

Новые возможности для обеспечения безопасности и защиты данных

Андрей Гусаков
Консультант



От сертификации СЗИ к сертификации РБПО



Эволюция разработки средств ИБ

Компания Postgres Professional успешно доказала наличие ресурсов, знание технологий и зрелость процессов.

Цель сертификации – сохранив безопасность ПО, снизить издержки разработчиков и ускорить доставку обновлений пользователям.

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



СЕРТИФИКАТ СООТВЕТСТВИЯ

№ 7

Выдан: 21 октября 2025 г.
Действителен до: 21 октября 2030 г.

Настоящий сертификат удостоверяет, что процессы безопасной разработки, реализованные обществом с ограниченной ответственностью «Постгрес Профессиональный» (ООО «Постгрес Профессиональный»), соответствуют требованиям национального стандарта ГОСТ Р 56939-2024 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного и введенного в действие приказом Федерального агентства по техническому регулированию и метрологии от 24 октября 2024 г. № 1504-ст.

Сертификат выдан на основании результатов сертификации, проведенной органом по сертификации федерального государственного бюджетного учреждения науки Институт системного программирования им. В.П. Иванникова Российской академии наук (аттестат аккредитации от 24.05.2024 № СЗИ RU.0001.01БИ00.A009) - экспертное заключение от 26.09.2025.

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



В.Лютиков

Требования к процессам

- Состав процессов
- Регламенты и методики
- Документирование
- Получаемые результаты (артефакты)
- Регулярность
- Объем (границы) применения

Требования к технологиям

- Технологии анализа
 - Качественные характеристики
 - Количественные характеристики
- Базовые IT-системы
 - Интеграция

Источник требований

- ГОСТ Р 56939 «Общие требования»
- Технологические стандарты
 - ГОСТ Р 71206-2024, 71207-2014, ...
- Отраслевые требования
 - ФСТЭК России: Требования Доверия, Методика ВУИНДВ
 - ...

Требования к ресурсам

- Сотрудники
 - Должное количество
 - Навыки/умения
- Инфраструктура
 - Серверы
 - Каналы связи

Новые решения для ИБ

2025H2

Нейтрализация угроз:

- Злоумышленник имеет доступ к серверу, на котором установлена СУБД, и может читать файлы; как вариант – он является администратором инфраструктуры (OS root)
- Злоумышленник имеет физический доступ к серверу СУБД, но не имеет прав входа в систему
- Злоумышленник имеет физический доступ к хранилищу резервных копий
- Злоумышленник имеет доступ к сети, по которой передаются данные между Master и Standby

Нейтрализация угроз:

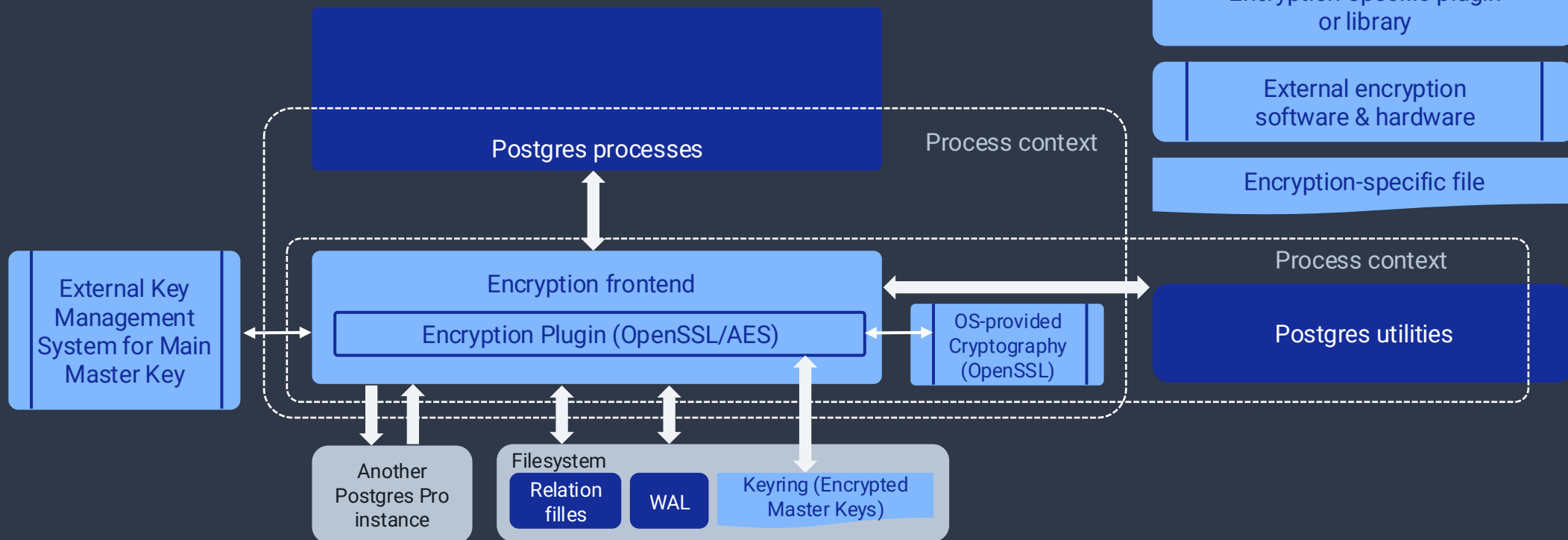
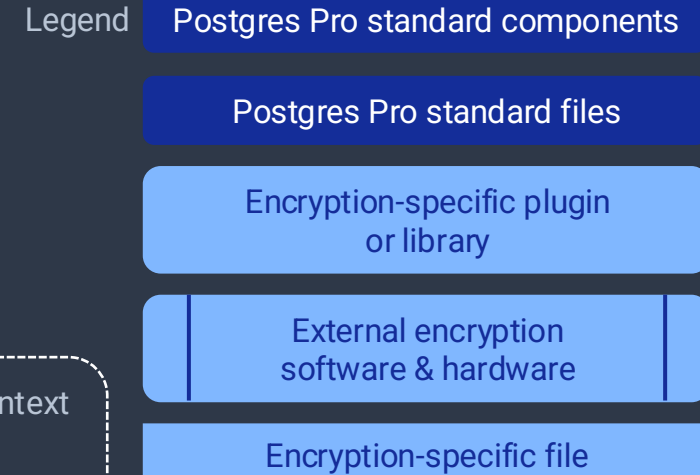
- Злоумышленник имеет доступ к серверу, на котором установлена СУБД, и может читать файлы; как вариант – он является администратором инфраструктуры (OS root)
- Злоумышленник имеет физический доступ к серверу СУБД, но не имеет прав входа в систему
- Злоумышленник имеет физический доступ к хранилищу резервных копий
- Злоумышленник имеет доступ к сети, по которой передаются данные между Master и Standby

Прозрачность преобразований:

- Все запросы к защищенным данным СУБД, выполняемые через соединение по libpq, выполняются точно так же, как к незащищенным. Полная обратная совместимость
- Все поставляемые в составе сервера СУБД утилиты работают с защищенными данными СУБД точно так же, как с незащищенными

Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

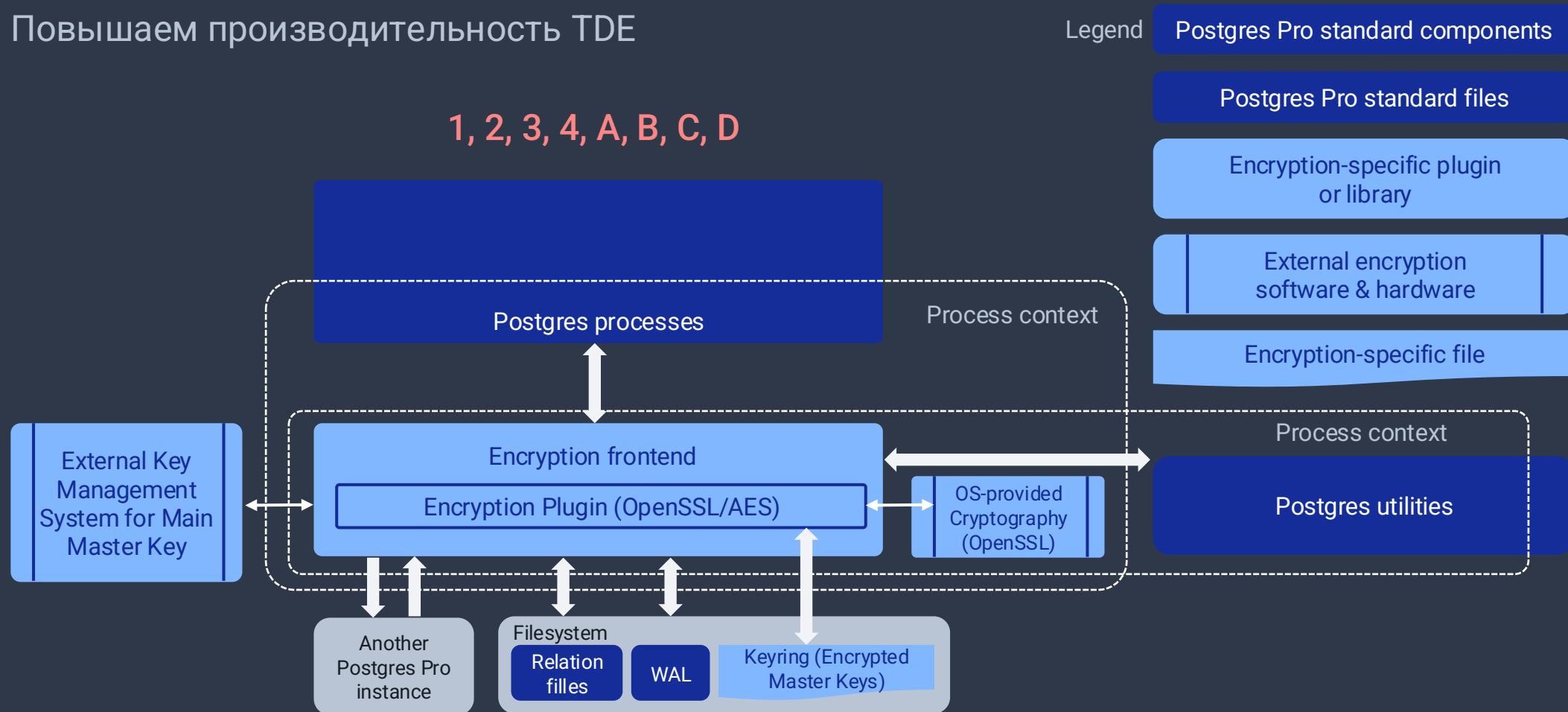
Повышаем производительность TDE



Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

Повышаем производительность TDE

1, 2, 3, 4, A, B, C, D



Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

Повышаем производительность TDE

Legend

Postgres Pro standard components

Postgres Pro standard files

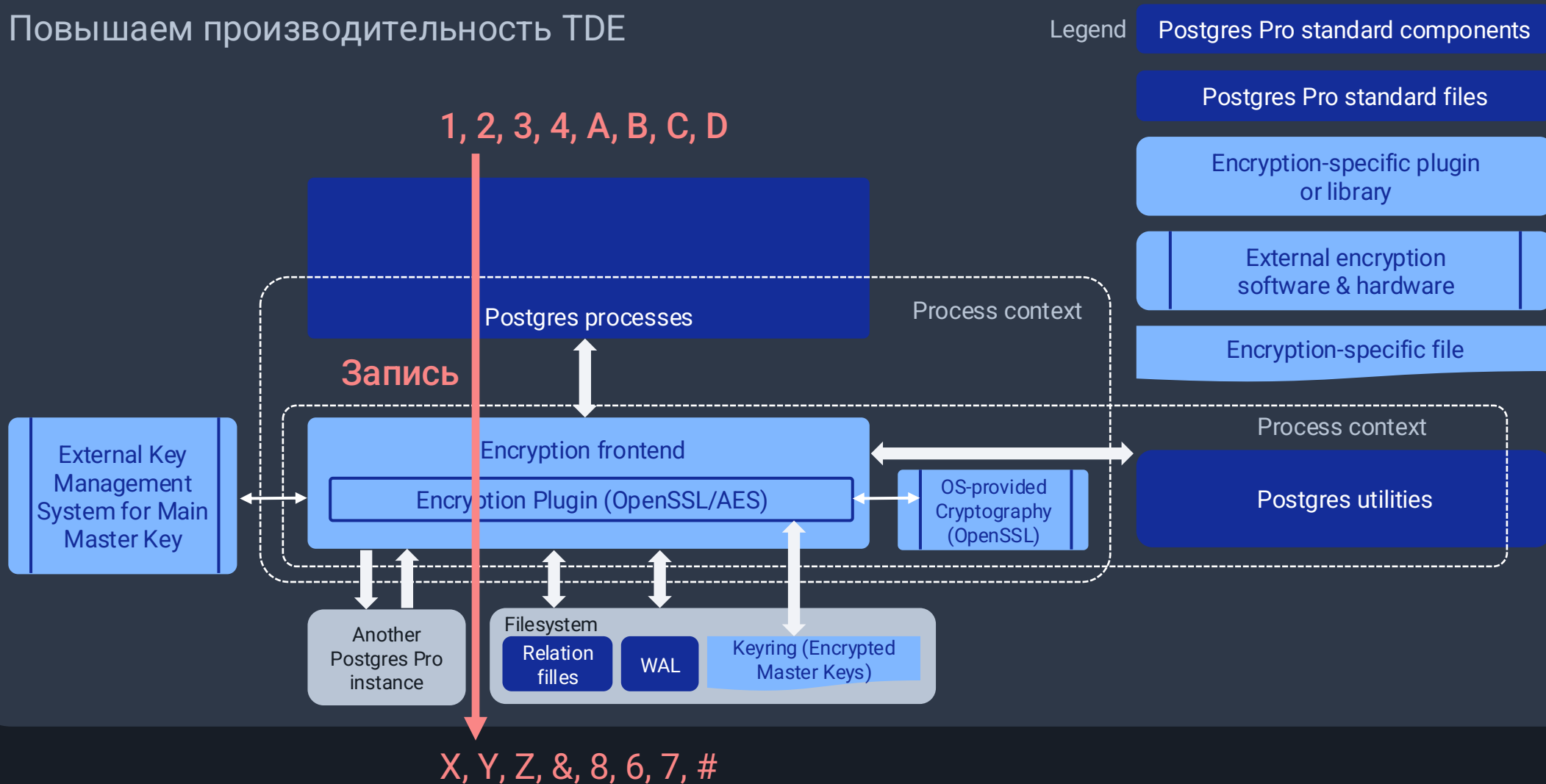
Encryption-specific plugin or library

External encryption software & hardware

Encryption-specific file

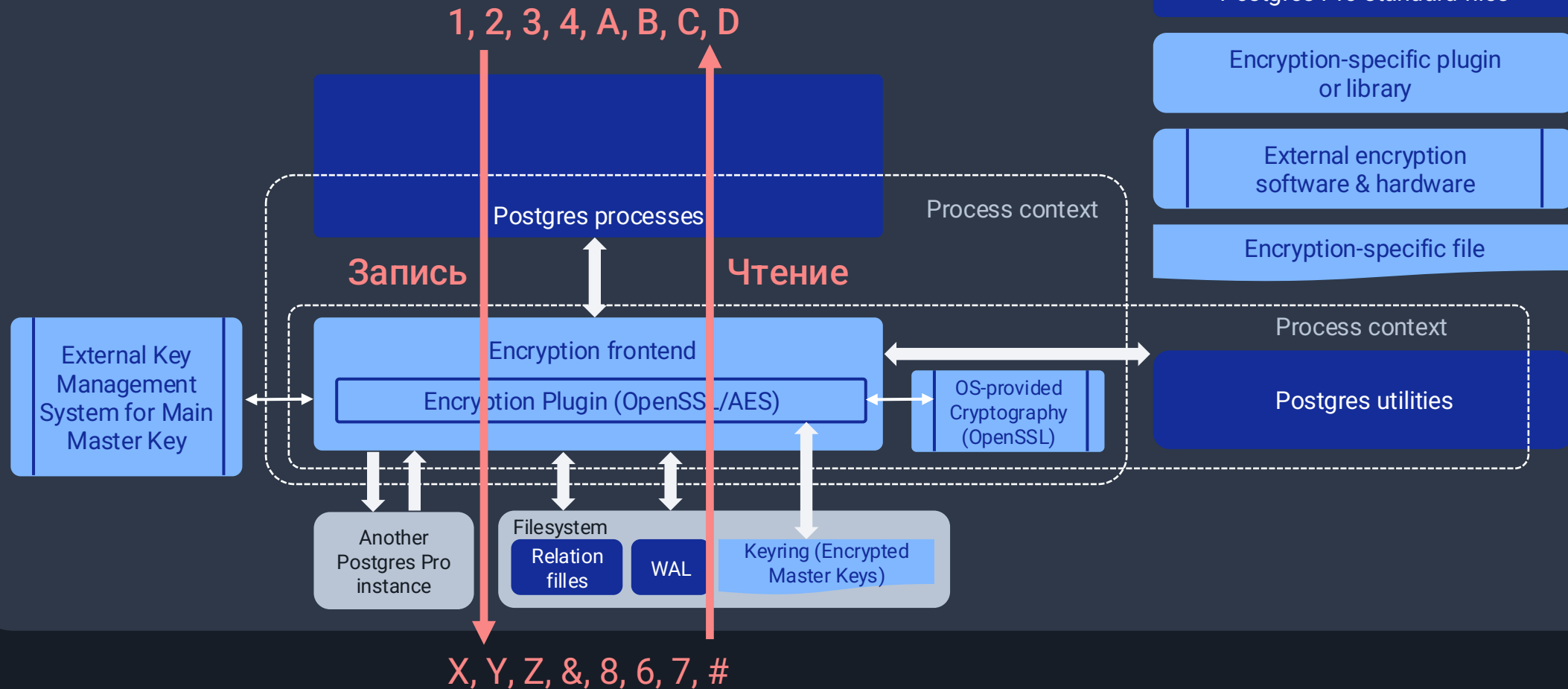
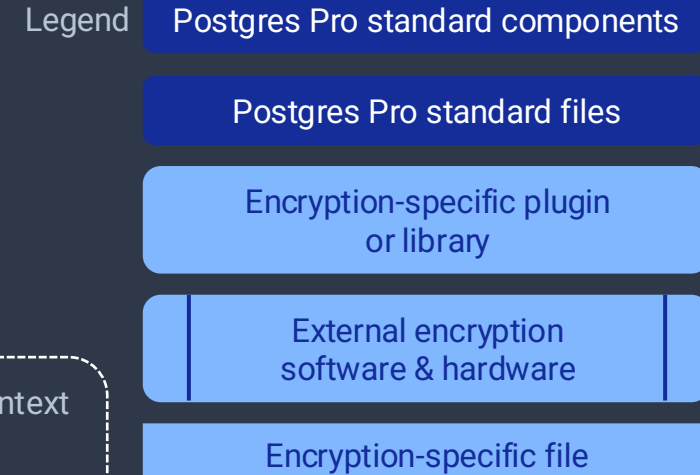
1, 2, 3, 4, A, B, C, D

Запись



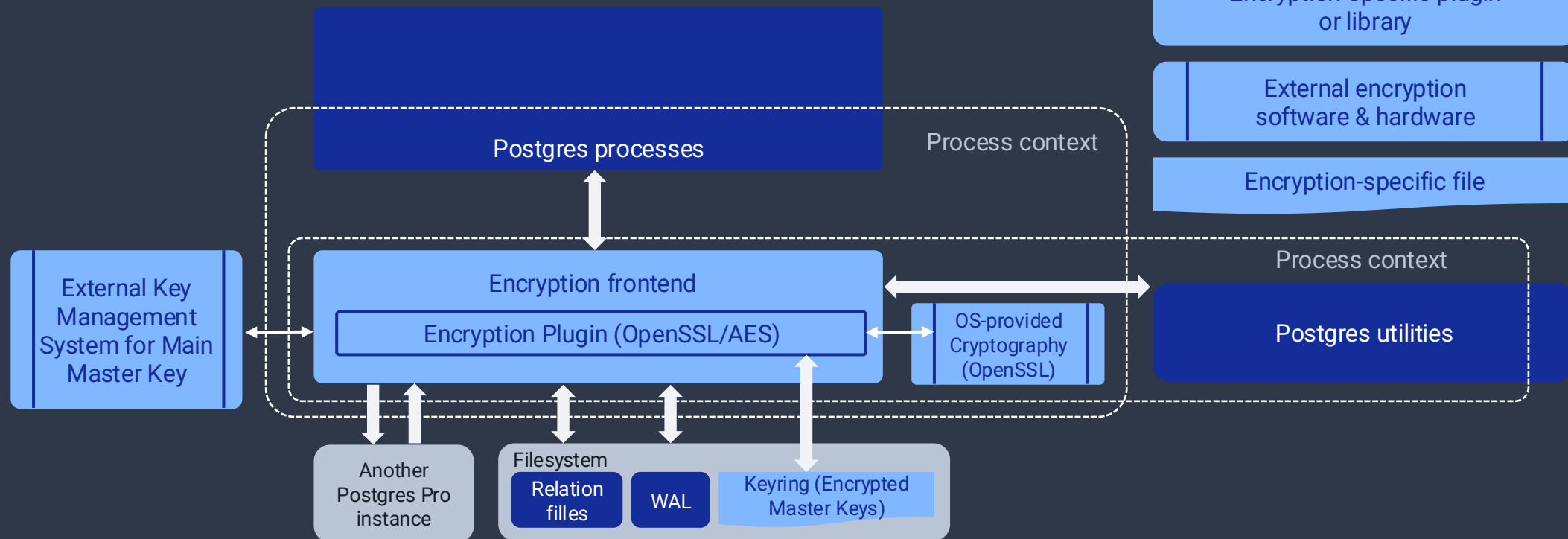
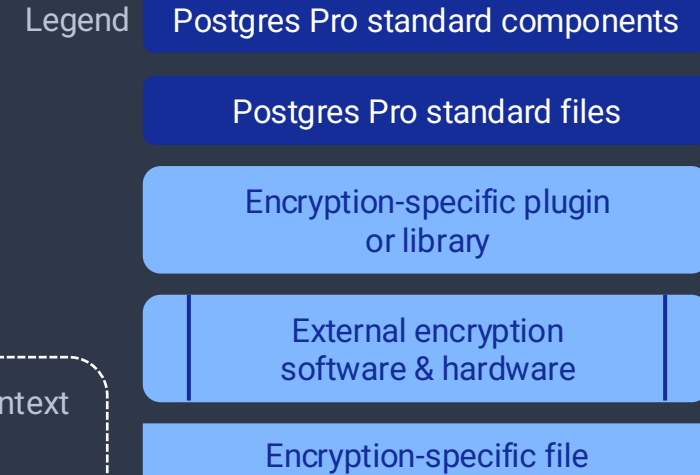
Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

Повышаем производительность TDE



Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

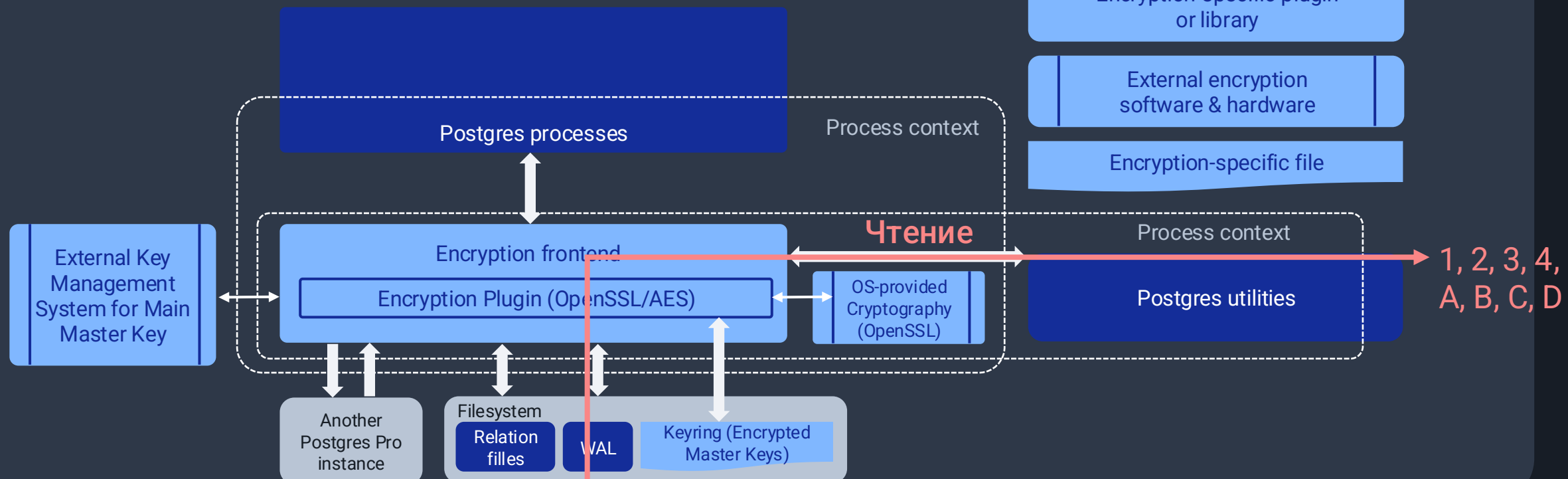
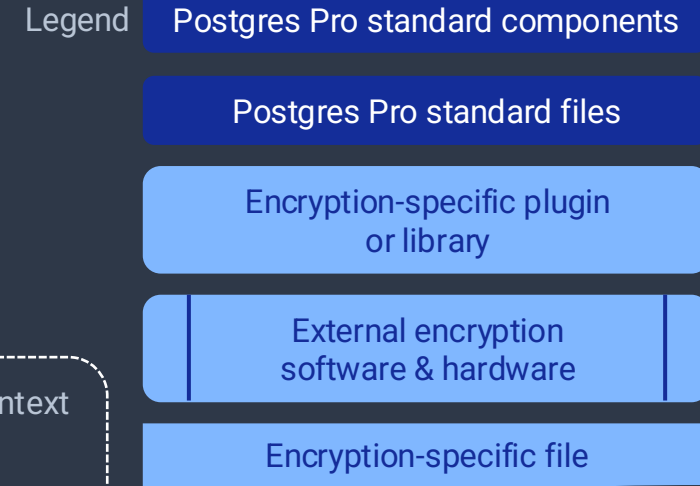
Повышаем производительность TDE



