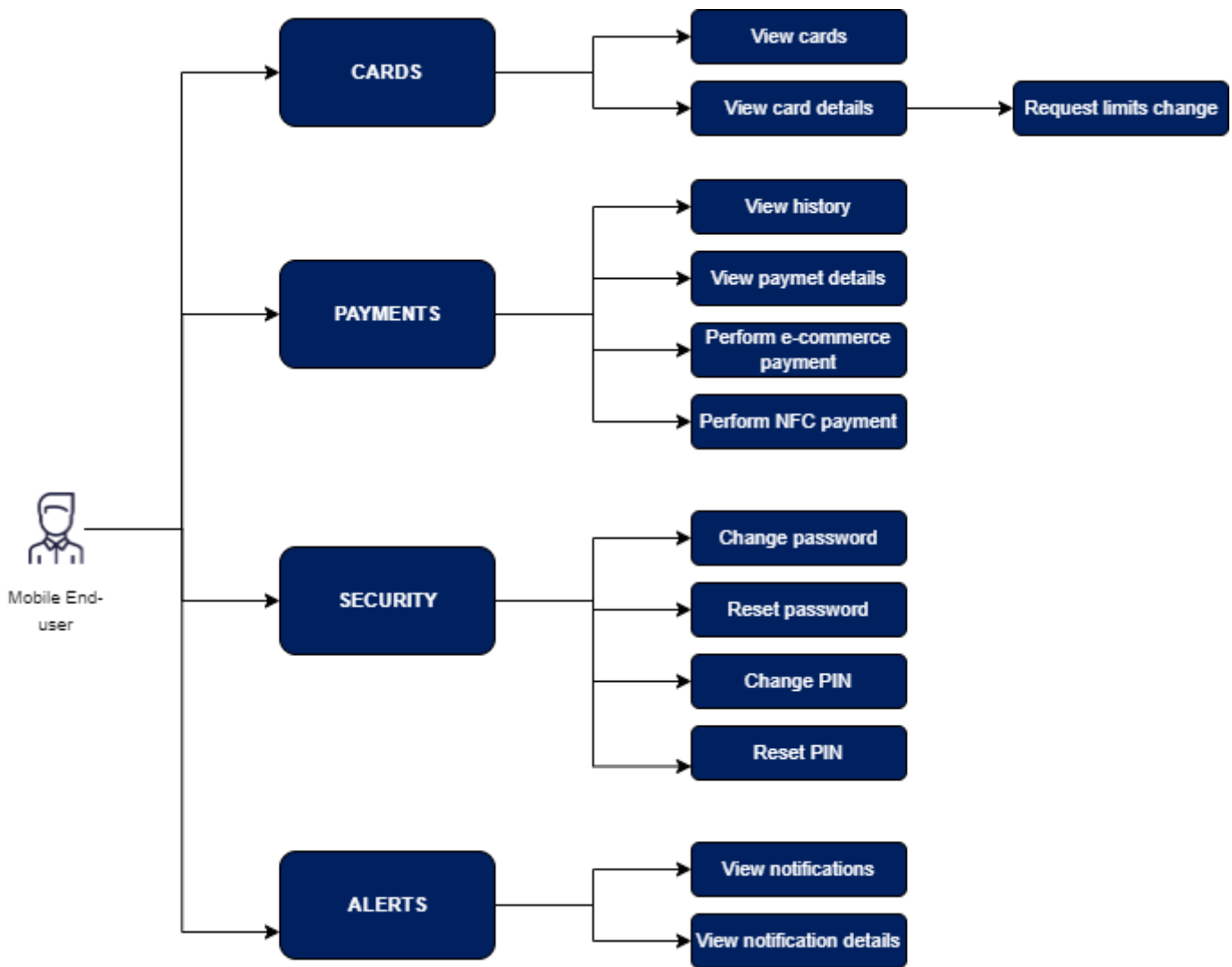- View transaction details

Corporate Manager

The role of manager in a corporation almost exactly matches with the administrator's capabilities. The difference is the inability to add new portal users.

