BYOK

bring your own key

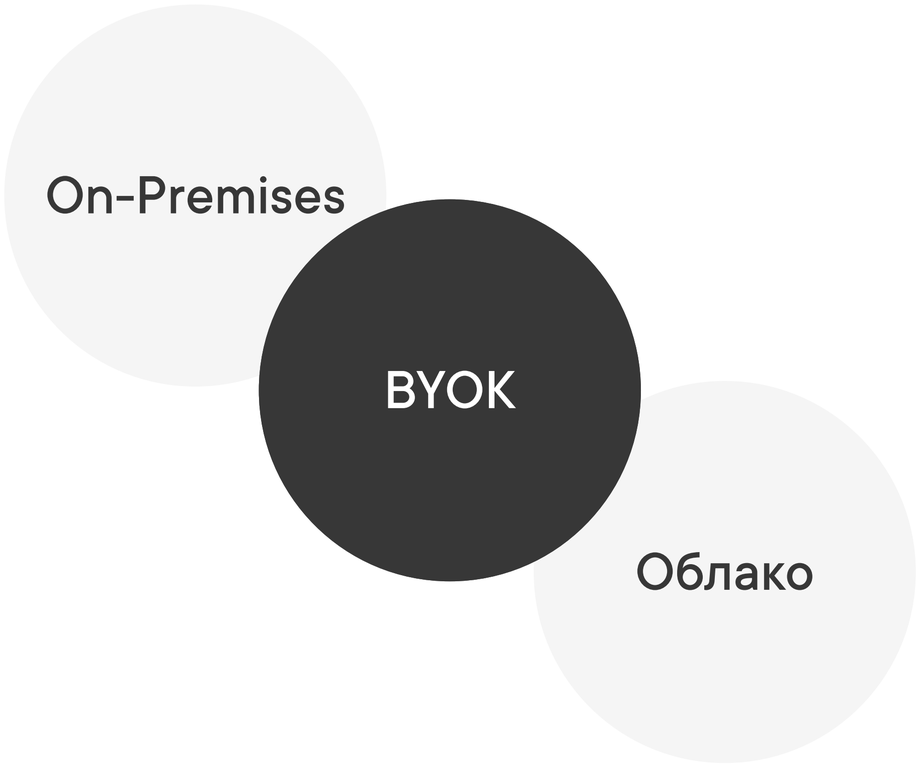
Пачка

rT9mA3sL6vB2nE8bQ4zR7wK1jX5t
M9oBbringiL8rN4cU7xD3mP6sS1zO
5fH9kJ2wG8rY4pB7kM1nT6vI3qC9
bR5zsK7nB1rM4vQ8qA5bO2zP6wF3
hT9tG7oY4pU1iN8rL3dO6xC5mK2s
R9zN7fJ4lM8wH2rY6pA1kO3nV9vH
5qD2bS8ztL4mC8rN1vS5nB2bPKzQ
3wE6hU7tH4eX1pW5iO2rNEcV4xD7

Стандарт безопасности SAAS-сервисов

Bring your own key

bring your own encryption



BYOK (BYOE) — гибридное решение между on-premise и облаком: вы сохраняете полный контроль над данными без необходимости разворачивать и обслуживать собственную инфраструктуру.

Данные хранятся на стороне Пачки, но шифруются вашими ключами. Доступ к их обработке невозможен без вашего разрешения и не сможет пройти незаметно для систем мониторинга.