X, Y, Z, &, 8, 6, 7, #

Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

Повышаем производительность TDE



1, 2, 3, 4,
A, B, C, D

X, Y, Z, &, 8, 6, 7, #

Выделяем под данные табличное пространство, применяем оптимальные алгоритмы

Повышаем производительность TDE

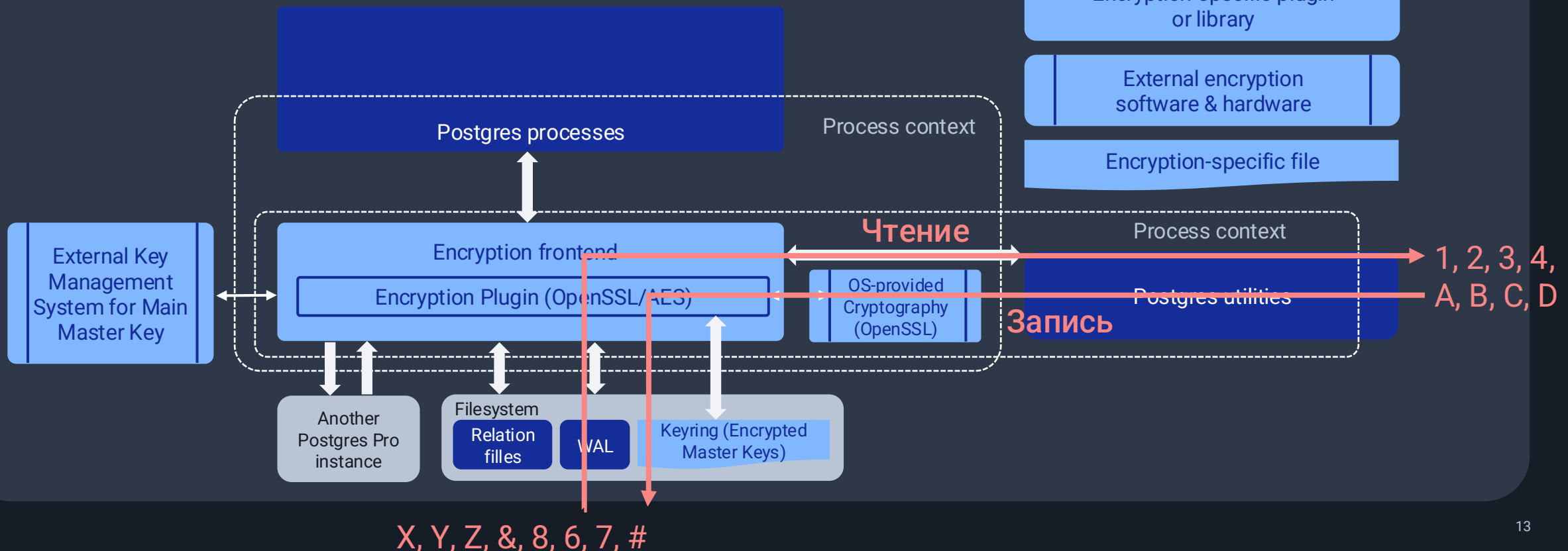
Legend Postgres Pro standard components

Postgres Pro standard files

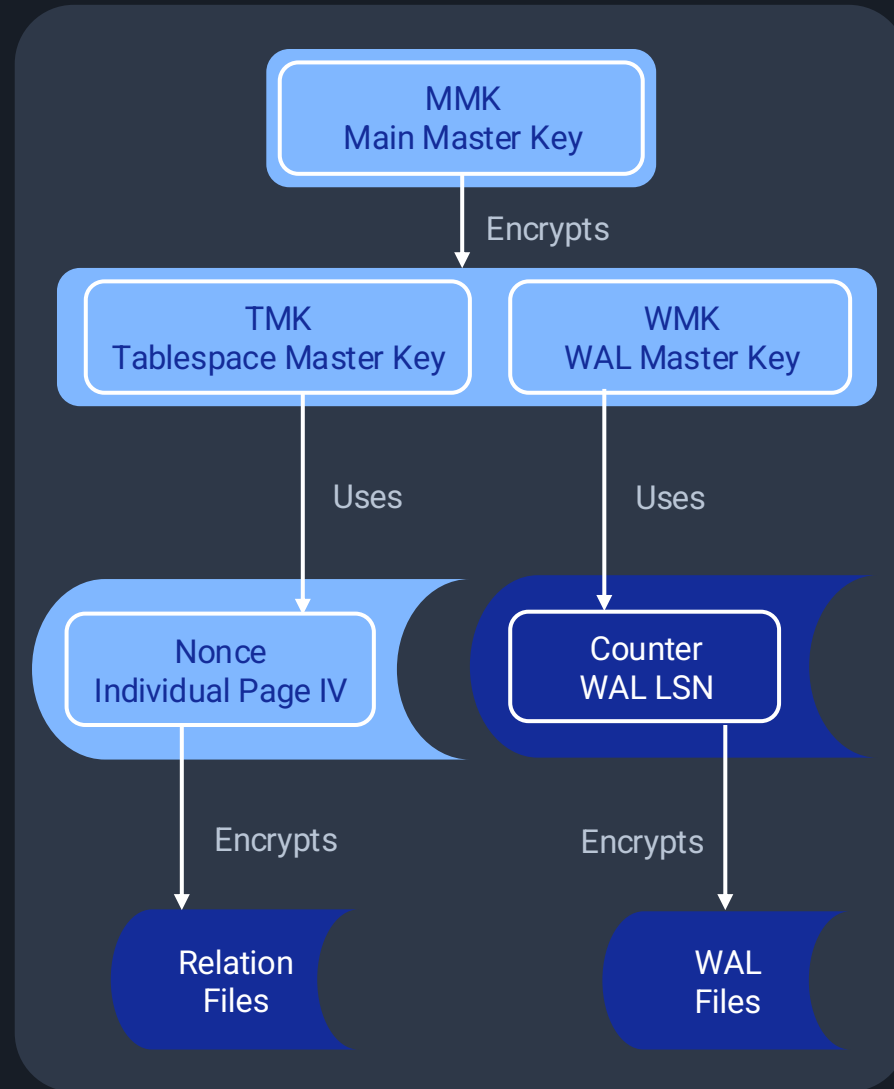
Encryption-specific plugin or library

External encryption software & hardware

Encryption-specific file

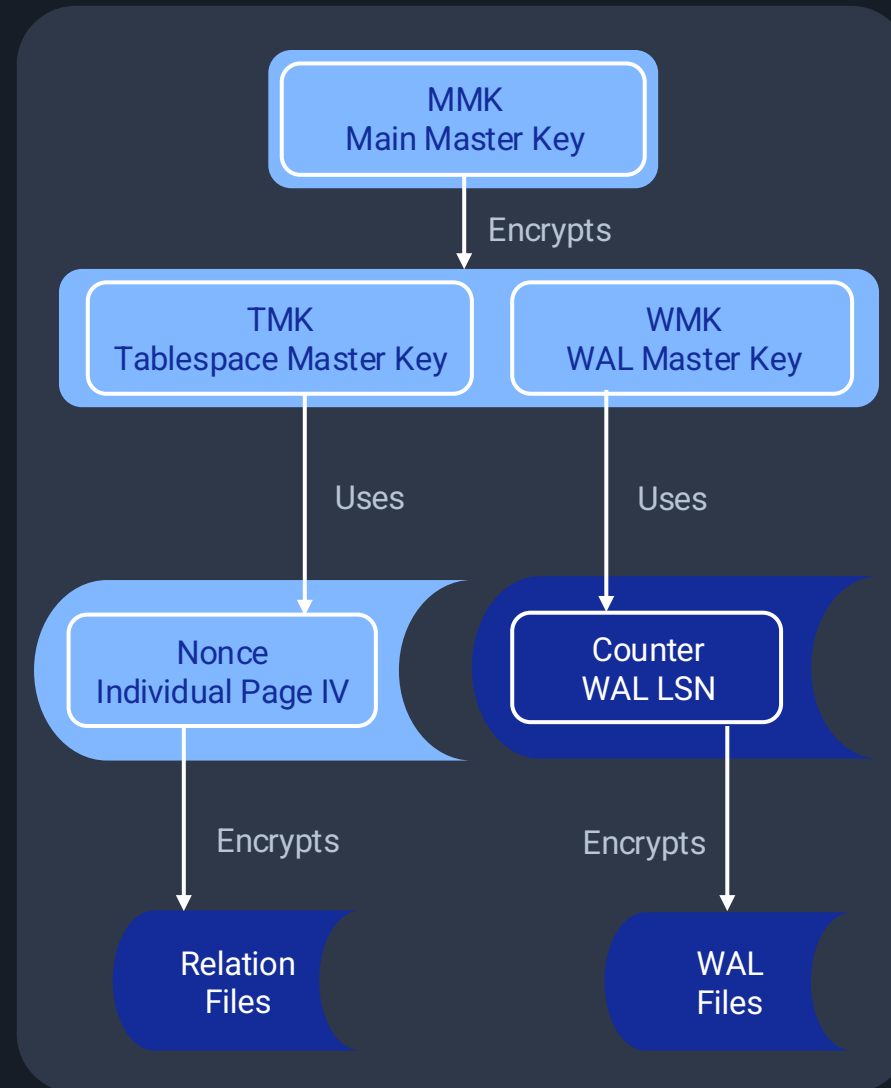


Управление ключами, их защита и ротация



Управление ключами, их защита и ротация

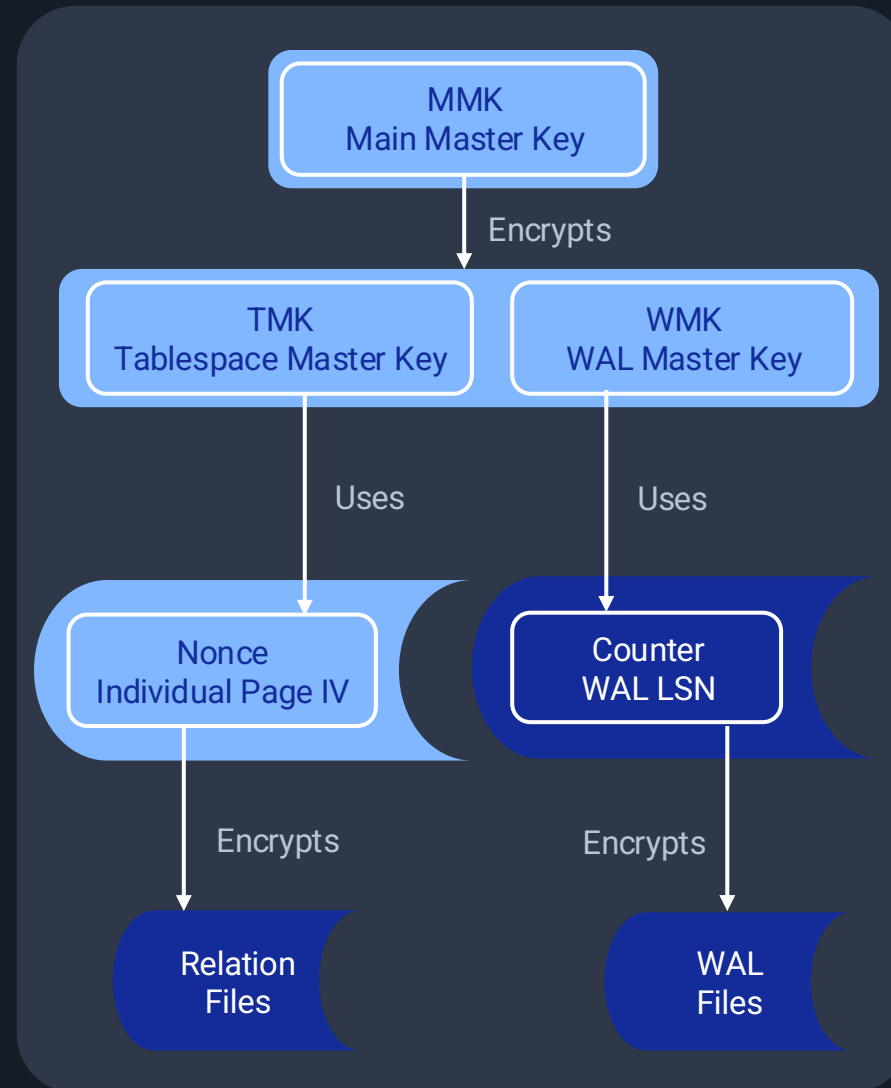
Автоматическая генерация первых ключей в ключнице



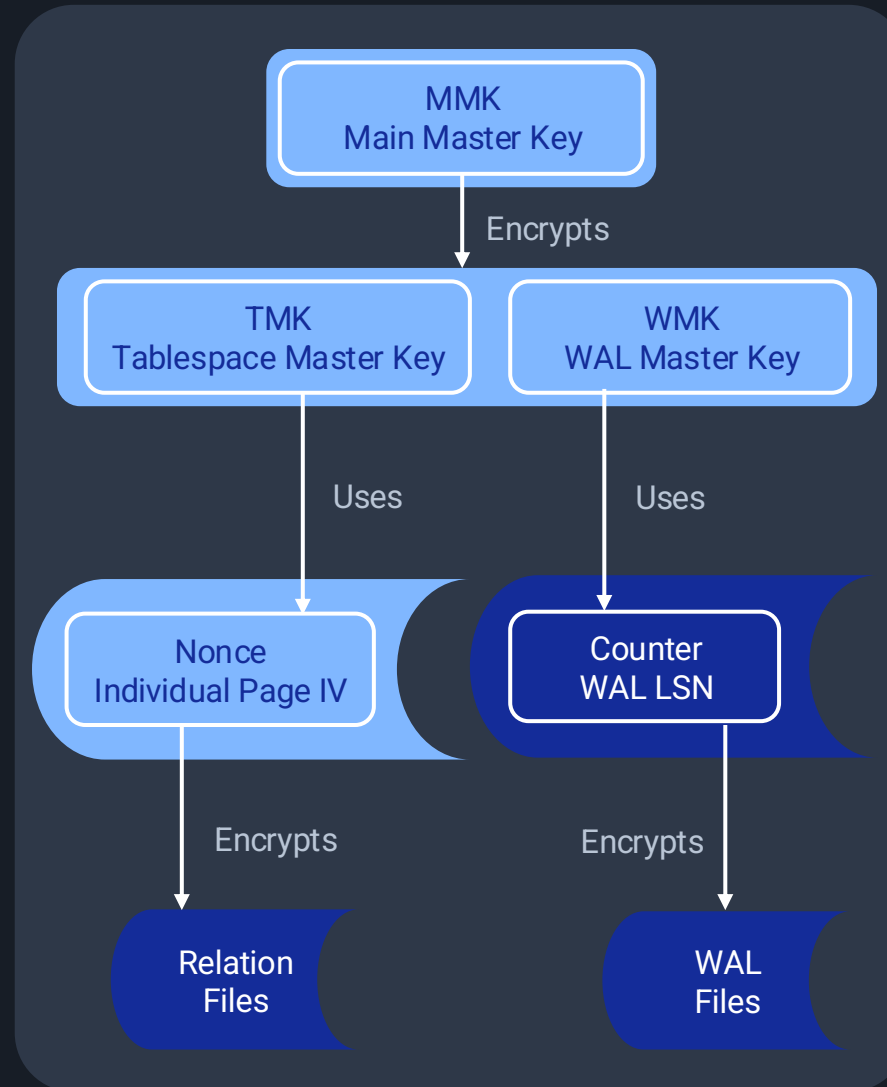
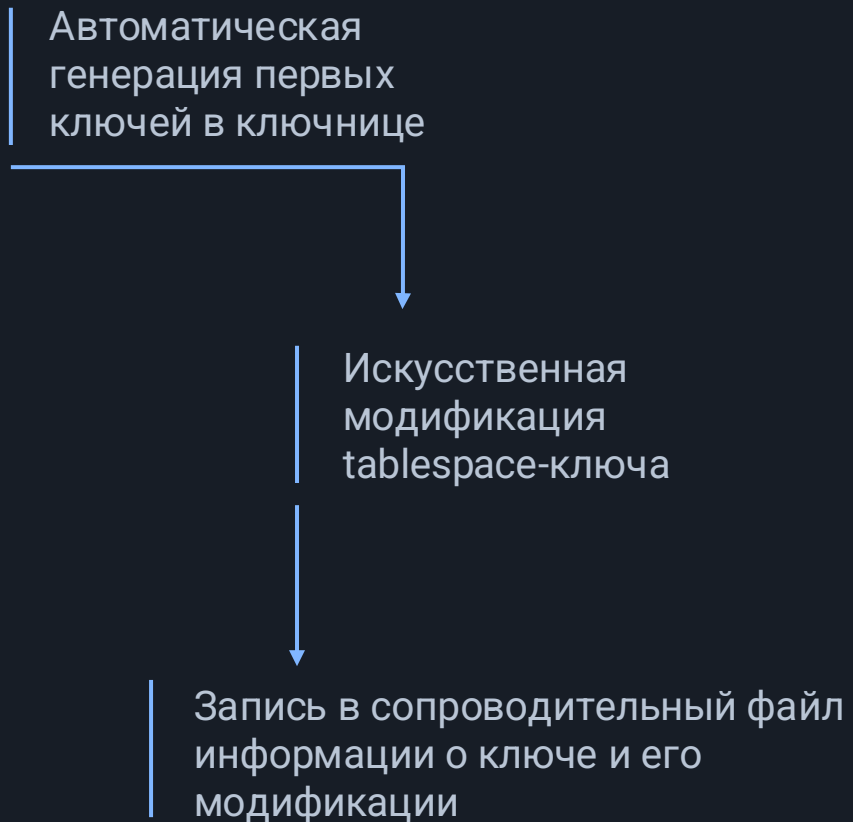
Управление ключами, их защита и ротация