Corporate User

The basic role in the corporation, should be assigned to a lower level user. Capabilities are limited to viewing other operators at the same permission level in their group and groups below, assigning cards, and displaying cards. That means Corporate User cannot view groups higher in the hierarchy or other users than Corporate Users in the details of group.

Mobile user - Enduser

Flow of creating the mobile user account doesn't depends on portal. End-user could install application and register without any invitation. Until the card is received from the system, it can use the mobile application capabilities. Only the assignment of the card binds him strongly to the system. Importantly, the code necessary to assign the card is sent to the phone number and e-mail address given by the portal operator on the assignment form, but the end user can redeem the code on any account (so on an account registered with different data than the one provided in the form). In such case it is required to provide the OTP code sent to the number from the form. As a result, the user can use one account for both private and corporate cards (but the authentication sent to the corporate data is required).

Notifications

This section contains all push messages and email messages that are sent in the system.

The following breakdown was used:

- emails regarding the basic functionality of the portal and sent to the operator,
- emails concerning the business processes of the product and sent to the operator,
- emails regarding the product's business processes and sent from the end-user,
- push notifications sent to the end-user.

Emails from Admin Panel to operator

Process	Topic	Details	Comment

Invitation to the system	Set password to administration panel	Hello! You are receiving this e-mail because an account was created for you, and you need to set a new password. <button to set password> Regards, <corporation>	Standard email sent when portal operator added new operator.
Login process	Login code	Hello! Your login code: <code> Regards, <corporation>	Standard AP email sent when portal operator entered correct email and password.
Reset password	Reset password to administration panel	Hello! You are receiving this mail because someone initialized password reset for your account. If it was not you, you can ignore this mail. <button to reset password> Regards, <corporation>	Standard Admin Panel email sent when portal operator uses "reset password" button on login page. In Business Control also send when portal operator uses "reset password" action on staff member row.

Emails from Business Control to operator

Process	E-mail name	Topic	Details	Comment
Approval	**BC_OPERATOR_PENDING_APPROVAL**	Request approval	Hello! There is a pending request for a card with a limit greater than allowed in requestor's administration panel group. Please log in for more detailed information. Regards, <corporation>	Email sent to higher group operator when someone from group below wants to assign card with the limit exceeded group limit.

Approval	**BC_OPERATOR_APP ROVAL_ACCEPTED**	Approval accepted	Hello! Your request to send card to <email> has been approved. You can check the details in the Administration panel. Regards, <corporation>	Email sent to requestor when someone from group higher (who is able to accept this kind of limit) accepted the approval.
Approval	**BC_OPERATOR_APP ROVAL_CANCELLED**	Approval cancelled	Hello! Your request to send card to <email> has been cancelled. You can check the details in the Administration panel. Regards, <corporation>	Email sent to requestor when someone from group cancelled the approval.
Approval	**BC_OPERATOR_APP ROVAL_REJECTED**	Approval rejected	Hello! Your request to send card to <email> has been rejected. You can check the details in the Administration panel. Regards, <corporation>	Email sent to requestor when someone from group higher (who is able to accept this kind of limit) rejected the approval.

Approval	**BC_OPERATOR_APP ROVAL_CARD_CHA NGED**	Approval card changed	Hello! Card changed on your request to send card to <email>. You can check the details in the Administration panel." Regards, <corporation>	Sent in the rare case when card have to be changed to meet the requirements (original card has expiration date earlier than approval end date).
Mobile reapproval	**BC_OPERATOR_PEN DING_MOBILE_APP ROVAL**	Request to change limits from mobile	Hello! There is a pending request to change card limits from mobile application for a card <last4digits>. Please log in for more detailed information. Regards, <corporation>	Email sent to requestor when mobile end-user sent request for changing the limit.

