

# Crypto Bunker

Централизованное управление децентрализованными секретами

#### Проблематика

- Пользователям и сервисам надо аутентифицироваться
- Разрозненные системы настройки аутентификации
- Хранение и передача секретов в открытом виде

Текущее решение: Hashicorp Vault

- Не любит русских
- На CI/CD секреты в открытом виде
- Секреты утекают через образы контейнеров

### Наши технологии: фреймворк \$mol

- Самая продвинутая система реактивности
- Микромодульная архитектура
- Богатая библиотека готовых решений
- Высокая степень настраиваемости

#### Наши технологии: база данных CRUS-DB

- Секреты никогда не передаются в открытом виде
- Синхронизация безопасна даже по ненадёжным каналам
- Секреты синхронизируются в реальном времени
- Секреты всегда доступны локально
- Самовосстановление бд с других узлов

#### Наша архитектура

- При первом запуске создаётся приватный ключ и сохраняется локально
- Владелец секрета выдаёт права для публичного ключа
- База данных в фоне синхронизируется через любой сервер синхронизации
- Если у сервиса есть права, то он сможет расшифровать секрет из локальной реплики

## Соответствие требованиям

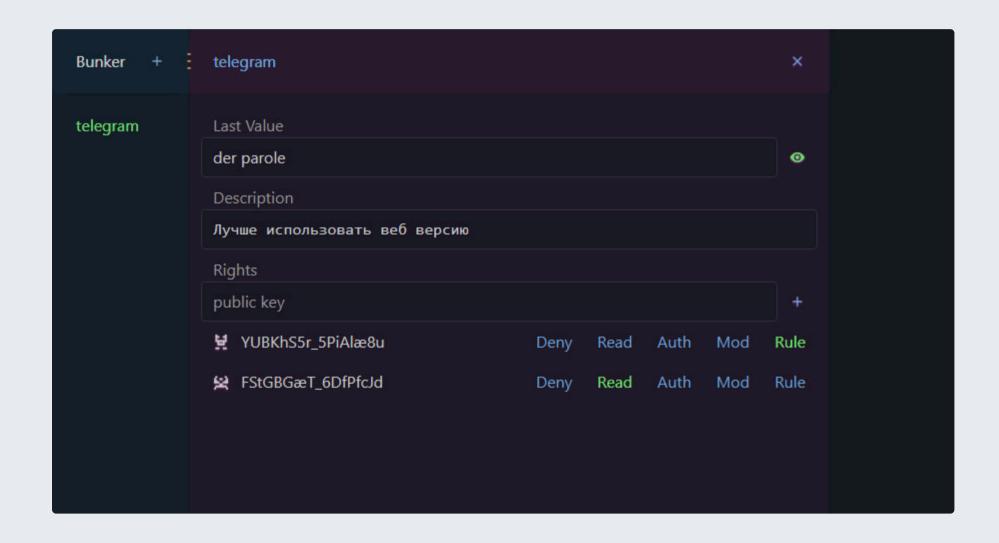
Требование	Наши улучшения
Клиент-серверное взаимодействие по API	✓ Пиринговая сеть со своим протоколом
Нулевое доверие между узлами	Авторизация всех входящих изменений
💢 Только защищённые каналы связи	
<b>Х</b> Аутентификация через сторонние сервисы	
💢 Журналирование доступа	☑ Предоставление доступа через запись в БД
Высокая доступность и масштабирование	✓ Local-First архитектура

- Иультитенантность
- Иифрование
- High Availability
- **Disaster Recovery**
- Active-Active
- 🗸 Аудит доступа
- 🗸 🕸 Мониторинг ресурсов
- 🔽 Работа в оффлайне
- И Синхронизация в реальном времени
- 🔽 Самовосстановление данных
- ✓ ⊕ WEB-UI

- 💢 Версионирование
- 💢 Запечатывание
- 💢 Политики
- ★ REST API
- 💢 Генерация секретов
- 💢 Интеграция с облаками
- 💢 Интеграция с CI/CD
- 💢 Многофакторная аутентификация

#### Дорожная карта

- Иерархия секретов с наследованием прав
- Версионирование секретов
- Local-Only REST API
- Интеграция с Kubernetes
- Реализации для разных языков помимо TS



#### Варианты использования

- Индивидуальное хранение паролей
- Шаринг паролей с коллегами
- Автоматическая загрузка секретов в сервисы

#### Команда

- Дмитрий Карловский тимлид, фронт
- Станислав Яременко бэкенд
- Павел Зубков девопс
- Екатерина Амельчакова дизайн, преза, маскот
- Кристина Гарас дизайн