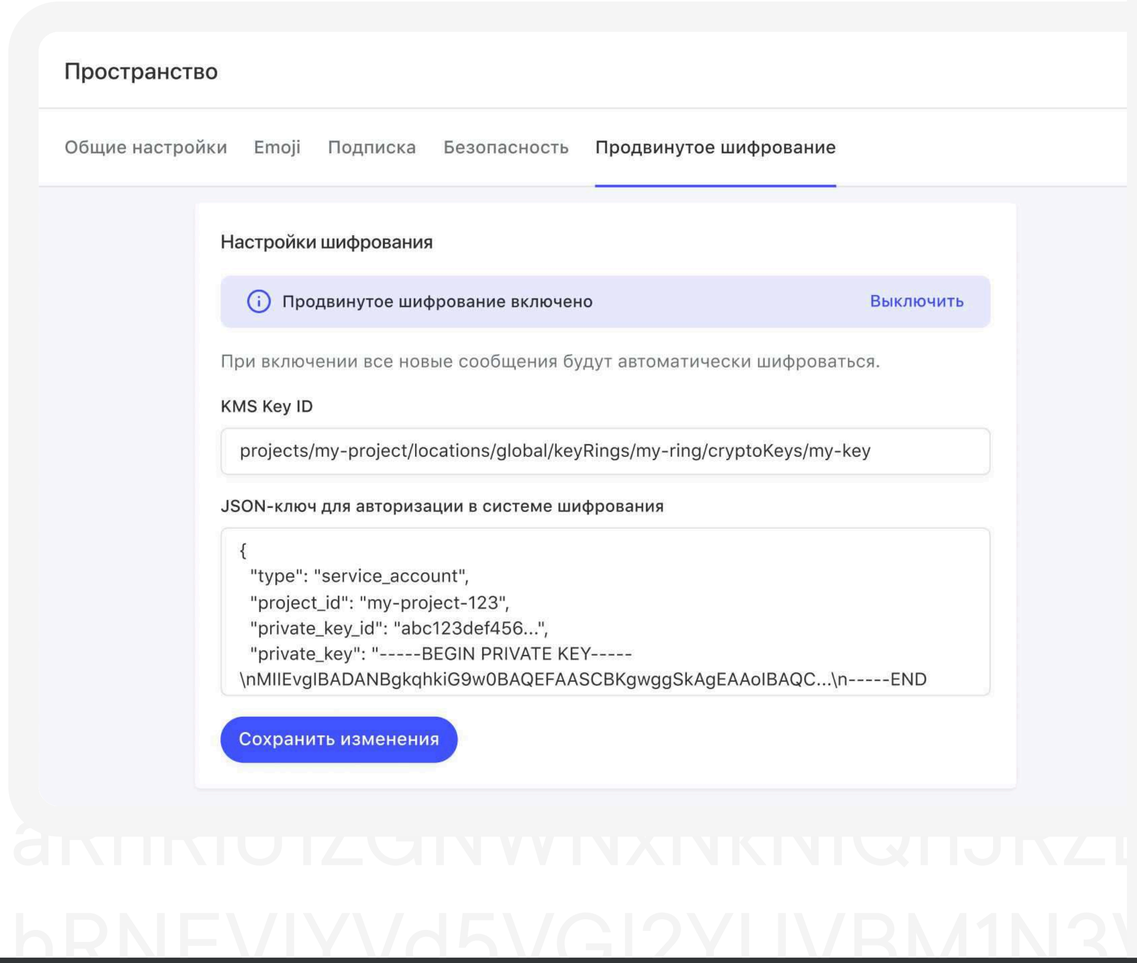
Проверенный стандарт на мировом рынке

Подход BYOK более 10 лет используют государственные и оборонные организации во всем мире.

Для его работы необходимо KMS (Key Management Service) решение. Оно управляет ключами для шифрования сообщений на стороне клиента.

Сами KMS-системы популярны в России: их использует более 90% технологический компаний для разных задач, а крупные разработчики предоставляют свои решения. Например, Яндекс KMS и Cloud.ru.

Как это работает?