Emails from Business Control to end-user

Process	E-mail name	Topic	Details	Comment

Card received	**BC_USER_PENDING _CARD**	A payment card has been assigned to you.	Hello! To se the card, you must have the <corporation> Wallet application installed and an account created. Using this code in the application, you can assign the card to your account - <activationCode>. After this action you will be able to use all features of the application and make payments. Regards, <corporation>	Email sent to end-user every time when new card has been assigned.
Card adding	**BC_USER_NEW_CAR D**	A new card has been added to your account.	Hello! You are receiving this mail because a card provided by <corporation> has been added to you account. Through the <corporation>Wallet application you can monitor your available balance and completed transaction on an ongoing basis. Regards, <corporation>	Email sent to end-user when card has been properly added to the account.
Card expiring	**BC_USER_CARD_EX PIRING**	The temporary card issued to you by <corporation> is no longer valid.	Hello! The temporary card issued to you by <corporation> is no longer available for use. The card <last4digits> has been removed from your account. You do not need to take any action, this email is for awareness only. Regards, <corporation>	Email sent to end-user when assigned card is no longer valid (cancelled, locked, removed or just expired).

Card locked	**BC_USER_CARD_LOCKED**	Your card has been locked.	Your card <last4digits> issued by `<corporation>` has been blocked. Regards, `<corporation>`	Email sent to end-user when assigned card is locked.
New T&C	**BC_USER_PENDING _TERMS_AND_CON DITIONS**	New terms and conditions.	Hello! There are pending Terms and Conditions for acceptance. To keep receiving cards from Issuer, please log in and accept pending Terms and Conditions. Regards, `<corporation>`	Email sent to end-user when Issuer updated the T&C and an end-user action is required to obtain a new card. This email is send only when a new card is assigned. Even if Issuer changed T&C before and no card has been assigned the email shouldn't be send.

Push notifications from Business Control to end-user

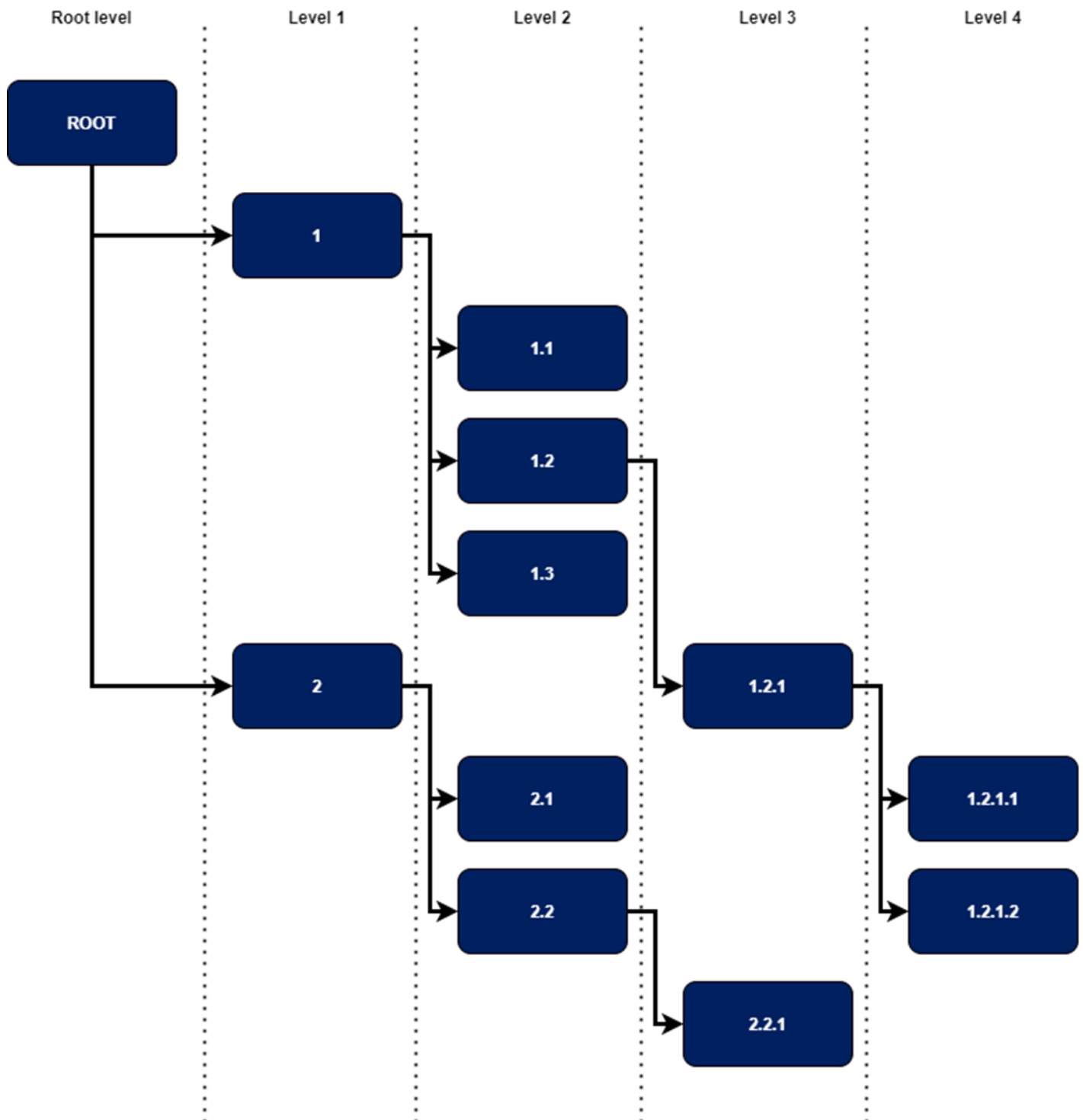| Process	Topic	Details	Comment
Card redemption	New card.	A card has been assigned to your account. Check the budget details in the app.	Push notification sent to end-user when a new card has been assigned to logged account.
Mobile approval	Mobile request to change limits reviewed and accepted.	Your request to change card limits has been reviewed and accepted. Details are available on alerts screen within mobile application.	Push notification sent to end-user when a mobile request to change limits has been reviewed to operator from original group and group higher. Basically send when double-check on portal has been made. This case is only possible when the requested limit exceeded the original group limit.