Автоматическая генерация первых ключей в ключнице

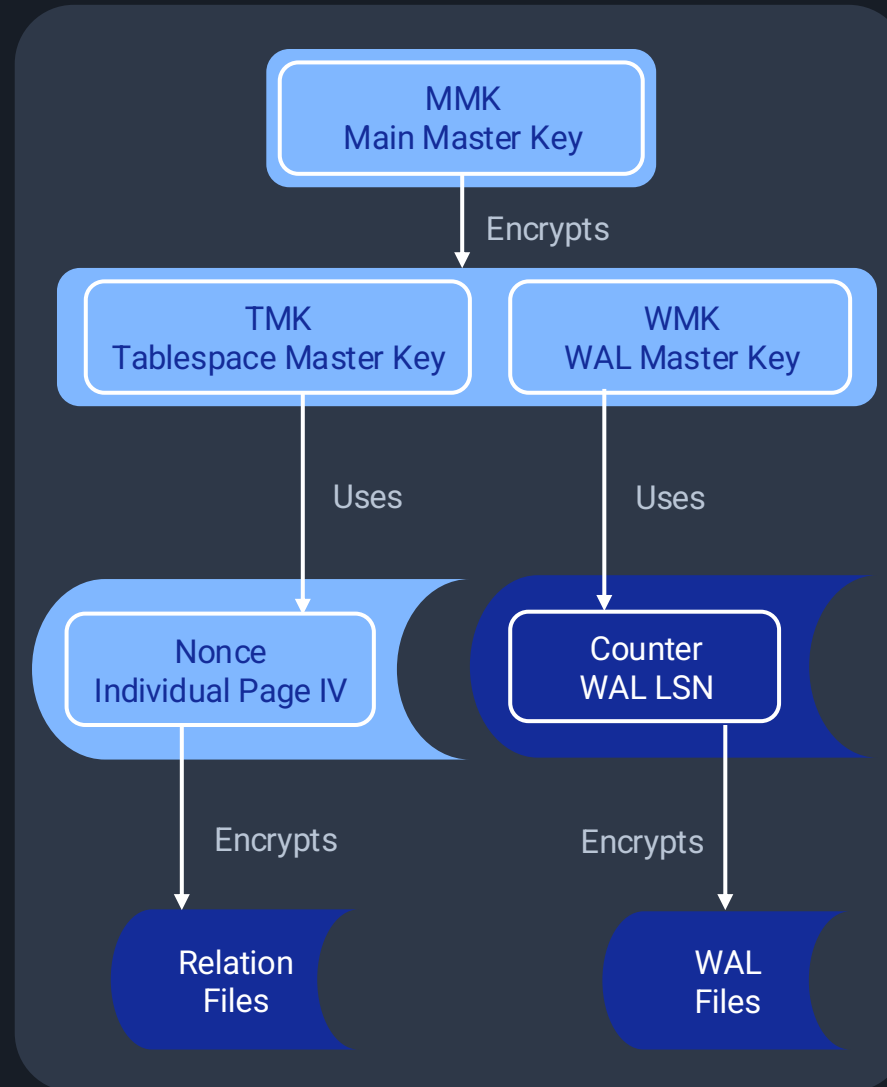
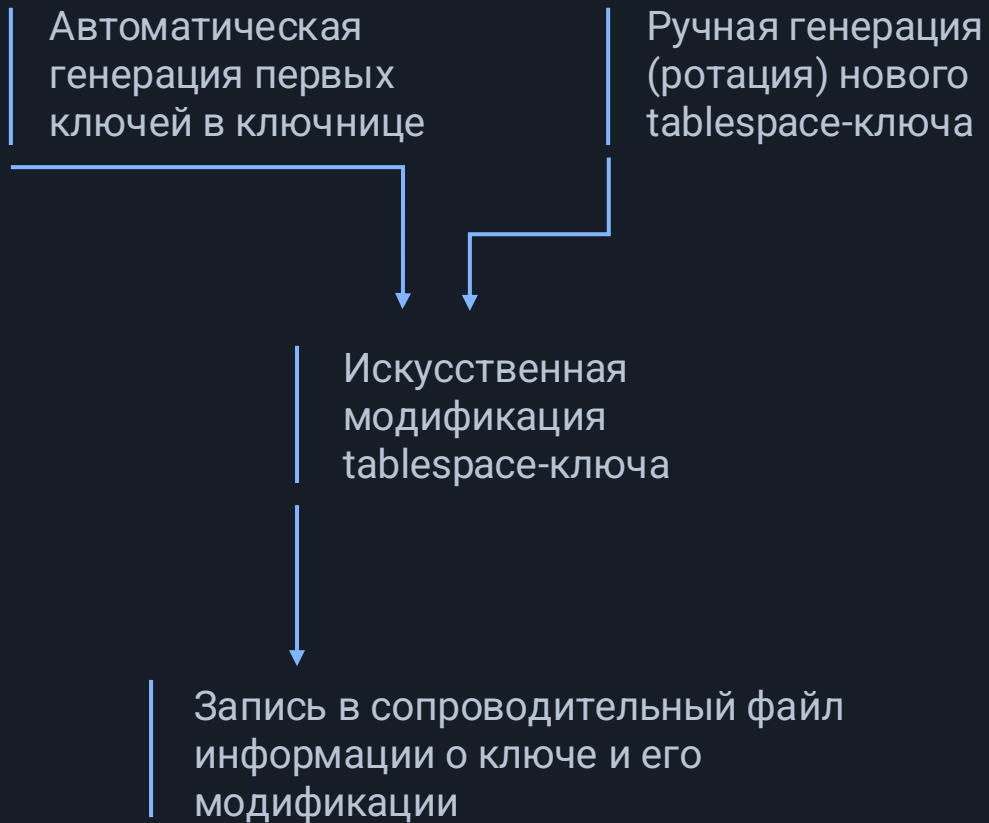
Искусственная модификация tablespace-ключа



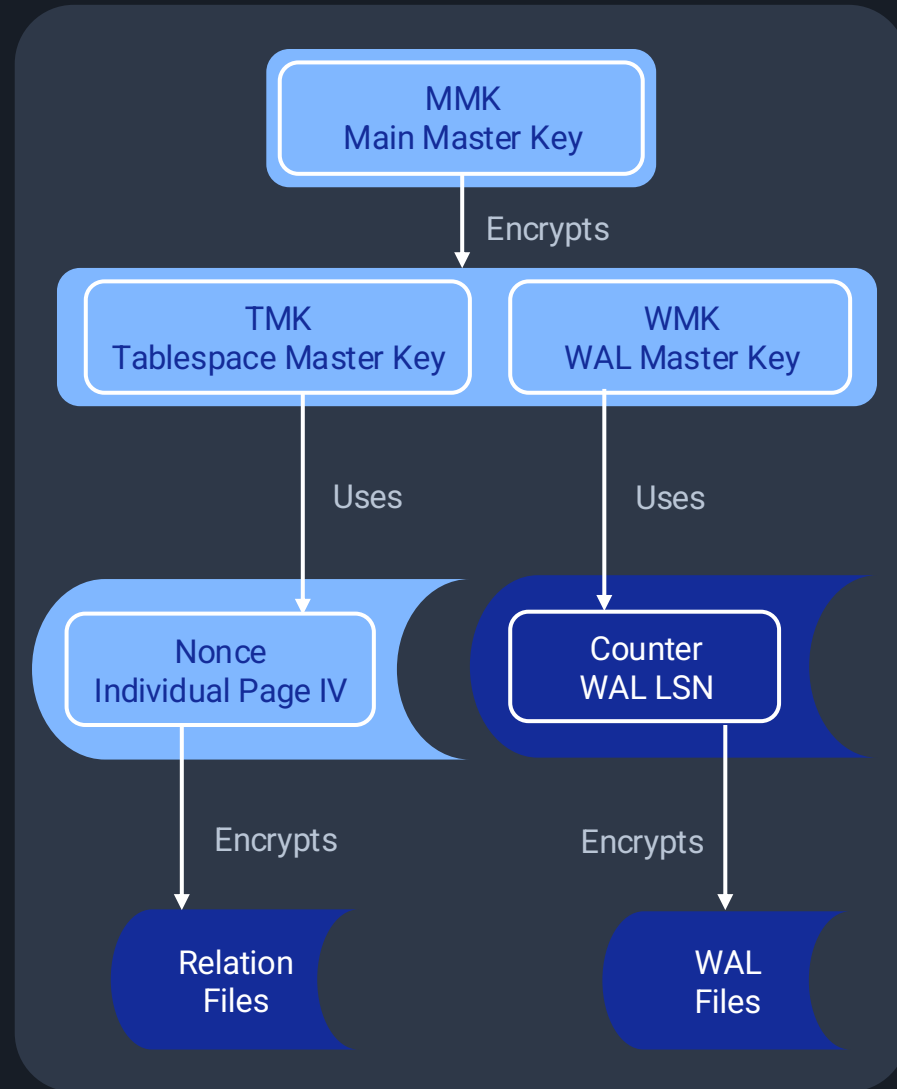
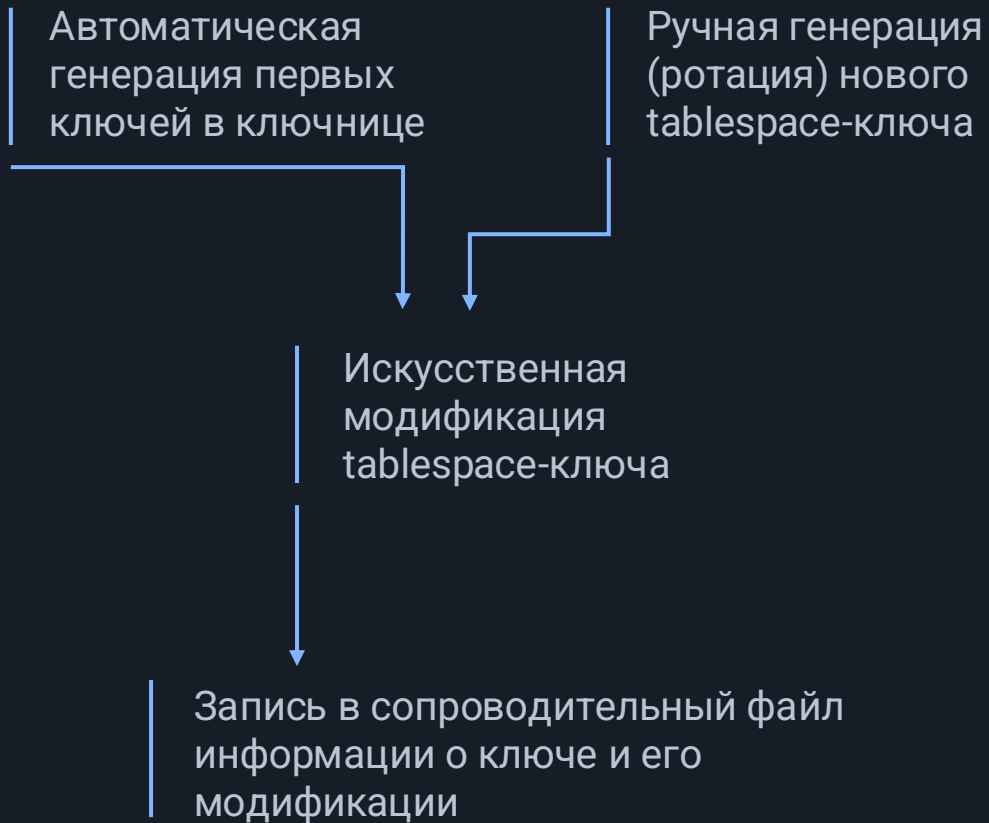
Управление ключами, их защита и ротация



