

Стандартная авторизация по логину и паролю:

- 1. Система отображает форму «Авторизация», разделенную вертикально на два блока и содержащую:
- 2. В левой части:
 - а. Меню выбора типа аутентификации
 - і. Таб выбора аутентификации по номеру, "Номер"
 - іі. Таб выбора аутентификации по логину и паролю, "Почта"
 - ііі. Таб выбора аутентификации по почте и паролю, "Логин"
 - iv. Таб выбора аутентификации по лицевому счету и паролю, "Лицевой счет"
 - b. Форма ввода "Номер" или "Логин" или "Почта" или "Лицевой счет" (По умолчанию выбрана форма авторизации по телефону)
 - с. Форма ввода "Пароль"
- 3. В правой части:
 - а. Продуктовый слоган ЛК "Ростелеком ID".
 - b. Вспомогательная информация для клиента.

При вводе номера телефона/почты/логина/лицевого счета - таб выбора аутентификации меняется автоматически.

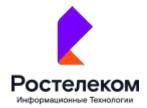
Сценарий авторизации клиента по номеру телефона, кнопка "Номер":

- 1. Клиент вводит номер телефона и пароль
- 2. Система:
 - а. Проверяет корректность введенного номера;
 - b. Проверяет связку Номер+Пароль;
 - с. При успешной проверки Номера и пароля система переходит к следующему шагу п.3., иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
 - d. При некорректном вводе связки Номер + Пароль, выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
- 3. Система:
 - а. Выполняет успешный поиск УЗ по введенному номеру телефона;
 - b. Аутентифицирует клиента;
 - с. Выполняет перенаправление клиента на страницу redirect_uri.

Сценарий авторизации клиента по номеру телефона, кнопка "Почта":

- 1. Клиент вводит Почта и пароль
- 2. Система:
 - а. Проверяет корректность введенной почты;

Исп.



- b. Проверяет связку Почта+Пароль;
- с. При успешной проверки почты и пароля система переходит к следующему шагу п.3. , иначе клиенту отображается ошибка, сценарий начинается с пункта 1
- d. При некорректном вводе связки Номер + Пароль, выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
- е. Ограничение на ввод 12 цифр и подсказка под символами в виде нижних подчеркиваний

3. Система:

- а. Выполняет успешный поиск УЗ по введенной почте;
- b. Аутентифицирует клиента;
- с. Выполняет перенаправление клиента на страницу redirect_uri.

Сценарий авторизации клиента по номеру телефона, кнопка "Логин":

- 1. Клиент вводит Логин и пароль
- 2. Система:
 - а. Проверяет корректность введенного логина;
 - b. Проверяет связку Логин+Пароль;
 - с. При успешной проверки почты и пароля система переходит к следующему шагу п.3. , иначе клиенту отображается ошибка, сценарий начинается с пункта 1
 - d. При некорректном вводе связки Номер + Пароль, выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.

3. Система:

- а. Выполняет успешный поиск УЗ по введенному логину;
- b. Аутентифицирует клиента;
- с. Выполняет перенаправление клиента на страницу redirect uri.

Сценарий авторизации клиента по номеру телефона, кнопка "Лицевой счет":

- 1. Клиент вводит Лицевой счет и пароль
- 2. Система:
- а) Проверяет корректность введенного лицевого счет и ищет логин связанный с лицевым счетом, в следующих шагах проверяется найденный логин;
- b) Проверяет связку Логин+Пароль;
- с) При успешной проверки логина и пароля система переходит к следующему шагу п.3., иначе клиенту отображается ошибка, сценарий начинается с пункта 1.
- d) При некорректном вводе связки Номер + Пароль, выводим сообщение "Неверный логин или пароль" и элемент "Забыл пароль" перекрашивается в оранжевый цвет.
- 3. Система:
- а) Выполняет успешный поиск УЗ по Лицевому счету;

Исп.



- b) Аутентифицирует клиента;
- c) Выполняет перенаправление клиента на страницу redirect uri.

