**Сводка по back-channel logout:**

1. **Событие в Keycloak:** Когда второй пользователь успешно логинится и User Session Count Limiter помечает старую сессию как недействительную, Keycloak генерирует событие "logout" для этой старой сессии.
2. **Уведомление ЛК:** Если для клиента вашего ЛК в Keycloak настроен Back-Channel Logout, Keycloak отправит подписанный **Logout Token** (специальный JWT) на заранее сконфигурированный URL вашего бэкенда ЛК. Этот запрос идет напрямую от сервера Keycloak к серверу ЛК (поэтому "back-channel").
3. **Обработка в ЛК:** Ваш бэкенд ЛК должен:
   * Принять этот POST-запрос от Keycloak.
   * Валидировать подпись Logout Token'а, используя публичные ключи Keycloak.
   * Извлечь из токена идентификатор сессии Keycloak (sid) или идентификатор пользователя (sub), которая была завершена.
   * Найти соответствующую *активную сессию пользователя в ЛК* (по sid или sub) и немедленно ее завершить (удалить из хранилища сессий ЛК).
4. **Результат:** Как только бэкенд ЛК завершит сессию, при следующей попытке пользователя в *первом* браузере выполнить какое-либо действие, требующее активной сессии в ЛК (переход по ссылке, запрос к API), ЛК обнаружит, что сессия недействительна, и перенаправит пользователя на страницу входа. Это произойдет *гораздо быстрее*, чем ожидание истечения Access Token'а.

**Как реализовать:**

**Шаг 1: Настройка в Keycloak (для клиента вашего ЛК)**

1. Перейдите в вашу Realm -> Clients -> ваш клиент ЛК.
2. Найдите секцию "OpenID Connect Compatibility Modes" или подобную (в новых версиях интерфейс может немного меняться, ищите настройки Logout).
3. Включите опцию **"Backchannel Logout URL"**.
4. Укажите **абсолютный URL** на вашем бэкенде ЛК, который будет принимать Logout Token от Keycloak. Например: https://my-lk-backend.com/api/v1/auth/keycloak/logout.
5. Убедитесь, что опция **"Backchannel Logout Session Required"** включена. Это заставит Keycloak включать sid (Session ID) в Logout Token, что упростит поиск нужной сессии на стороне ЛК.
6. Опцию "Backchannel Logout Revoke Offline Sessions" обычно можно оставить выключенной, если вы не используете offline токены специфичным образом, требующим их отзыва при logout.
7. Сохраните изменения.

**Шаг 2: Реализация обработчика на бэкенде ЛК**

Вам нужно создать эндпоинт (например, /api/v1/auth/keycloak/logout), который будет:

1. **Принимать POST-запросы:** Keycloak будет отправлять POST-запрос с Content-Type: application/x-www-form-urlencoded.
2. **Извлекать Logout Token:** Токен будет передан в параметре logout\_token.
3. **Валидировать Logout Token (JWT):** Это **критически важный** шаг для безопасности.
   * Используйте библиотеку для работы с JWT для вашего языка/фреймворка.
   * Получите публичные ключи Keycloak (обычно доступны по URL вида https://your-keycloak.com/realms/your-realm/protocol/openid-connect/certs). Кешируйте их, но предусмотрите механизм обновления.
   * **Проверьте подпись** токена, используя полученные ключи и алгоритм, указанный в заголовке токена (обычно RS256).
   * **Проверьте iss (issuer):** Должен совпадать с URL вашего реалма Keycloak.
   * **Проверьте aud (audience):** Должен содержать Client ID вашего ЛК.
   * **Проверьте, что это действительно Logout Token:** В нем должно быть поле events с объектом, содержащим ключ "http://schemas.openid.net/event/backchannel-logout": {}. Также может присутствовать typ: "Logout".
   * **Проверьте iat (issued at):** Убедитесь, что токен не слишком старый (защита от replay-атак). У Logout Token нет exp, он валиден короткое время.
   * **Запретите nonce:** В Logout Token не должно быть поля nonce.
4. **Извлечь sid:** Получите значение поля sid из payload'а токена. Это идентификатор сессии Keycloak, которая была завершена.
5. **Найти и завершить сессию ЛК:**
   * Нужен механизм, который при логине пользователя в ЛК сохраняет соответствие между сессией ЛК и sid сессии Keycloak (этот sid можно получить из ID Token'а при логине).
   * Используя sid из Logout Token'а, найдите соответствующую активную сессию в вашем хранилище сессий ЛК (Redis, база данных, память сервера и т.д.).
   * Удалите/инвалидируйте эту сессию ЛК.
6. **Ответить Keycloak:** Отправьте ответ HTTP 200 OK. Если Keycloak не получит успешный ответ, он может попытаться повторить отправку.

**Уведомление фронтенда**

Даже с Back-Channel Logout, пользователь в старом браузере узнает о logout'е только при следующем действии. Чтобы сделать это еще более "мгновенным", после того как бэкенд ЛК завершил сессию по сигналу от Keycloak, он может:

* Использовать **WebSockets** или **Server-Sent Events (SSE)**, чтобы отправить сообщение на фронтенд этой конкретной сессии, заставляя его немедленно показать сообщение о logout'е или перенаправить на страницу входа.