Управление ключами, их защита и ротация

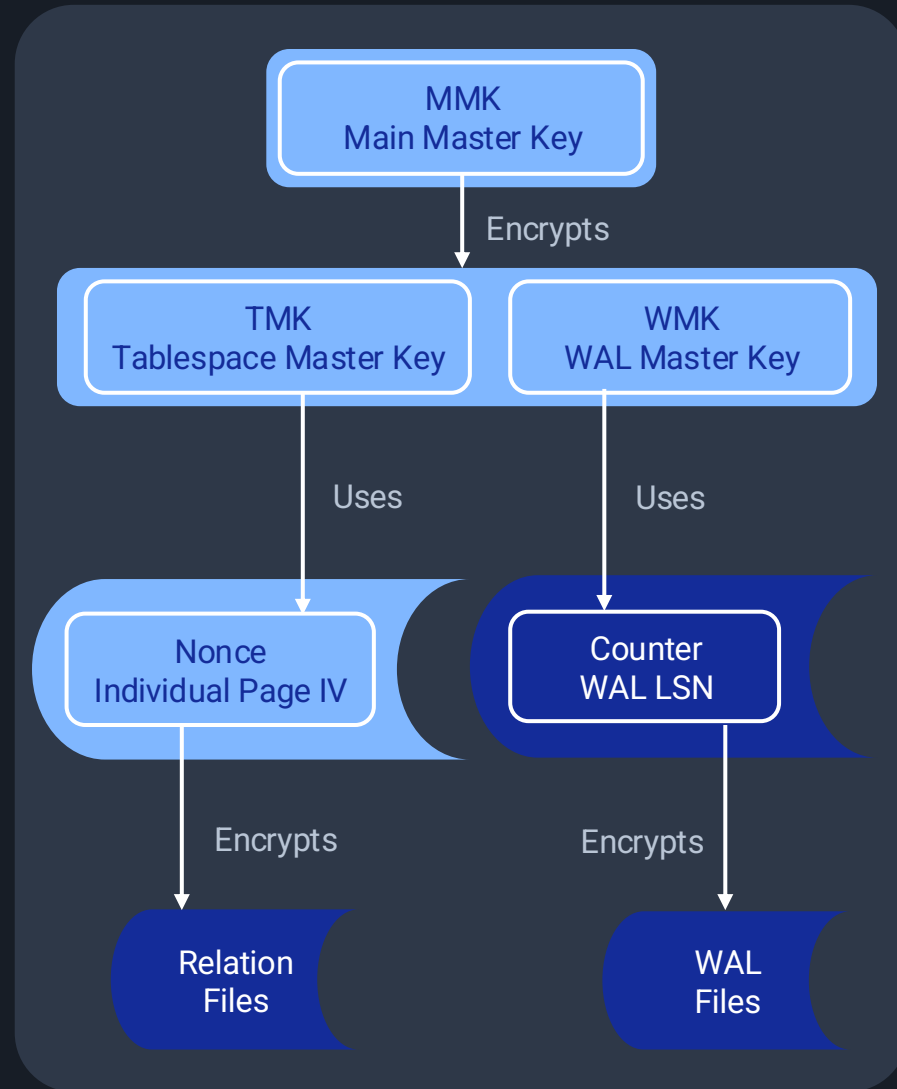
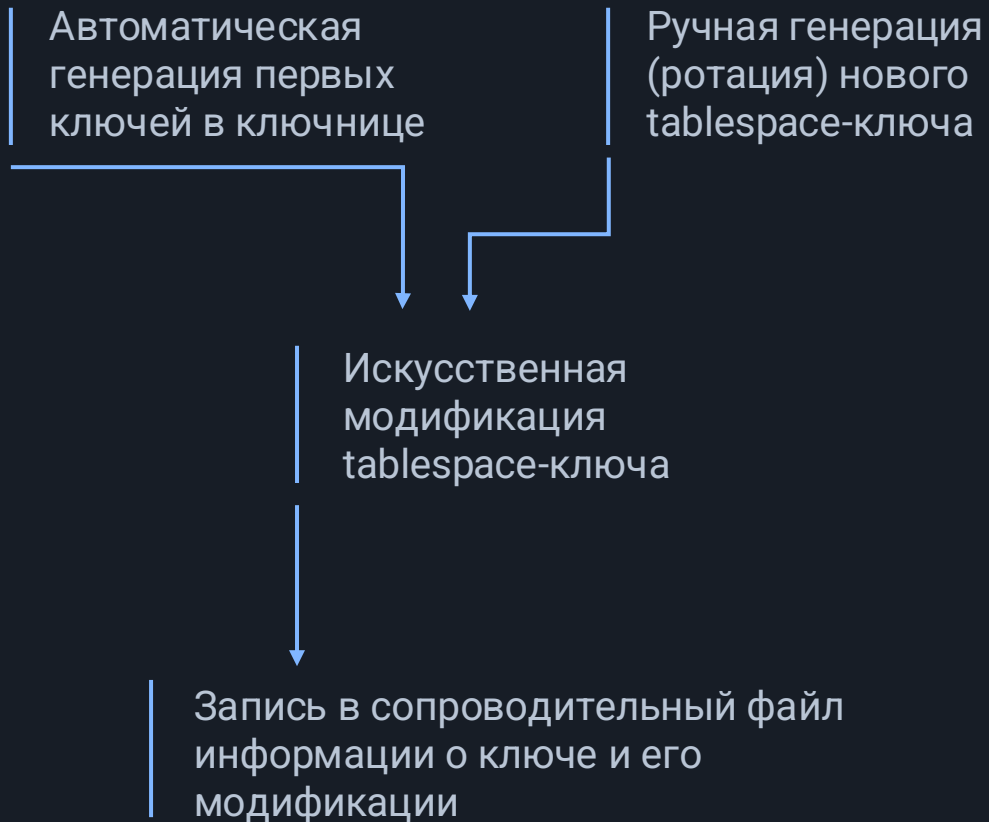


Управление ключами, их защита и ротация



Модификация WAL-ключа с использованием счетчика LSN

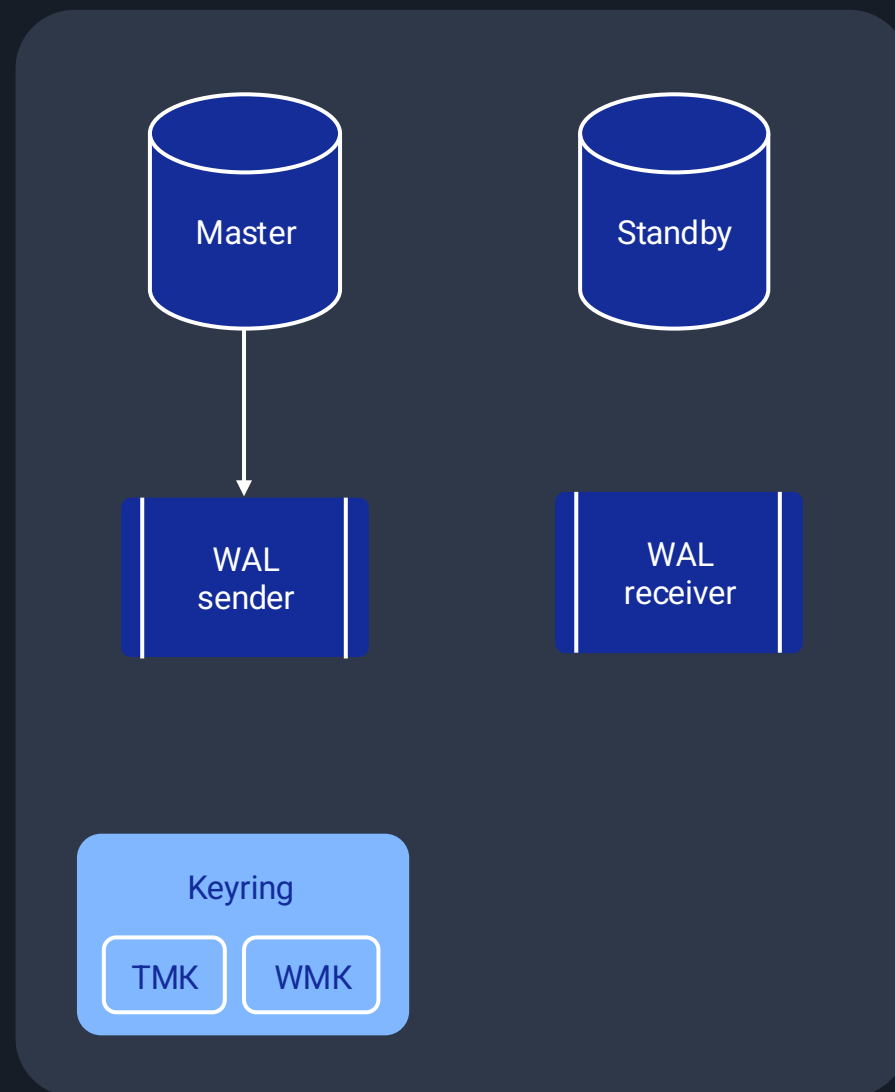
Управление ключами, их защита и ротация



Все ключи (старые и новые) всегда хранятся в ключнице

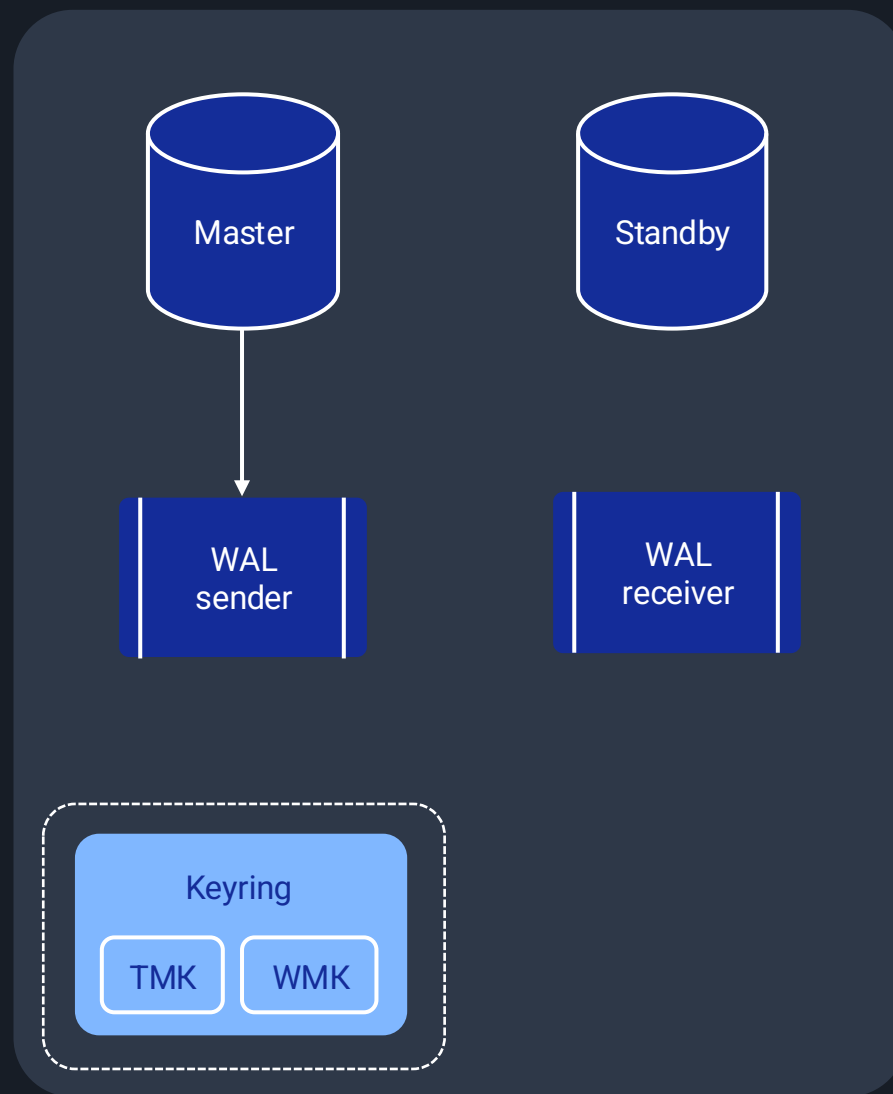
Модификация WAL-ключа с использованием счетчика LSN

Синхронизация ключей в многоузловой конфигурации



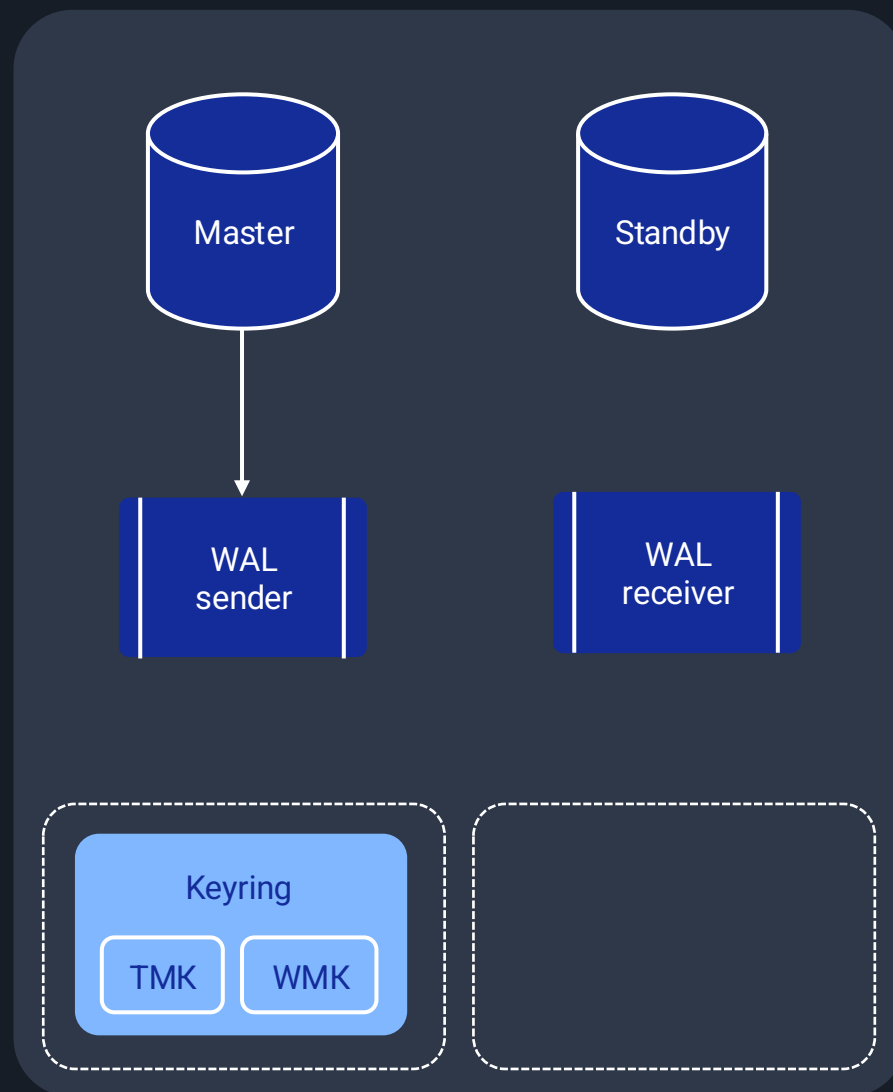
После генерации первых ключей на мастере ключница должна быть вручную скопирована на реплику до ее старта