Авторизация по временному коду:

- 1. Система отображает форму «Авторизация по коду», содержащую:
 - а) Подсказку по работе с формой "Укажите контактный номер телефона или почту, на которые необходимо отправить код подтверждения";
 - b) Поле ввода номера телефона или почты;
 - с) Кнопку "Получить код".
- 2. Клиент вводит номер телефона/почту и нажимает кнопку "Получить код";

3. Система:

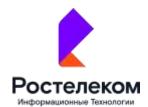
- а) Проверяет корректность введенного номера/почты;
- b) Отправляет код на введенный номер телефон/почту;
- 4. Отображает форму ввода кода подтверждения, содержащую:
- а) Номер телефона/Почту на который был отправлен код;
- b) Ссылку "Изменить номер", если пользователь ввел телефон на 2 шаге или ссылку "Изменить почту", если пользователь ввел почту на шаге 2 (ссылка ведет на форму ввода номера телефона/почты);
- с) Шесть отдельных полей для ввода кода подтверждения;
- d) Текст с обратным отсчётом времени до повторной попытки отправки код, по завершении отсчёта отображается ссылка "Получить новый код";
- 5. Клиент начинает вводить полученный код;

6. Система:

- а) После ввода каждой цифры переводит фокус ввода в следующее поле;
- b) При событии заполнения всех 6 полей производит верификацию кода;
- с) При успешной верификации кода система переходит к следующему шагу, иначе клиенту отображается ошибка, сценарий останавливается.
- d) Ограничение на ввод только цифр

7. Система:

- а) Выполняет поиск УЗ по введенному номеру телефона/почте:
 - i. Если УЗ с таким телефоном/почтой не найдена, то создает новую без пароля, ФИО, Региона после чего переход на шаг 8;
 - іі. Если УЗ найдена переход на шаг 8;
- 8. Аутентифицирует клиента;
- 9. Выполняет перенаправление клиента на страницу из redirect uri;



Восстановление пароля

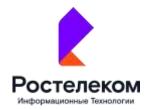
Окно выбора типа восстановления пароля:

- 1. Система отображает форму «Восстановление пароля» содержащую:
 - а. Меню выбора типа ввода контактных данных:
 - і. Таб выбора восстановления пароля по номеру, "Номер"
 - іі. Таб выбора восстановления пароля по логину и паролю, "Почта"
 - ііі. Таб выбора восстановления пароля по почте и паролю, "Логин"
 - iv. Таб выбора восстановления пароля по ЛС, "Лицевой счет"
 - b. Форма ввода "Номер" или "Логин" или "Почта" или "Лицевой счет" (По умолчанию выбрана форма восстановления пароля по телефону)
 - с. Форма ввода "Капча"
 - d. Кнопка "Далее" переход в п.3. (Продолжить сценарий восстановления пароля)
 - i. Если к УЗ привязан только телефон, то переход в Сценарий восстановления пароля клиента по номеру телефона, кнопка "По SMS на номер телефона"
 - Если к УЗ привязан только почту, то переходв Сценарий восстановления пароля клиента по номеру телефона, кнопка"По ссылке на почту"
 - е. Кнопка "Вернуться" (Вернуться на форму авторизации)
- 2. После введения телефона, почты, логина или ЛС отображается форма выбора восстановления пароля:
 - а) Выбор "По SMS на номер телефона" (Если телефон привязан к УЗ)
 - b) Выбор "По ссылке на почту" (Если почта привязана к У3)
 - с) Кнопка "Продолжить" (Продолжить сценарий восстановления пароля)
 - d) Кнопка "Вернуться назад" (Вернуться на форму ввода контактных данных п.1 для восстановления пароля)

Сценарий восстановления пароля клиента по номеру телефона, кнопка "По номеру телефона":

- 1. Пользователь выбирает восстановить по номеру телефона;
- 2. Система отправляем пользователю смс с кодом на номер привязанный к УЗ SSO;
- 3. Открывается форма с полем для ввода кода из СМС которая содержит:
 - 3.1 Кнопку "Получить код повторно" (Повторная отправка смс с новым кодом);
 - 3.2 Кнопка "Вернуться назад" (Вернуться на шаг ввода контактных данных для

Исп.



