Standard Login and Password Authentication:

The system displays an "Authentication" form vertically divided into two sections, containing:
In the left part:

Authentication type selection menu
Tab for authentication by number, "Number"
Tab for authentication by email and password, "Email"
Tab for authentication by email and password, "Username"
Tab for authentication by account number and password, "Account Number"
Input form for "Number" or "Username" or "Email" or "Account Number" (Authentication by phone form is selected by default)
Input form for "Password"
In the right part:

Product slogan of "Rostelecom ID" account.
Auxiliary information for the customer.
When entering a phone number/email/username/account number, the authentication selection tab changes automatically.

Customer Authentication Scenario by Phone Number, "Number" Button:
The customer enters their phone number and password.
The system:

Checks the correctness of the entered number.
Validates the combination of Number + Password.
Upon successful validation of the Number and password, the system proceeds to the next step (step 3), otherwise, an error is displayed to the customer, and the scenario restarts from step 1.
In case of incorrect Number + Password combination, displays the message "Incorrect login or password," and the "Forgot Password" element changes color to orange.
The system:

Performs a successful search for the user account using the entered phone number.
Authenticates the customer.
Redirects the customer to the redirect_uri page.

Client Authentication Scenario by Email, "Email" Button:
The customer enters their email address and password.
The system:

Checks the correctness of the entered email.
Validates the combination of Email + Password.
Upon successful validation of the email and password, the system proceeds to the next step (step 3), otherwise, an error is displayed to the customer, and the scenario restarts from step 1.
In case of an incorrect Email + Password combination, displays the message "Incorrect login or password," and the "Forgot Password" element changes color to orange.
Input is limited to 12 digits, and there is a hint beneath the characters in the form of underscores.
The system:

Performs a successful search for the user account using the entered email.
Authenticates the customer.
Redirects the customer to the redirect_uri page.

Client Authentication Scenario by Account Number, "Account Number" Button:
The customer enters their account number and password.
The system:

Checks the correctness of the entered account number and searches for the associated login. In the following steps, the found login is verified.
Validates the combination of Login + Password.
Upon successful validation of the login and password, the system proceeds to the next step (step 3). If validation fails, an error is displayed to the customer, and the scenario restarts from step 1.
In case of an incorrect Login + Password combination, displays the message "Incorrect login or password," and the "Forgot Password" element changes color to orange.
The system:

Performs a successful search for the user account using the entered account number.
Authenticates the customer.
Redirects the customer to the redirect_uri page.

Password Recovery Scenario:

Password Recovery Type Selection Window:
The system displays a "Password Recovery" form containing:

Selection menu for entering contact information type
Tab for password recovery by number, "Number"
Tab for password recovery by email and password, "Email"
Tab for password recovery by username and password, "Username"
Tab for password recovery by account number, "Account Number"
Input form for "Number" or "Username" or "Email" or "Account Number" (Password recovery by phone form is selected by default)
Input form for "Captcha"

"Next" button to proceed to step 3 (Continue password recovery scenario)
If the user is only linked to a phone number, then clicking the "Number" button proceeds to the scenario for password recovery by phone using SMS.
If the user is only linked to an email, then clicking the "Number" button proceeds to the scenario for password recovery by sending an email link.
"Back" button (Return to the authentication form)
After entering the phone number, email, username, or account number, a form for password recovery options is displayed:

Option "Via SMS to Phone Number" (If phone number is linked to the account)
Option "Via Email Link" (If email is linked to the account)
"Continue" button (Proceed with password recovery scenario)
"Go Back" button (Return to step 1 for entering contact information for password recovery)
Password Recovery Scenario by Phone Number, "Via Phone Number" Option:
The user chooses to recover the password via their phone number.
The system sends an SMS with a code to the user's phone number linked to the account.
A form opens with a field for entering the code from the SMS, containing:

"Resend Code" button (Resend SMS with a new code)
"Go Back" button (Return to step 1 for entering contact information for password recovery)
Upon entering an incorrect code, an error message is displayed: "Incorrect code. Please retry."
When entering an expired temporary code, an error message is displayed: "Code has expired."
Input is limited to numbers only.
The user enters the correct verification code (proceed to step 5).
After entering the correct SMS code, a form for entering a new password opens, consisting of:

New password input field
Confirmation input field for the new password
"Save" button to confirm the new password (proceed to step 5)
Password creation rules
The user enters the new password, confirms the password, and clicks the "Save" button.
The system checks the password correctness according to the rules. If successful, the next form is displayed; otherwise, an error is displayed:

If the user enters a password less than 8 characters: "Password must be at least 8 characters long" below the "New Password" field.
If the user enters a password without uppercase letters: "Password must contain at least one uppercase letter" below the "New Password" field.
If the user enters a password with non-Latin characters: "Password must only contain Latin letters" below the "New Password" field.
If the password in the "Confirmation Password" field does not match the "New Password" field: "Passwords do not match" below the "Confirmation Password" field.
If the user enters a password according to the password policy, the system checks the entered password against the last three passwords:

If the user enters a password identical to any of the last three: "This password has already been used. Please enter a different password."
If the user enters a password different from the last three, proceed to the next step.
The client is redirected to the authentication page.

Registration Scenario:

Main Steps of the Scenario:

The client navigates to the authentication page.
The client clicks on the "Register" link.
The system displays a registration form divided vertically into two halves.
Right part contains:
Input field for first name (mandatory)
Input field for last name (mandatory)
Region selection field (mandatory)
Input field for email or mobile phone (mandatory)
Input field for password (mandatory)
Input field for confirming the password (mandatory)
"Continue" button
Links to privacy policy and user agreement
Left part contains the logo and product slogan of the dashboard.
The user fills in the first name field.
The system checks the correctness of the entered data. The input field must contain at least 2 characters consisting of Cyrillic letters or a hyphen (-).
The user fills in the last name field.
The system checks the correctness of the entered data. The input field must contain at least 2 characters consisting of Cyrillic letters or a hyphen (-).
The user selects a region from the dropdown list (default: Moscow).
The user enters an email or phone number.
The system validates the format of the entered address/phone number.
The user enters a password and confirms the password.
The system checks the correctness of the password according to the rules. If successful, proceed to the next step; otherwise, display an error:
If the password is less than 8 characters: "Password must be at least 8 characters long" below the "New Password" field.
If the password lacks uppercase letters: "Password must contain at least one uppercase letter" below the "New Password" field.
If the password contains non-Latin characters: "Password must only contain Latin letters" below the "New Password" field.
If the password in the "Confirmation Password" field does not match the "New Password" field: "Passwords do not match" below the "Confirmation Password" field.
If the password adheres to the password policy, proceed to step 9.
The user clicks the "Continue" button.
The system sends a confirmation code to the email or phone number.
The system checks all mandatory fields, validates the phone/email, and displays an error if any field does not meet the requirements.
The system checks the entered email for uniqueness. If the entered email is linked to an existing SSO account, an alert form is displayed, containing:
"Login" button - redirect to the login form.
"Recover Password" button - redirect to the password recovery form.
"x" button - close the alert popup.

The system checks the entered phone number for uniqueness. If the entered phone number is linked to an existing SSO account, an alert form is displayed, containing:
"Register" button - unlink the phone from the existing account and link it to a newly created account during registration.
"Cancel" button - close the alert form.
The system redirects the user to the page to enter the code from SMS or email, which contains:
(Masked phone number if a phone number was entered during registration)
(Masked email if an email was entered during registration)
Fields for entering the code
"Resend Code" button (Resend SMS with a new code if a phone number was entered during registration)
"Resend Email" button (Resend email with a new code if an email was entered during registration)
"Change Phone Number" button (If a phone number was entered during registration) - redirects to step 2 for entering registration data, displaying all previously entered data
"Change Email" button (If an email was entered during registration) - redirects to step 2 for entering registration data, displaying all previously entered data
Upon entering an incorrect code, an error message is displayed: "Incorrect code. Please retry."
Upon entering an expired temporary code, an error message is displayed: "Code has expired."
Input is limited to numbers only.
The user enters the correct verification code (proceed to step 13).
The user is redirected to the initiator's dashboard.