Синхронизация ключей в многоузловой конфигурации



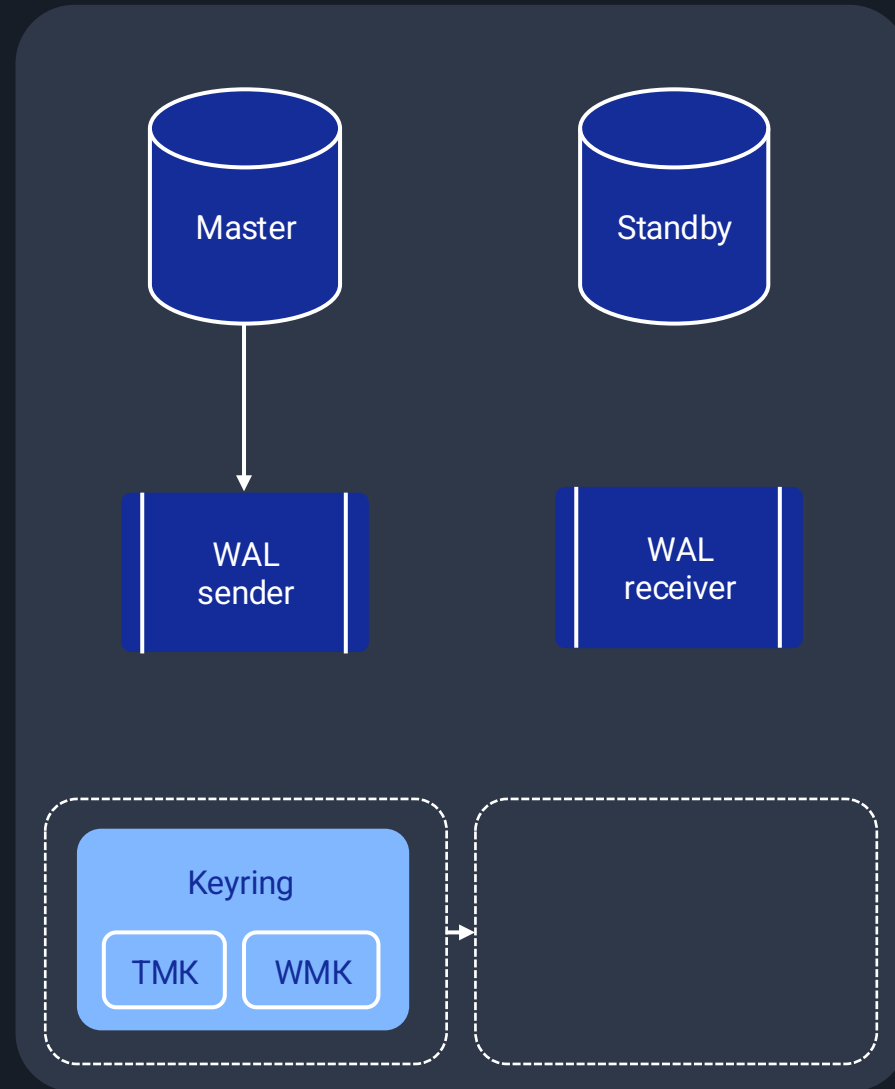
После генерации первых ключей на мастере ключница должна быть вручную скопирована на реплику до ее старта

Синхронизация ключей в многоузловой конфигурации



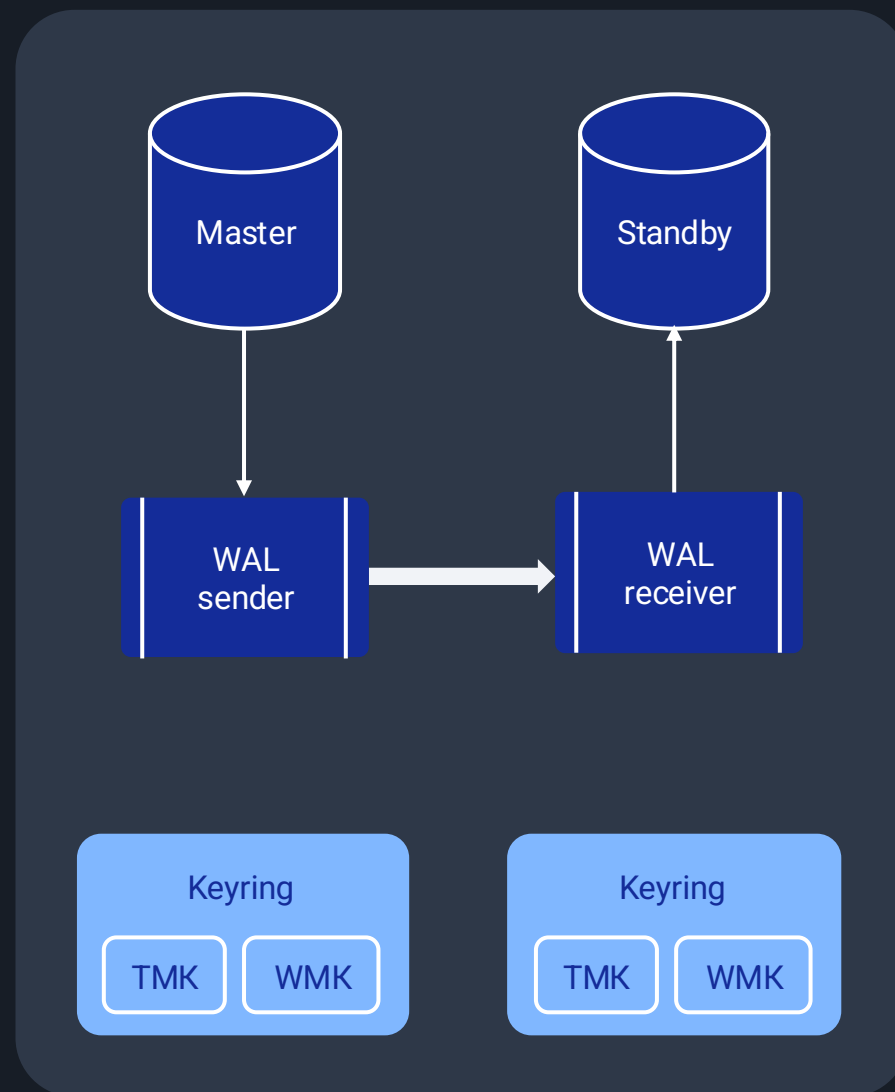
После генерации первых ключей на мастере ключница должна быть вручную скопирована на реплику до ее старта

Синхронизация ключей в многоузловой конфигурации



После генерации первых ключей на мастере ключница должна быть вручную скопирована на реплику до ее старта

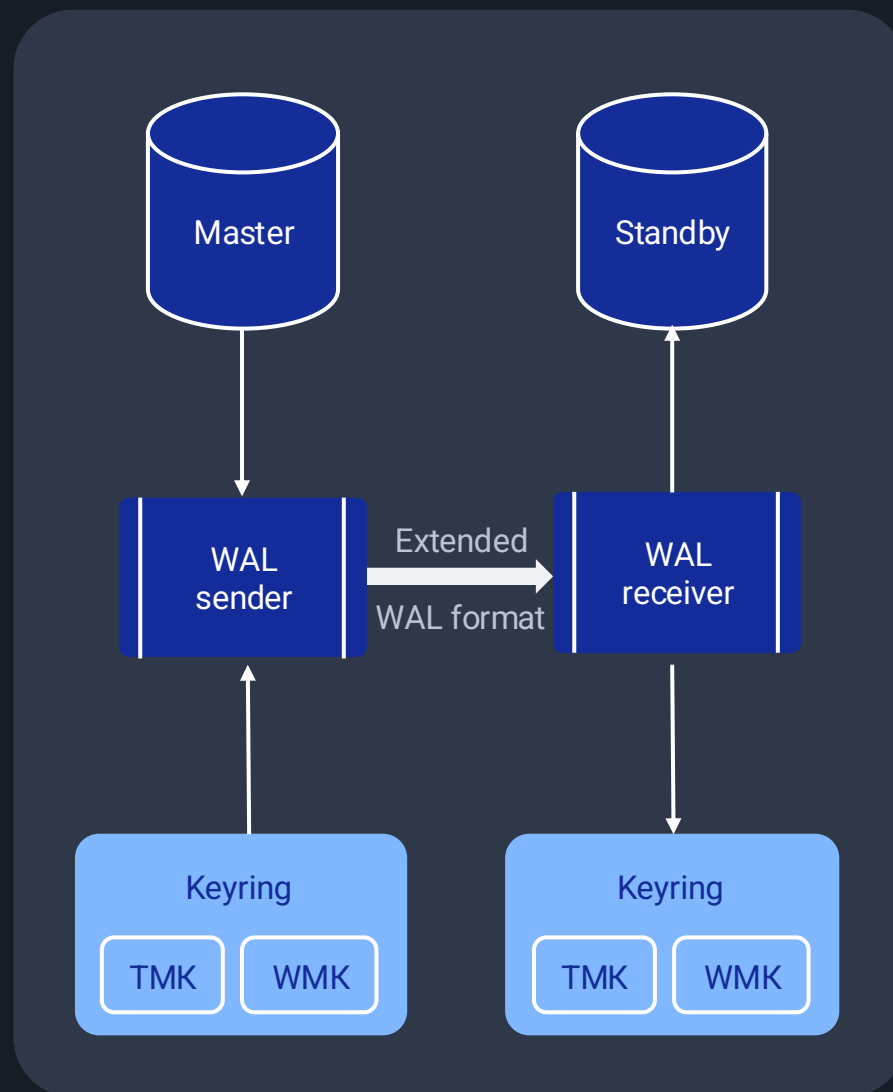
Синхронизация ключей в многоузловой конфигурации



WAL-ключ на реплике позволит декодировать защищенные WAL-записи с мастера и корректно их обработать

Синхронизация ключей в многоузловой конфигурации

Расширенный формат передачи WAL-записей позволит автоматически отправлять на реплику все новые tablespace-ключи



WAL-ключ на реплике позволит декодировать защищенные WAL-записи с мастера и корректно их обработать

Преимущества TDE перед преобразованием на уровне приложения

Не требуется хранение секретов и процедура их ротации на стороне многочисленных клиентов

Не требуется изменять запросы приложений к БД

Можно фильтровать данные (sql where, having) по значению колонки защищённой таблицы

Можно связывать таблицы (foreign key) по значению колонки защищённой таблицы

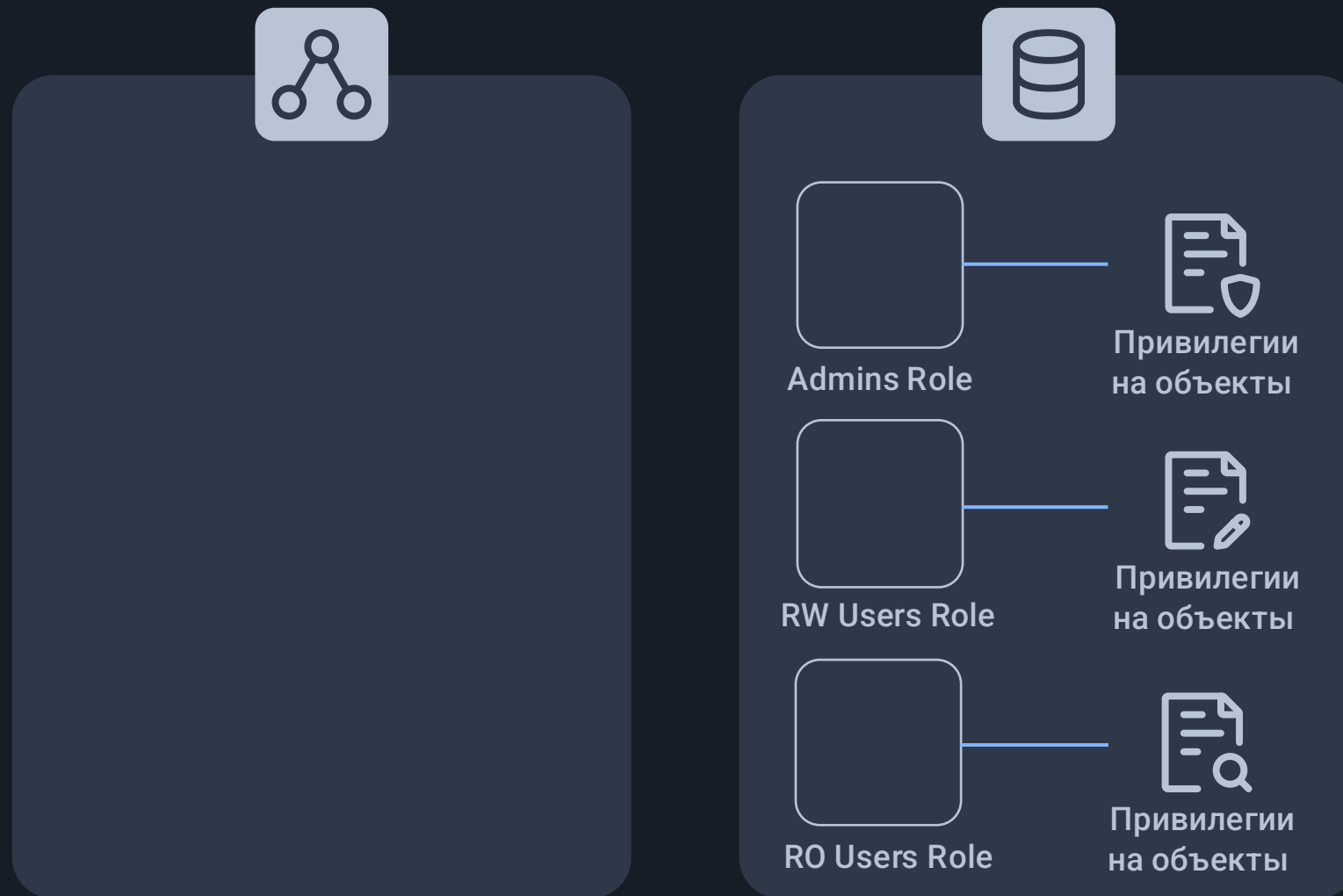
Можно накладывать ограничения (constraints) по значению колонки защищённой таблицы