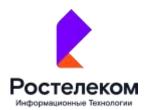
восстановления доступа);

- 3.3 При вводе неправильного кода отображается ошибка "Неверный код. Повторите попытку"
- 3.4 При вводе временного кода срок времени которого закончился отображается ошибка "Время жизни кода истекло"
- 3.5 Ограничение на ввод только цифр
- 4. Пользователь вводит корректный проверочный код (переход в п.5);
- 5. После ввода корректного кода из смс открывается форма для ввода нового пароля, состоящая из:
 - 5.1 Поле ввода нового пароля
 - 5.2 Поле ввода для подтверждения нового пароля
 - 5.3 Кнопка "Сохранить" для подтверждения нового пароля (Переход в п.5)
 - 5.4 Правила для создания пароля
- 6. Пользователь вводит новый пароль, подтверждение пароля и нажимает кнопку "Сохранить";
- 7. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка:
 - 7.1 Если пользователь ввел пароль менее 8 символов "Длина пароля должна быть не менее 8 символов" под полем "Новый пароль"
 - 7.2 Если пользователь ввел пароль без заглавных букв "Пароль должен содержать хотя бы одну заглавную букву" под полем "Новый пароль"
 - 7.3 Если пользователь ввел пароль не с латинскими буквами "Пароль должен содержать только латинские буквы" под полем <u>"Новый пароль"</u>
 - 7.4 Если пользователь ввел в поле "Подтверждение пароля" пароль отличный от пароль <u>"Новый пароль"</u> выводим "Пароли не совпадают" под полем <u>"Подтверждение пароля"</u>
- 8. Если пользователь ввел пароль согласно парольной политике, система проверяет введенный пароль с тремя предыдущими:
 - 8.1 Если пользователь ввел пароль, идентичный трем предыдущим "Этот пароль уже использовался, укажите другой пароль"
 - 8.2 Если пользователь ввел пароль, отличный от трех предыдущих переход на шаг
- 9. Клиент перенаправляется на страницу авторизации.

Сценарий восстановления пароля клиента по номеру телефона, кнопка "По e-mail":

- 1. Пользователь выбирает восстановить по почте;
- 2. Система отправляем пользователю письмо с кодом на почту привязанную к УЗ SSO;
- 3. Открывается форма с полем для ввода кода из письма которая содержит:
 - 3.1 Кнопку "Получить код повторно" (Повторная отправка письма с новым кодом);
 - 3.2 Кнопка "Вернуться назад" (Вернуться на шаг ввода контактных данных для восстановления доступа);

Исп.



- 3.3 При вводе неправильного кода отображается ошибка "Неверный код. Повторите попытку"
- 3.4 При вводе временного кода срок времени которого закончился отображается ошибка "Время жизни кода истекло"
- 3.5 Ограничение на ввод только цифры
- 4. Пользователь вводит корректный проверочный код (переход в п.5);
- 5. После ввода корректного кода из письма открывается форма для ввода нового пароля, состоящая из:
 - 5.1 Поле ввода нового пароля
 - 5.2 Поле ввода для подтверждения нового пароля
 - 5.3 Кнопка "Сохранить" для подтверждения нового пароля (Переход в п.5)
 - 5.4 Правила для создания пароля
- 6. Пользователь вводит новый пароль, подтверждение пароля и нажимает кнопку "Сохранить";
- 7. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка:
 - 7.1 Если пользователь ввел пароль менее 8 символов "Длина пароля должна быть не менее 8 символов" под полем "Новый пароль"
 - 7.2 Если пользователь ввел пароль без заглавных букв "Пароль должен содержать хотя бы одну заглавную букву" под полем "Новый пароль"
 - 7.3 Если пользователь ввел пароль не с латинскими буквами "Пароль должен содержать только латинские буквы" под полем <u>"Новый пароль"</u>
 - 7.4 Если пользователь ввел в поле "Подтверждение пароля" пароль отличный от пароль <u>"Новый пароль"</u> выводим "Пароли не совпадают" под полем <u>"Подтверждение</u> пароля"
- 8. Если пользователь ввел пароль согласно парольной политике, система проверяет введенный пароль с тремя предыдущими:
 - 8.1 Если пользователь ввел пароль, идентичный трем предыдущим "Этот пароль уже использовался, укажите другой пароль"
 - 8.2 Если пользователь ввел пароль, отличный от трех предыдущих переход на шаг
- 9. Пользователь перенаправляется на страницу авторизации.

