

Требования к приложению

Требования к приложению Wallenc

1.2 Анализ предметной области (выдержка)

В рамках анализа предметной области рассмотрены подходы к хранению чувствительных данных в мобильных приложениях и облачных хранилищах. Выделены требования: конфиденциальность при хранении и передаче; отсутствие необходимости доверять инфраструктуре хранилища; устойчивость к компрометации удалённого провайдера; разделение логики хранения и криптографической защиты; удобные сценарии создания хранилища, шифрования, открытия и работы с содержимым.

Сформирован вывод о приоритете клиентских криптографических механизмов, унифицированного доступа к разным типам хранилищ и архитектуры с чётким разделением слоёв.

1.3 Разработка требований к программному продукту

1.3.1 Назначение и цели создания системы

Назначение системы Wallenc — предоставление пользователю мобильного клиента для работы с иерархией **VaultsManager** → **vault** → **storage** → **файлы**: один LocalVault на устройстве, удалённые vault по OAuth; внутри vault пользователь создаёт и управляет **storage**; шифрование (StorageEncryptionInfo, Encryptor) применяется к storage, а не к vault.

Цели создания: обеспечить единую модель vault и storage; минимизировать доверие к провайдеру; поддерживать расширение списка провайдеров через адаптеры; сохранить служебные метаданные в локальной БД без хранения пользовательского контента в открытом виде.

1.3.2 Функциональные требования

Функциональные требования сведены в таблице Таблица 1.

Таблица 1. Свод функциональных требований

Код	Требование
ФР-1	Создание, просмотр, переименование и удаление storage в локальном vault (LocalVault — один на устройстве)
ФР-2	Включение шифрования storage, проверка ключа, открытие и закрытие зашифрованного представления
ФР-3	Просмотр и операции с файлами внутри storage; текстовые секреты и 2FA
ФР-4	OAuth-авторизация (Яндекс), регистрация удалённых vault и листинг их storage
ФР-5	Синхронизация: группы хранилищ, журнал коммитов, фоновый Worker без передачи ключей
ФР-6	Очередь фоновых задач: шифрование, синхронизация, отображение прогресса

1.3.2.1 Управление storage в локальном vault

Пользователь создаёт storage, просматривает список, переименовывает и удаляет их в единственном LocalVault. Служебные каталоги и системные пути не отображаются в пользовательском представлении.

1.3.2.2 Шифрование и открытие storage

При включении шифрования формируются параметры StorageEncryptionInfo; открытие выполняется только после успешной проверки ключа. Повторное шифрование одного storage до завершения предыдущей операции блокируется.

1.3.2.3 Работа с содержимым storage

Операции чтения и записи выполняются через единый интерфейс файлового доступа независимо от типа хранилища. Внутри открытого storage доступны текстовые секреты и генерация TOTP для 2FA.

1.3.2.4 Удалённые хранилища и авторизация во внешних провайдерах

Реализован поток OAuth 2.0 для Яндекса.

1.3.2.5 Синхронизация зашифрованных данных

Спроектирован механизм фоновой синхронизации: в Room хранятся записи с UUID хранилищ; по таймеру запускается сервис, сравнивающий истории коммитов локального и удалённого представления без передачи ключей на сервер провайдера.

1.3.3 Нефункциональные требования

К системе предъявляются требования по производительности (асинхронные операции на Coroutines), безопасности (AES на клиенте, минимизация утечек через имена путей), расширяемости (модульная структура Gradle) и устойчивости к гонкам при длительных операциях шифрования.

1.3.4 Требования к программно-аппаратной платформе

Минимальная платформа — Android с поддержкой Jetpack Compose; для OAuth и удалённых операций требуется сетевое подключение. Объём оперативной памяти должен быть достаточен для фоновых задач шифрования и Room.

1.4 Сравнение аналогов (обоснование требований)

Таблица 2. Сравнительная оценка аналогов

Критерий	Secure Folder	Proton	Bitwarden	Cryptomator	Wallenc
Собственный backend приложения	—	+	+/-	—	—
E2E / клиентское шифрование	+/-	+	+	+	+
Файловый vault	+	+	—	+	+
OAuth внешнего провайдера	—	+/-	+/-	+/-	+
Переносимость провайдеров	—	—	+/-	+	+
Unit-тесты без сервера	н/д	н/д	+/-	+/-	1. (68)

По итогам сравнения аналогов сформированы функциональные требования ФР-1...ФР-6 и нефункциональные ограничения, отражённые в таблице Таблица 1.