Доступно, начиная с 17.6.1 ENT,
поддерживается pg_probackup 2.8.11 ENT и 3.2.0

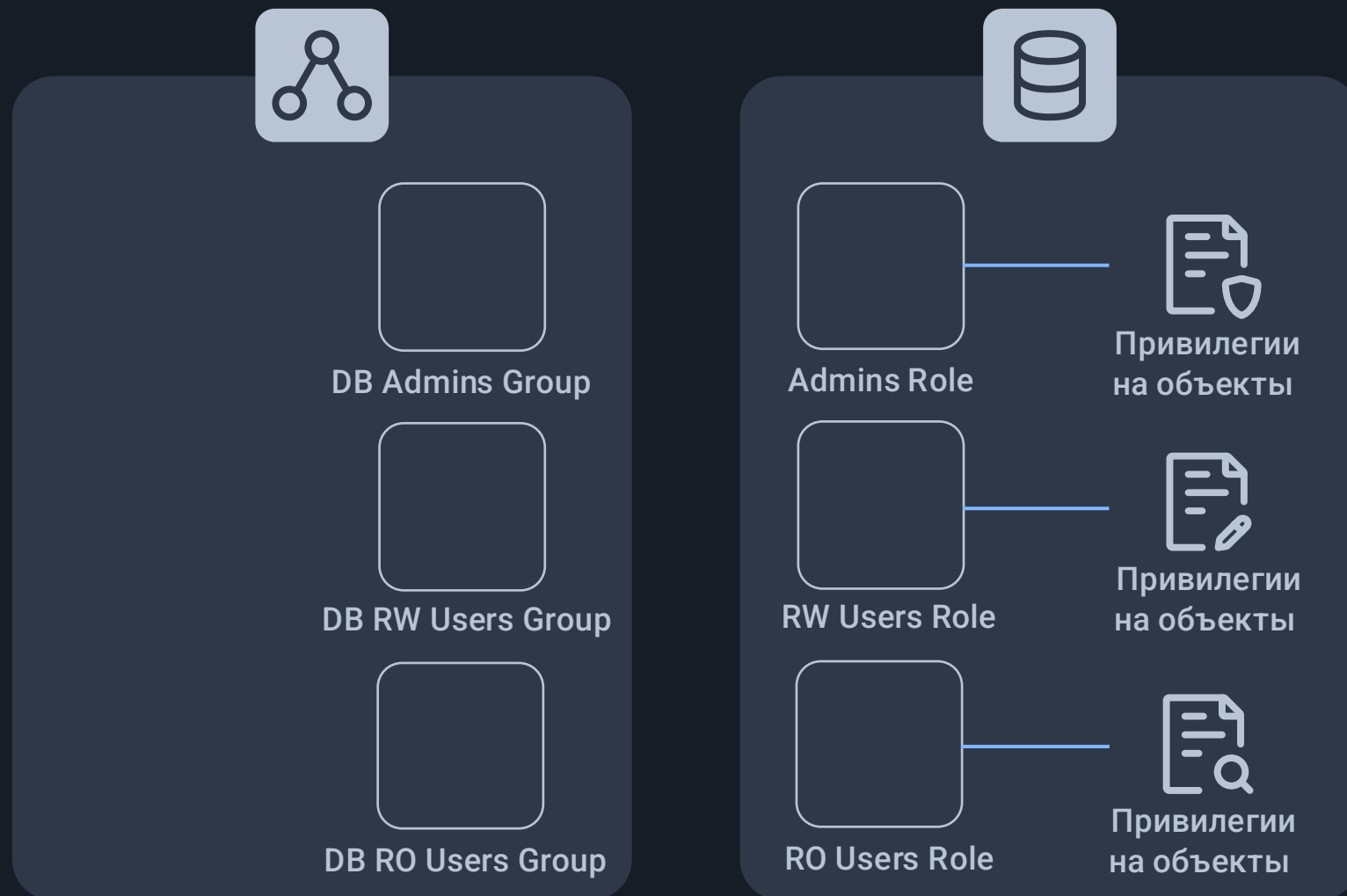


habr.com/ru/companies/postgrespro/articles/937246

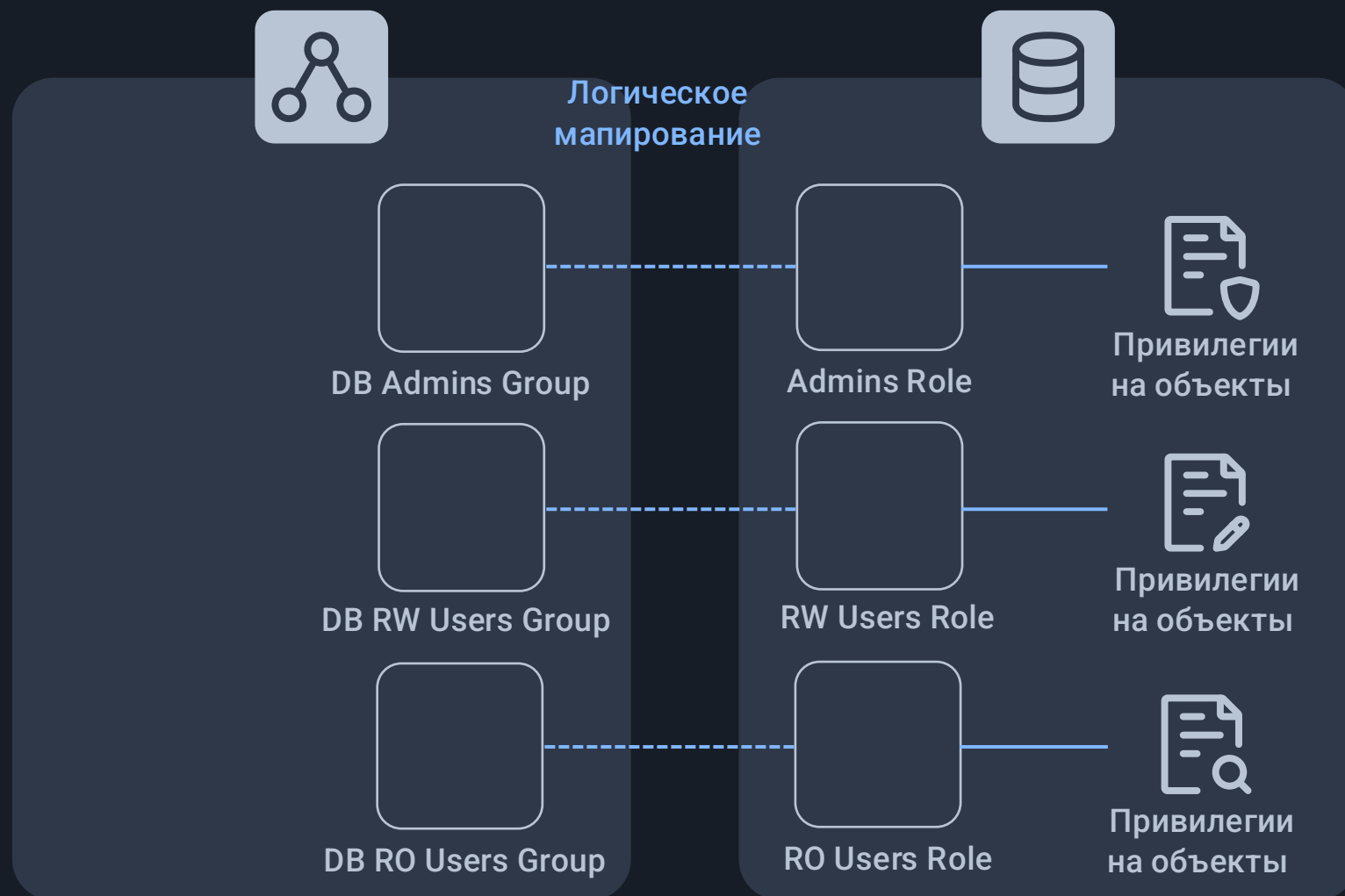
Синхронизация ролей и привилегий СУБД с группами LDAP



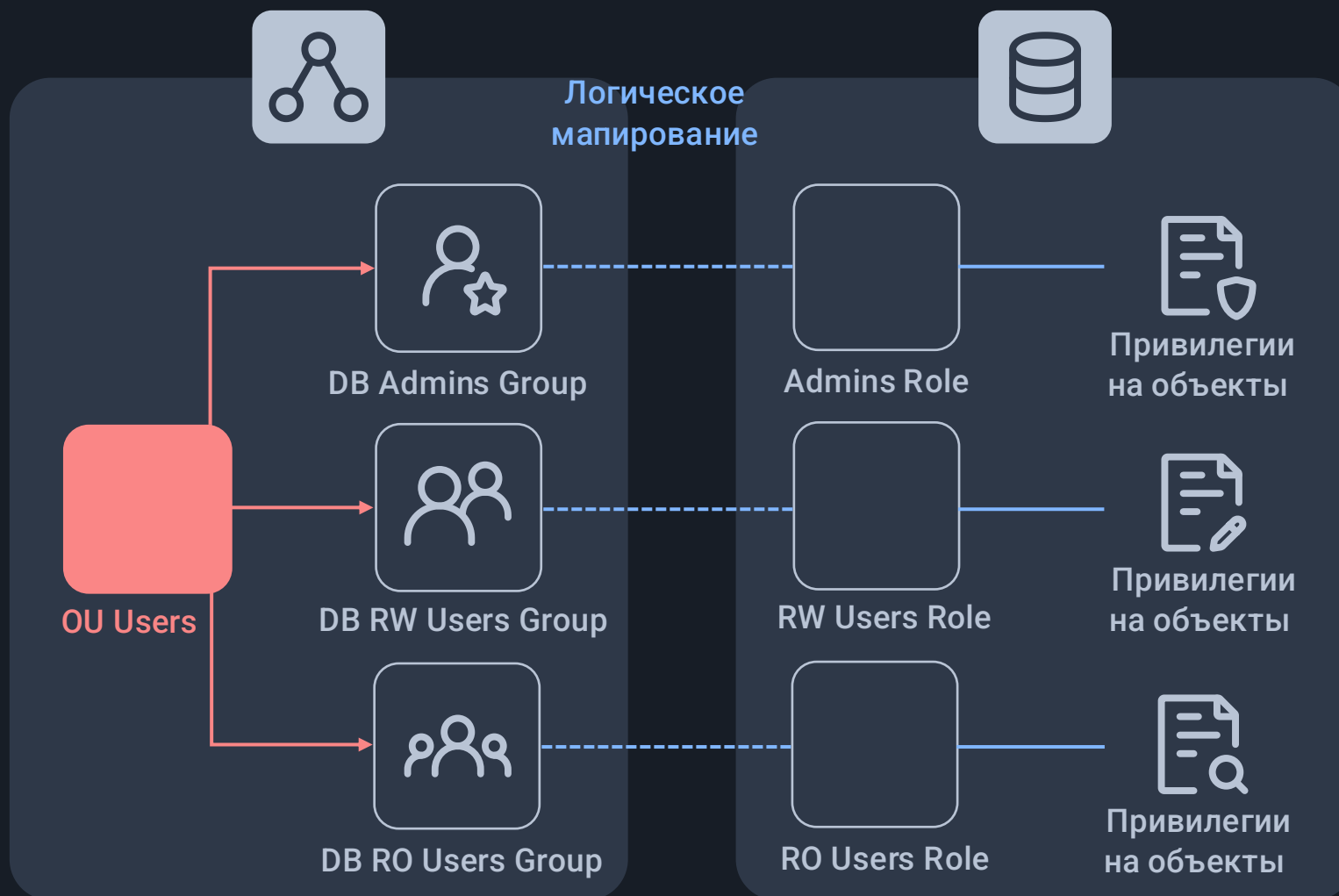
Синхронизация ролей и привилегий СУБД с группами LDAP



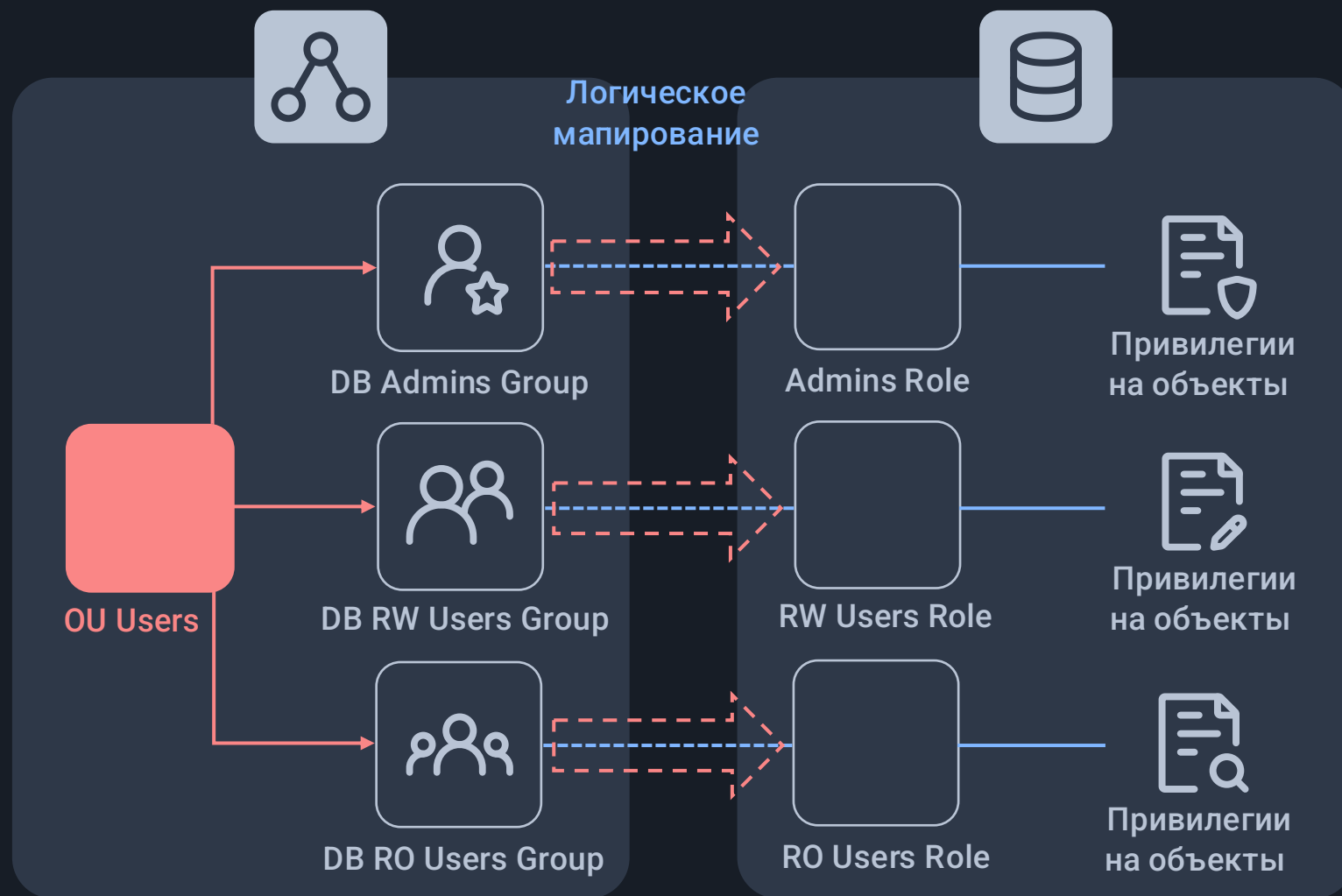
Синхронизация ролей и привилегий СУБД с группами LDAP