Mobile approval	Mobile request to change limits rejected.	Your request to change the assigned card limits has been rejected. Details are available on alerts screen within mobile application.	Push notification sent to end-user when a mobile request to change limits has been rejected.
Mobile approval	Mobile request to change limits accepted.	Your request to change the assigned card limits has been accepted. Details are available on alerts screen within mobile application.	Push notification sent to end-user when a mobile request to change limits has been accepted.
Transcation	Transaction declined.	Card ending <last4digits>; Purchase of <currency&amount> was attempted at <merchant> and declined per your settings.	Push notification sent to end-user when a transaction has been declined during processing.

Business Logic and Groups

This section contains all necessary information about key business processes in the system.
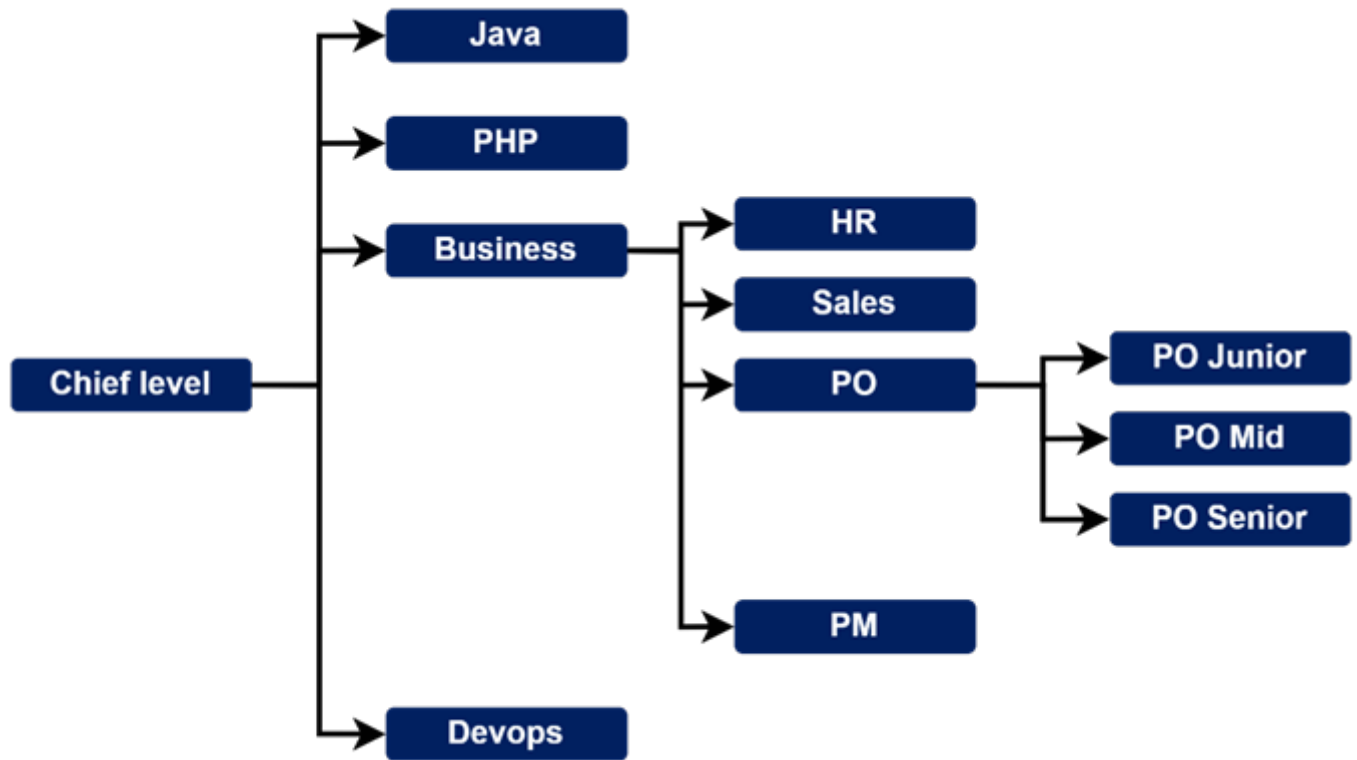
8.1 Groups

The group hierarchy always has a tree structure with one top group named Root Group. Other groups are below in the hierarchy and there can be unlimited of them on each level. There is no limit of levels or branches.

Root level	Level 1	Level 2	Level 3	Level 4

Group limits

To understand group limits, it is important to remember that these limits are related only to the card assignment process itself. They have no direct relationship to the corporation's limits. They are used to limit the ability to assign cards within the organization structure.

Sample group structure:

Assumptions

- Approval Limit - This limit determines the maximum amount with which anyone in the group can assign a card to a user.
- Spend Limit - This limit determines the maximum amount on a card that can be accepted in a given group if an assignment confirmation request comes in from a group with a lower limit.
- Cumulative limit cannot exceed Spend limit of group from which the card is assigned. If Cumulative limit during assigning to the card exceeds Spend limit then card request will send to right parent group to approve.
- PO group has Approval limit 500 and Spend limit 500.
- PO Junior group has Approval limit 200 and Spend limit 200 also.

Case	Description	Result
1 – green path	User from PO Junior group wants to assign card with limit 200 to enduser.	It is possible without additional confirmation.
2 – yellow path (direct group above)	User from PO Junior group wants to assign card with limit 300 to enduser. It is possible with additional confirmation from higher group (group with Approval limit higher or equal to 300).	Approval goes to PO group after the creation to get the confirmation.

3 - yellow path (another group above)	User from PO Junior group wants to assign card with limit 600 to enduser. It is possible with additional confirmation from higher group (group with Approval limit higher or equal to 600).	Approval goes to group which could accept the limit (higher the PO group).
4 – red path (no group to handle)	User from PO Junior group wants to assign card with limit 1600 to enduser. It is possible with additional confirmation from higher group (group with Approval limit higher or equal to 1600). In the group structure there's no group with possibility to handle this limit.	Card assignment has been declined.