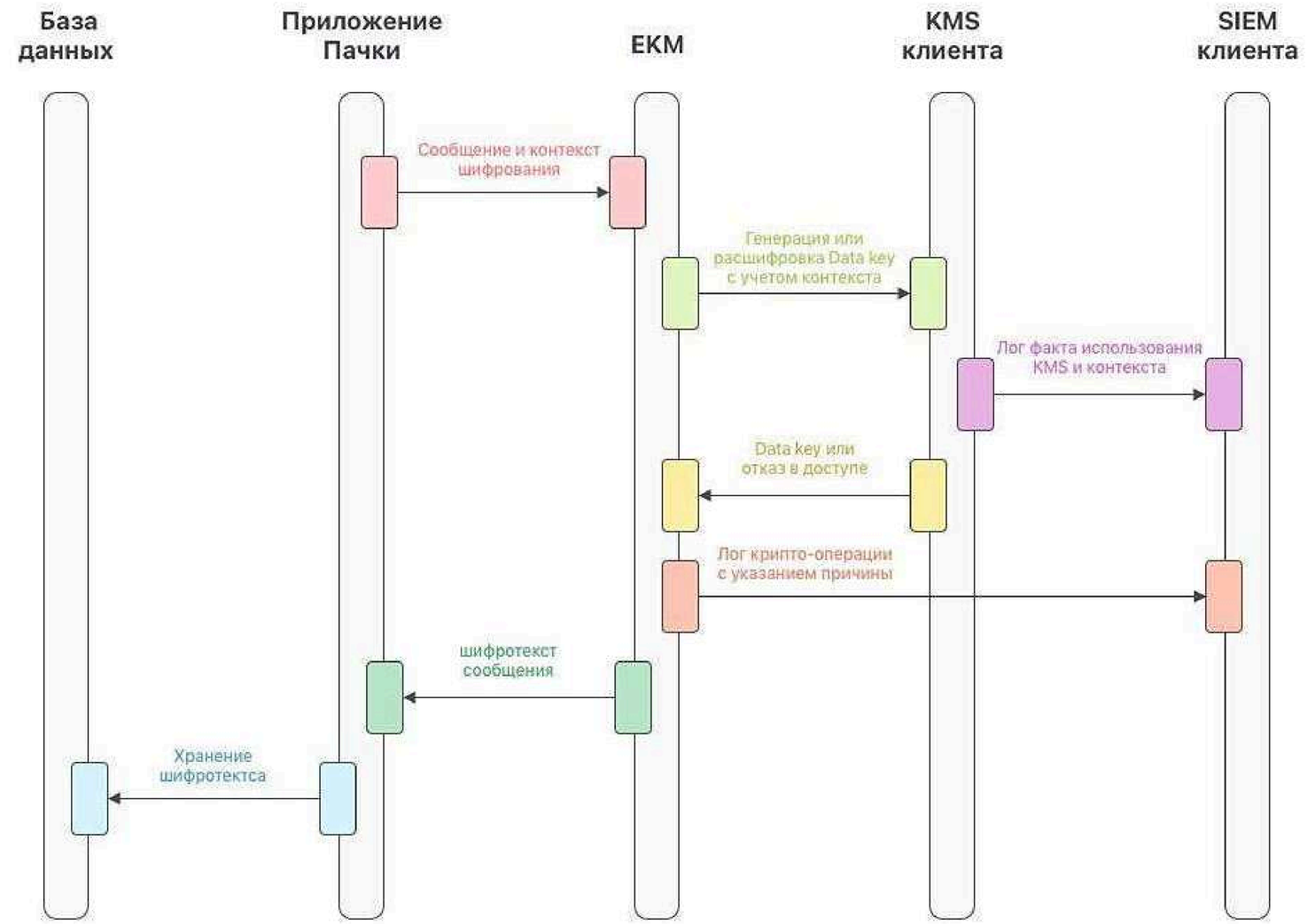


Внутри вашей инфраструктуры работает KMS (Яндекс KMS, Cloud.ru или HashiCorp Vault), которая выдаёт Пачке ключи для шифрования сообщений при отправке.

После того, как сообщения зашифровали, то ключи расшифровки удаляются на стороне Пачки. Без этих ключей у мессенджера остаётся лишь набор зашифрованных данных.

Расшифровать сообщения можно только с вашего разрешения. А все запросы на эту операцию будут автоматически логироваться в вашей системе мониторинга. Также в любой момент, через KMS можно ограничить доступ Пачке к расшифровке.

Продвинутое шифрование в Пачке



Полная прозрачность для вашей компании

Логирование в BYOK подходе обеспечивает полную прозрачность работы и позволяет настраивать гибкие политики безопасности.

Вы всегда видите, когда и зачем Пачка обратилась за ключами для расшифровки. И в случае подозрительной активности или каких-либо подозрений вы можете оперативно ограничивать доступ к данным и начать внутреннее расследование.

Обычный облачный подход не даёт такой прозрачности в отслеживании активности с сообщениями, а в on-prem решениях аналогичная система логов требует самостоятельного проектирования и настройки.

Быстрая блокировка данных и уменьшение рисков утечек

В нештатной ситуации (например, подозрительная активность или аномальные всплески трафика) вы можете оперативно принять меры для защиты данных:

- Вы видите все обращения к вашим данным и их цели
- Возможно оперативное отключение доступа к данным для локализации инцидента и проведения расследования для снижения рисков
- Гранулярное управление доступом — отключение доступа к определенной дате или чату

Распределение рисков и независимость от вашей инфраструктуры

Мессенджер не становится точкой входа для атак на внутреннюю инфраструктуру.

А в случае, если ваши сервера подверглись атаке, злоумышленник не получит доступ к переписка м и мессенджер остаётся доступен, как инструмент оперативного реагирования.

Все преимущества облака с повышенным контролем за данными

Обновления без участия пользователя

Вам не нужно самим обновлять сервис, тратить время и ресурсы на контроль версий и развёртывание фиксов.

Меньше нагрузки на ИБ-команды

Ваша ИБ-команда может не беспокоиться на счёт доступности сервиса и обеспечения его безопасности, чтобы заниматься более приоритетными задачами.

Безопасные обновления в облаке

Все обновления в облаке проходят гладко, без риска сломать функционал у пользователей.

Минимум инфраструктуры

Нет необходимости в дополнительной инфраструктуре и её обслуживании.

Пачка

Написать нам

Проведём согласование технологии с вашими отделами ИБ:

1. Созвон с вашими ИБ, презентация технологии и всех компонентов системы
2. Презентация, архитектура и документация технологии
3. Тестирование и аудит ключевых блоков со стороны ИБ