# Войти в систему

**Цель**: вход в учетную запись.

**Актор**: неавторизованный пользователь.

**Стейкхолдеры**: отсутствуют.

**Предварительное условие**: пользователь находится на любом экране, содержащем ссылку на экран "Форма стандартной авторизации".

**Активатор**: Пользователь производит переход на экран "Форма стандартной авторизации" по кнопке или ссылке.

**Основной сценарий:**

1. Выводится форма стандартной авторизации;

2. Пользователь заполняет форму;

3. Пользователь нажимает на кнопку [Войти в кабинет];

4. Система направляет данные, введенные пользователем, в API ЛКД;

5. Система получает ответ, содержащий признаки "Все данные верны, вход разрешен", а также Token;

6. Система выводит экран установки PIN;

7. Пользователь вводит PIN;

8. Система временно фиксирует введенный PIN локально;

9. Система выводит экран подтверждения PIN;

10. Пользователь вводит подтверждение PIN;

11. Система осуществляет проверку идентичности значений PIN и Подтверждение PIN;

12. Значения из п. 11 идентичны;

13. Система локально осуществляет запись PIN, а также производит запись пары логин + пароль, если пользователь выбрал "Запомнить имя";

14. Система проверяет доступность способа авторизации Touch ID на мобильном устройстве пользователя;

15. Способ авторизации Touch ID на устройстве пользователя доступен;

16. Система выводит экран / модальное окно с предложением установить Touch ID для последующего входа в мобильное приложение;

17. Пользователь выбирает "Использовать Touch ID" (кнопка [ОК]);

18. Система осуществляет запись признака "Использовать Touch ID = true (локально);

19. Система выводит экран главный экран.

20. Конец сценария

**Альтернативный сценарий 1:**

5.1. В API возвращается ответ, содержащий признак "Требуется заполнение CAPTCHA", а также графическое изображение и хеш капчи;

5.2. Система выводит форму авторизации с включением поля "Капча";

5.3. Пользователь заполняет форму;

5.4. Пользователь нажимает [Войти в кабинет];

5.5. Система осуществляет валидацию значений, в том числе капчи.

5.6. Переход к п. 4 основного сценария.

**Альтернативный сценарий 2**

5.1.1. Получен отказ в авторизации;

5.1.2. Система выводит причину отказа (ошибка / блокировка и т.п.) в виде модального окна;

5.1.3. Пользователь закрывает модальное окно;

5.1.4. Переход к п. 1 основного сценария ИЛИ конец сценария.

**Альтернативный сценарий 3**

11.1. PIN и подтверждение PIN не совпадают;

11.2. Система выводит ошибку в модальном окне;

11.3. Пользователь закрывает модальное окно;

11.4. Переход к п. 6 Основного сценария.

**Альтернативный сценарий 4**

6.1. Пользователь нажимает [Пропустить];

6.2. Переход к п.19 основного сценария.

**Альтернативный сценарий 5**

9.1. Пользователь нажимает [Пропустить];

9.2. Переход к п.19 Основного сценария.

**Альтернативный сценарий 6**

14.1. Touch ID не доступен на пользовательском устройстве;

14.2. Система осуществляет проверку доступности способа локальной авторизации "Face ID";

14.3. Способ авторизации Face ID на устройстве пользователя доступен;

14.4. Система выводит экран / модальное окно с предложением установить Face ID для последующего входа в мобильное приложение;

14.5. Пользователь выбирает "Использовать Face ID" (кнопка [ОК]);

14.6. Система осуществляет запись признака "Использовать Face ID = true;

14.7. Переход к п. 19 Основного сценария.

**Альтернативный сценарий 7**

14.2.1. Face ID не доступен на пользовательском устройстве;

14.2.2. Переход к п.19 Основного сценария.

**Альтернативный сценарий 8**

14.4.1. Пользователь отказывается от использования Face ID;

14.4.2. Система осуществляет запись признака "Использовать Touch ID = false (локально);

14.4.3. Переход к п.19 Основного сценария.

**Альтернативный сценарий 9**

16.1. Пользователь отказывается от использования Touch ID;

16.2. Система осуществляет запись признака "Использовать Touch ID = false (локально);

16.3 Переход к п.25 Основного сценария.