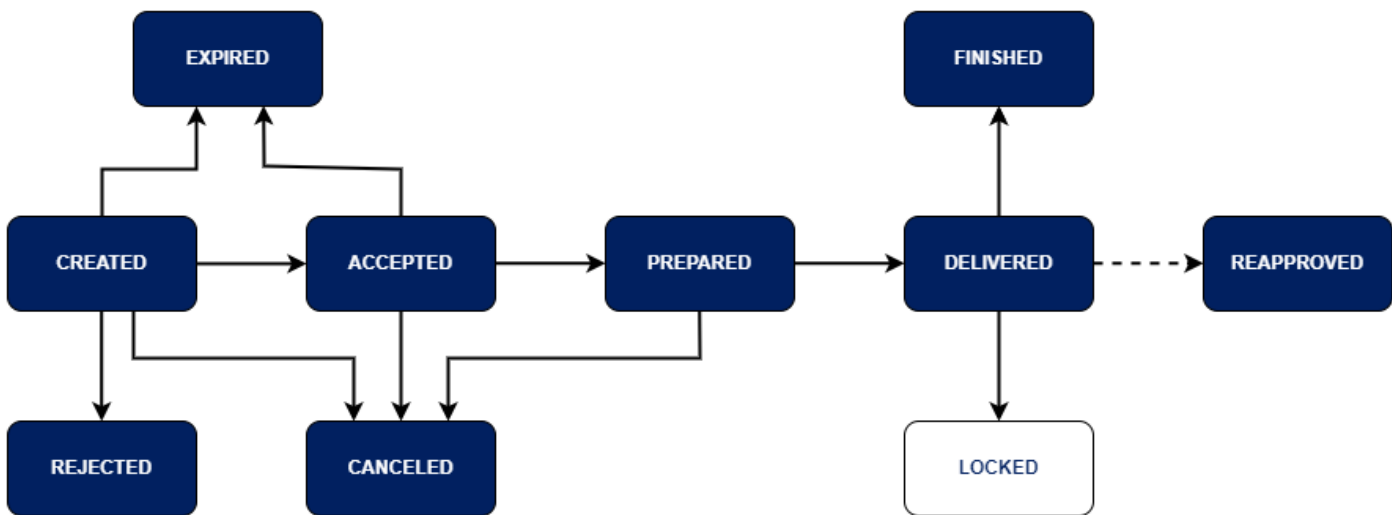# Card assignment statuses (approval statuses)

The table below contains all approval statuses that can occur in the system. Each status is described by a definition of occurrence. Knowledge of the table contents is necessary to understand the next two subsections.

Status	Description
CREATED	When an Approval is created with a limit higher than the group of the person creating it but lower than the group limit above.
ACCEPTED	When an Approval is created with a lower limit than the creator's group OR accepted by a higher group. **It changes to DELIVERED status after registration is complete and card is redeemed by end-user.**
CANCELED	When an Approval with status CREATED, ACCEPTED or PREPARED is cancelled by the anyone from creator group.
REJECTED	When an Approval with status CREATED is rejected by the group above.
EXPIRED	When an Approval with the status CREATED is not accepted/rejected or status is ACCEPTED but the card has not been redeemed by end-user within the given Approval time (until the end of the ValidTo date).
PREPARED	When approval has been ACCEPTED, redeemed by the end-user and is waiting for the start of the Approval.

DELIVERED	When an Approval is accepted and CARD REDEMPTION is created, the process of issuing the card to the end user is triggered.
FINISHED	When an Approval with status DELIVERED exceeds the end date of assignment.
REAPPROVED	When a reapproval is created for a given Approval that is in Accepted/Delivered status.
LOCKED	This is a status of a **card (not an approval)** but we display it on the diagram below to show that Delivered is the only state of a approval on which we have action to lock and unlock card.