Исп.

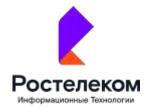


Регистрация

Основные шаги сценария

- 1. Клиент переходит на страницу авторизации;
- 2. Клиент нажимает на ссылку "Зарегистрироваться";
 - а. Система отображает форму регистрации, которая делится по вертикали на две половины;
 - b. Правая часть содержит:
 - і. Поле ввода имени (обязательное);
 - іі. Поле ввода фамилии (обязательное);
 - ііі. Поле выбора региона (обязательное);
 - iv. Поле ввода email или мобильного телефона(обязательное);
 - v. Поле ввода пароля(обязательное);
 - vi. Поле подтверждения пароля(обязательное);
 - vii. Кнопка "Продолжить";
 - viii. Ссылки на политику конфиденциальности и пользовательское соглашение;
 - с. Левая часть содержит логотип и продуктовый слоган кабинета;
- 3. Пользователь заполняет поле для ввода имени;
 - а. Система проверяет на корректность введенные данные, поле ввода должно содержать минимум 2 символа состоящих из букв кириллицы или знака тире (-);
- 4. Пользователь заполняет поле для ввода фамилии;
 - а. Система проверяет на корректность введенные данные, поле ввода должно содержать минимум 2 символа состоящих из букв кириллицы или знака тире (-)
- 5. Пользователь выбирает регион из выпадающего списка (по умолчанию Москва);
- 6. Пользователь вводит email или телефон;
 - а. Система проверяет формат введенного адреса\телефона;
- 7. Пользователь вводит пароль и подтверждение пароля;
- 8. Система проверяет корректность пароля по правилам и при успешной проверке отображается следующая форма, иначе отображается ошибка:
 - 8.1 Если пользователь ввел пароль менее 8 символов "Длина пароля должна быть не менее 8 символов" под полем "Новый пароль"
 - 8.2 Если пользователь ввел пароль без заглавных букв "Пароль должен содержать хотя бы одну заглавную букву" под полем "Новый пароль"
 - 8.3 Если пользователь ввел пароль не с латинскими буквами "Пароль должен содержать только латинские буквы" под полем "Новый пароль"
 - 8.4 Если пользователь ввел в поле *"Подтверждение пароля"* пароль отличный от пароль *"Новый пароль"* выводим *"Пароли не совпадают"* под полем *"Подтверждение*

Исп.



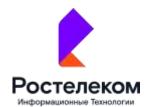
<u>пароля''</u>

- 8.5 Если пользователь ввел пароль согласно парольной политике переход на шаг 9.
- 9. Пользователь нажимает кнопку "Продолжить";
 - а. Система отправляет код подтверждения на email или телефон;
 - b. Система проверяет все обязательные к заполнению поля, валидацию телефона\email и отображает ошибку если какое-то поле не соответствует требованиям;
- 10. Система проверяет введенный email на уникальность, если введенный email привязан к имеющейся УЗ SSO, то отображается оповещающая форма, которая состоит из:
 - а) Кнопка "Войти" редирект на форму авторизации.
 - b) Кнопка "Восстановить пароль" редирект на форму восстановления пароля.
 - с) Кнопка "х" закрыть всплывающее окно оповещения.
- 11. Система проверяет введенный телефон на уникальность, если введенный телефон привязан к имеющейся УЗ SSO, то отображается оповещающая форма, которая состоит из:
 - а) Кнопка "Зарегистрироваться" телефон отвязывается от существующей УЗ и привязывается к УЗ, которая создается в процессе регистрации;
 - b) Кнопка "Отмена" закрыть оповещающую форму;
- 12. Система перенаправляет пользователя на страницу ввода кода из смс или email, которая содержит:

(Маскированный номер телефона, если введен номер телефона при регистрации) (Маскированная почта, если введена почта при регистрации)

- а) Поля для ввода кода;
- b) Кнопку "Получить код повторно" (Повторная отправка смс с новым кодом, если введен номер телефона при регистрации);
 - (Повторная отправка письма с новым кодом, если введена почта при регистрации)
- с) Кнопку "Изменить номер" (Если введен номер телефона при регистрации) (Переход на форму ввода регистрационных данных п.2, при этом необходимо отобразить все регистрационные данные, которые пользователь ввел до этого); Кнопку "Изменить почта" (Переход на форму ввода регистрационных данных п.2, при этом необходимо отобразить все регистрационные данные, которые пользователь ввел до этого);
- d) При вводе неправильного кода отображается ошибка "Неверный код. Повторите попытку"
- e) При вводе временного кода срок времени которого закончился отображается ошибка "Время жизни кода истекло"
- f) Ограничение на ввод только цифр

Исп.

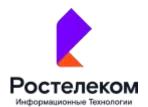


- 13. Пользователь вводит корректный проверочный код (переход в п.11);
- 14. Пользователь перенаправляется в кабинет инициатор.

Форма авторизации с настройкой (Блокировать/Отключить файлы cookie)

- 1. При переходе на страницу авторизации открывается рорир состоящий из:
- 1.1 Заглавного текста "Cookie отключены»;
- 1.2 Вспомогательной подсказки в виде «Для авторизации необходимо предоставить доступ к файлам cookie», где "cookie" это кнопка открывающая рорир с вспомогательным текстом объясняющий необходимость cookie и возможностью закрыть данный рорир;
- 1.3 Кнопка "Повторить попытку" перезагрузить текущую страницу.

Исп.

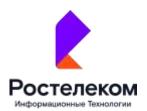


В зависимости от продукта необходимо менять атрибутивный состав форм авторизации, регистрации, восстановления пароля. Ниже перечислены продукты и таблицы с атрибутами.

| Название продукта | Ссылка |
|-------------------|-----------------------------|
| ЕЛК Web | https://lk.rt.ru/ |
| Онлайм Web | https://my.rt.ru/ |
| Старт Web | https://start.rt.ru/ |
| Умный дом Web | https://lk.smarthome.rt.ru/ |
| Ключ Web | https://key.rt.ru/ |

| | Аутентификация | | | | | | |
|------------------|----------------|----------|--------|------------|--------------------|--------------------|--|
| Продукт | | Телефон\ | | ЛС ЕЛК\ | Телефон\ | Почта\ | |
| | Пароль | Пароль | Пароль | Пароль | одноразовый код | одноразовый код | |
| ЕЛК Web | + | + | + | + | + | + | |
| Онлайм Web | + | + | + | - | + | + | |
| Старт Web | + | + | + | + | + | + | |
| Умный дом Web | + | + | + | - | + | - | |
| Ключ Web | + | + | + | - | + | + | |

Исп.



| | Регистрация | | | | |
|------------------|-------------|--------|---|---|--|
| | ФИО | ФИО | | | |
| Продукт | Телефон | Почта | Авторегистрация при входе по коду на | Авторегистрация при входе по коду на почту | |
| | Пароль | Пароль | номер телефона | влоде по коду на почту | |
| | Регион | Регион | | | |
| ЕЛК Web | + | + | + | + | |
| Онлайм Web | - | - | - | - | |
| Старт Web | + | + | + | + | |
| Умный дом Web | + | - | + | - | |
| Ключ Web | + | + | + | + | |

| Продукт | Восстановление доступа | | | |
|---------------|------------------------|-----------------------|--|--|
| | Ссылка на на почту | Код на номер телефона | | |
| ЕЛК Web | + | + | | |
| Онлайм Web | + | + | | |
| Старт Web | + | + | | |
| Умный дом Web | + | + | | |
| Ключ Web | + | + | | |

Исп.