# Включить уведомления

**Цель**: активация PUSH-уведомлений на пользовательском устройстве;

**Актор**: авторизованный пользователь;

**Стейкхолдеры**: отсутствуют;

**Предварительное условие 1**: у пользователя отключены PUSH-уведомления;

**Предварительное условие 2**: пользователь находится на экране "Настройки";

**Активатор**: пользователь меняет положение селектора (свитча) "PUSH-уведомления". Новое положение: ON.

**Основной сценарий:**

1. Система изменяет вид селектора (свитча) на положение ON;
2. Система активирует возможность получения уведомлений (только на текущем пользовательском устройстве);
3. Конец сценария.

**Альтернативные сценарии:** отсутствуют**.**

# Зарегистрировать обмен оборудования

**Цель**: обмен оборудования, связанного с действующим договором.

**Актор**: авторизованный пользователь.

**Стейкхолдеры**: абонент.

**Предварительное условие**: пользователь находится в главном меню

**Активатор**: Пользователь нажимает на пункт меню [Обмен]

**Основной сценарий:**

1. Система выводит форму ввода ID текущего оборудования;
2. Пользователь вводит ID;
3. По мере ввода Система производит валидацию по общим правилам и маскам: значение валидно;
4. Кнопка [Найти] становится активна;
5. Пользователь нажимает [Найти];
6. Система направляет запрос в API на проверку ID;
7. Система получает ответ: ID найден, обмен разрешен;
8. Система выводит форму для ввода данных об абоненте, ID нового оборудования и выбора подарков при наличии акции;
9. Пользователь заполняет форму;
10. По мере ввода Система производит валидацию по общим правилам и маскам: значения валидны;
11. Кнопка [Продолжить] становится активной;
12. Пользователь нажимает [Продолжить];
13. Система направляет запрос в API;
14. Система получает ответ: ввод секретного номера скретч-карты / индивидуального номера смарт-карты не требуется;
15. Система направляет в API данные для обмена;
16. Система получает ответ: Обмен выполнен;
17. Система выводит экран "Успешный обмен"

**Альтернативный сценарий 1:**

2.1. По мере ввода Система производит валидацию по общим правилам и маскам: значение НЕ валидно;

2.2. Система выводит ошибку под полем с ошибкой;

2.3. Переход к шагу 2 Основного сценария.

**Альтернативный сценарий 2:**

6.1. Система получает ответ: ID НЕ найден, обмен невозможен;

6.2. Система выводит ошибку в модальном окне;

6.3. Пользователь закрывает модальное окно;

6.4. Переход к шагу 2 Основного сценария.

**Альтернативный сценарий 3:**

9.1. По мере ввода Система производит валидацию по общим правилам и маскам: одно или несколько значений НЕ валидны;

9.2. Система выводит ошибку под соответствующими полями;

9.3. Переход к шагу 9 Основного сценария.

**Альтернативный сценарий 4:**

13.1. Система получает ответ: требуется ввод секретного номера скретч-карты / индивидуального номера смарт-карты;

13.2. Система выводит экран ввода секретного / индивидуального номера;

13.3. Пользователь вводит данные;

13.4. По мере ввода Система производит валидацию по общим правилам и маскам: значение валидно;

13.5. Система направляет в API запрос на проверку секретного / индивидуального номера;

13.6. Система получает ответ: значение верное;

13.7. Переход к шагу 15 Основного сценария.

**Альтернативный сценарий 4.1:**

13.3.1. По мере ввода Система производит валидацию по общим правилам и маскам: значение НЕ валидно;

13.3.2. Система выводит ошибку под соответствующим полем;

13.3.3. Переход к шагу 13.3 Альтернативного сценария 4

**Альтернативный сценарий 4.2:**

13.5.1. Система получает ответ: значение НЕ верное;

13.5.2. Система выводит ошибку в модальном окне;

13.5.3. Пользователь закрывает модальное окно;

13.5.4. Переход к шагу 13.3 Альтернативного сценария 4.

**Альтернативный сценарий 5:**

15.1. Система получает ответ: ошибка;

15.2. Система выводит сообщение об ошибке в модальном окне;

15.3. Пользователь закрывает модальное окно;

15.4. Переход к шагу 8 Основного сценария.