Approval state machine

The diagram below shows Approval's state machine - that is, the states it can reach and the sequence of changing states.
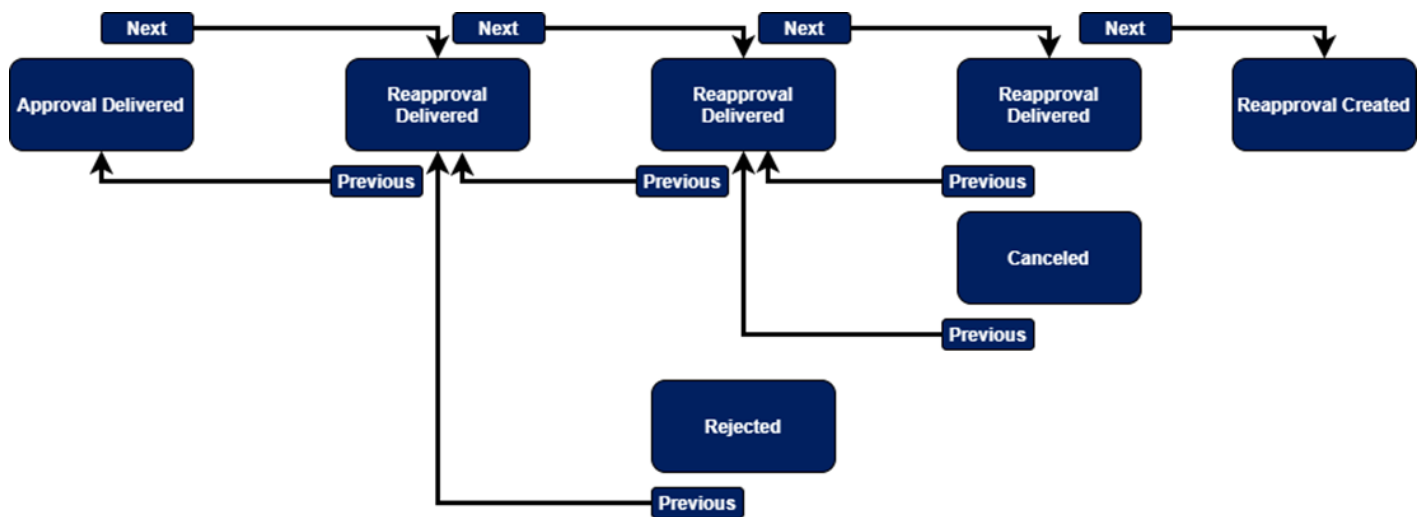

Actions available on approvals:

- Created: Accept, Reject, Edit, Cancel.
- Accepted: Cancel.
- Preprared: Cancel.
- Delivered: Lock, Unassign, Edit.
- Locked: Unlock.
- Rejected: —
- Expired: —
- Finished: —

Rules:

- **Accept** and **Reject** are available only when the request to change the limits comes from a mobile user from the same group OR when the approval creator has added an approval with an amount exceeding the group's limit.
- **Cancel** is available to approval creator and operators from creator group. The group above does not see Cancel.
- **Edit** is available to operators from creator group and operators from groups higher in the hierarchy.

Assignment lifetime flow

The way approvals are organized in flow is one line of transition from the first to the last correctly created (created) or delivered to the end user (delivered). This line can be followed by "next" and "previous". There can be branches from the main line - canceled, rejected, expired, but it is not possible to get to them via "next". There's no possibility to make a reapproval from status finished.

Card status

A card as an entity used to create a specific assignment can have different status in the system, depending on the state it is in.

Status	Description
Verified/Active	This means that the card has been correctly added to the system and can be used by assigning it to an end user.
Locked	This status indicates that the card has been manually blocked by the portal operator. There is no automated process in the system that results in the status changing to locked.

Transaction status

Status	Description
Authorized	Transaction has been authorized by the Issuer.
Declined	Transaction has been declined by the Issuer.
Cleared	Transaction has been cleared by the Issuer.
Reversed	Transaction has been reversed by the Issuer.