Синхронизация ролей и привилегий СУБД с группами LDAP

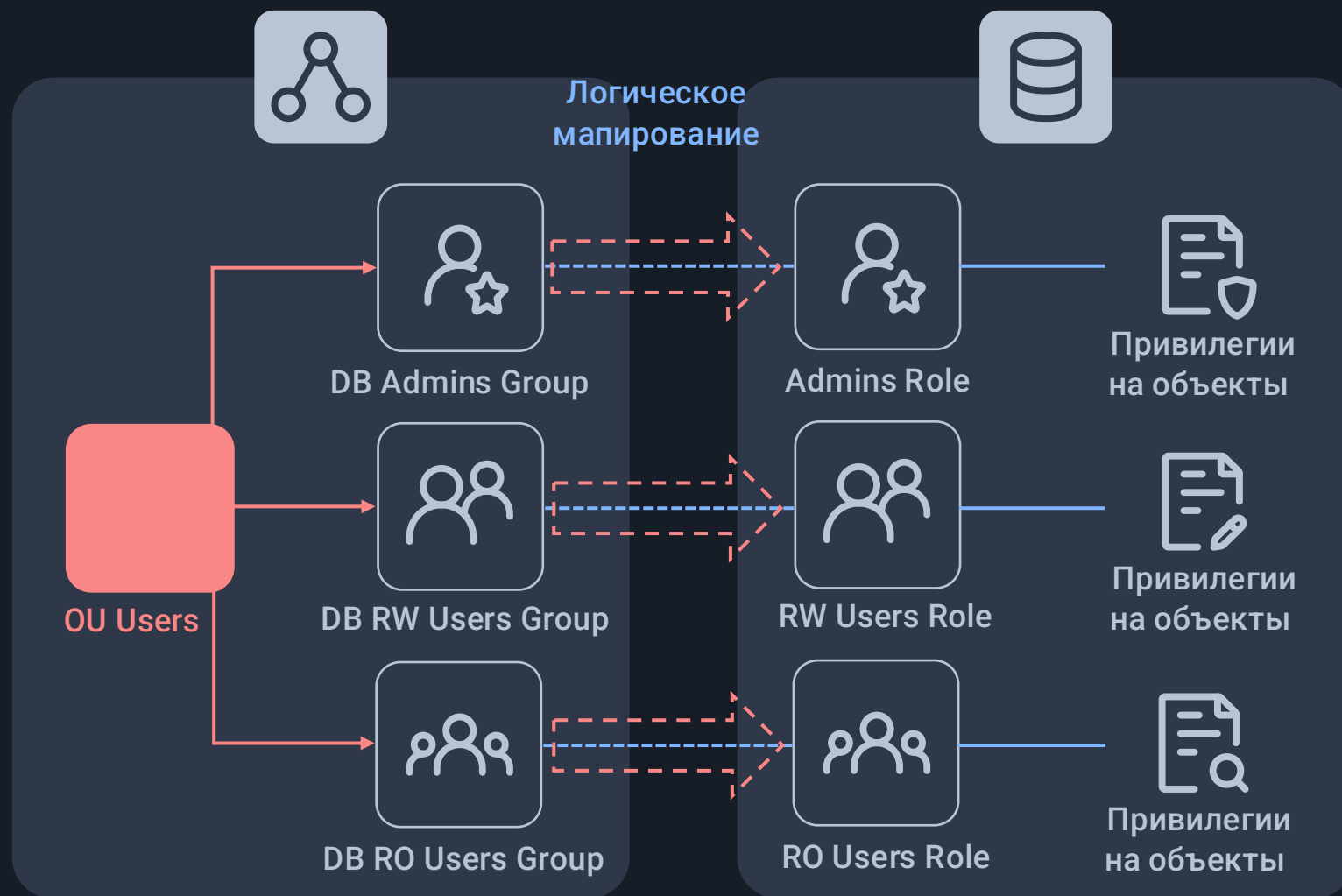


Синхронизация ролей и привилегий СУБД с группами LDAP

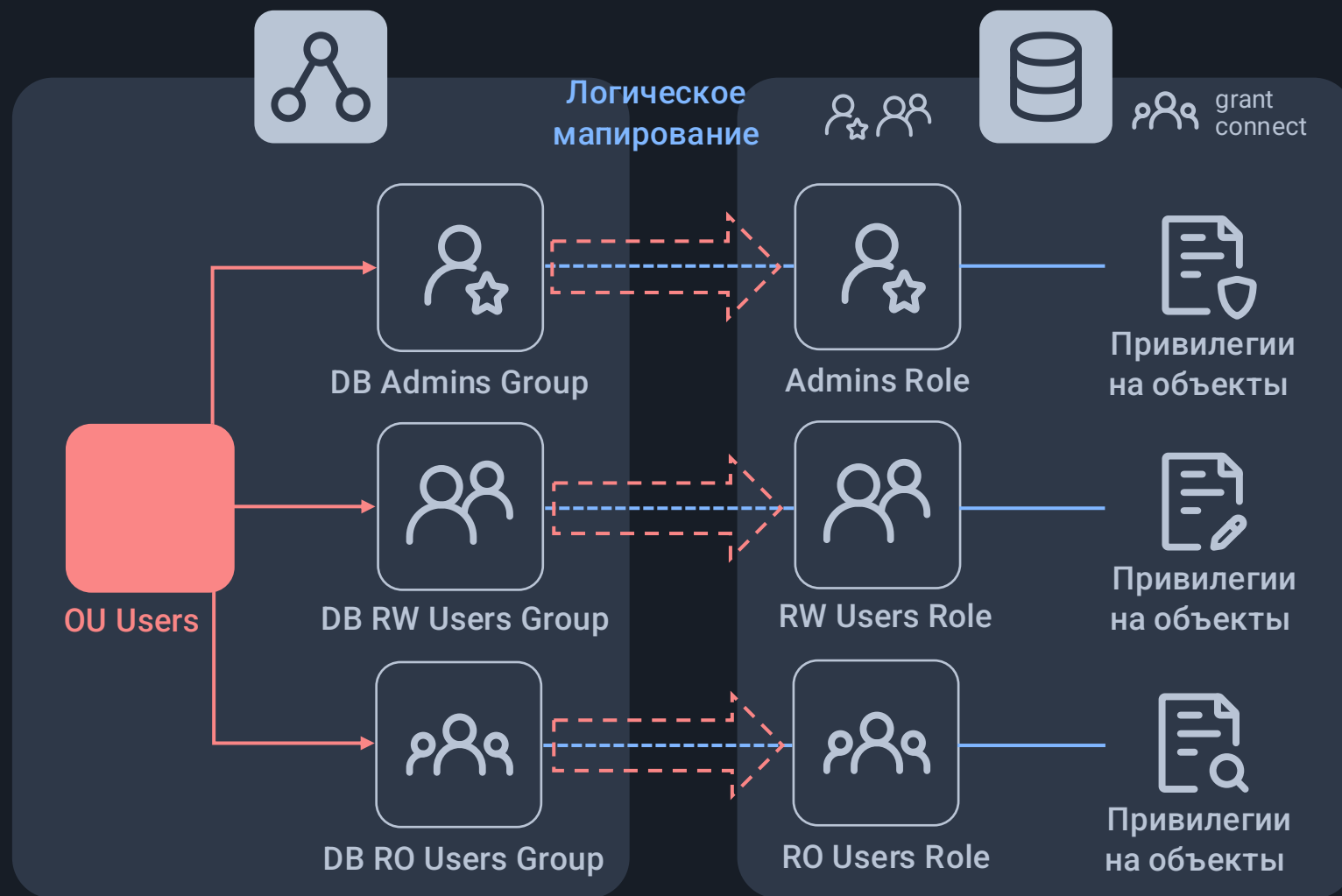


Синхронизация

Синхронизация ролей и привилегий СУБД с группами LDAP

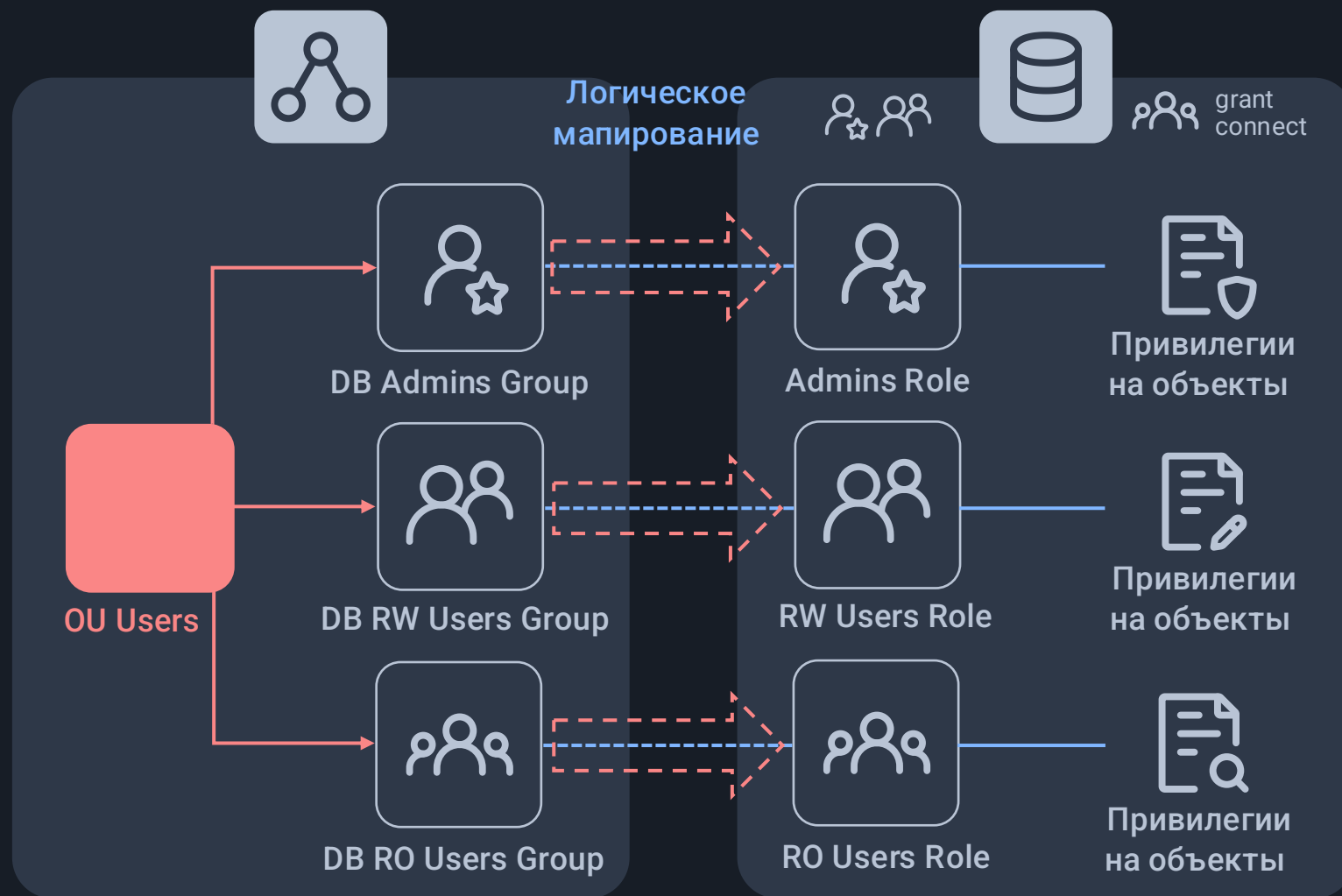


Синхронизация ролей и привилегий СУБД с группами LDAP



Синхронизация

Синхронизация ролей и привилегий СУБД с группами LDAP



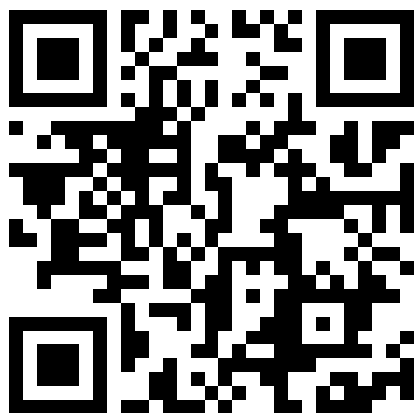
На базе расширения `ldap2pg` происходит периодический опрос состава выделенных групп каталога, сравнение с составом связанных групповых ролей СУБД и формирование набора применяемых к СУБД изменений (CREATE, DROP и ALTER)

Доступно, начиная с 16.11.1 в STD и ENT

Технологическое партнерство

Взаимная сертификация технологий

Совместно с компанией «Астра» подготовлена детальная инструкция по настройке LDAP-аутентификации и синхронизации ролей и привилегий с группами ALD Pro



postgrespro.ru/materials



СЕРТИФИКАТ СОВМЕСТИМОСТИ

Настоящим сертификатом
ООО «ППГ» и ООО «РусБИТех-Астра» подтверждают взаимную совместимость и
корректность работы программных продуктов

«ALD Pro – 3.0» и «Postgres Pro – 17»

Сертификат оформлен по результатам тестовых
испытаний проведенных специалистами компаний
ООО «ППГ» и ООО «РусБИТех-Астра»

Сценарий интеграции: аутентификация по протоколу LDAP,
синхронизация ролей и привилегий с группами LDAP



Дата выдачи:
28.10.2025



Директор сервисного центра
ООО «РусБИТех-Астра»
А. С. Фоменко



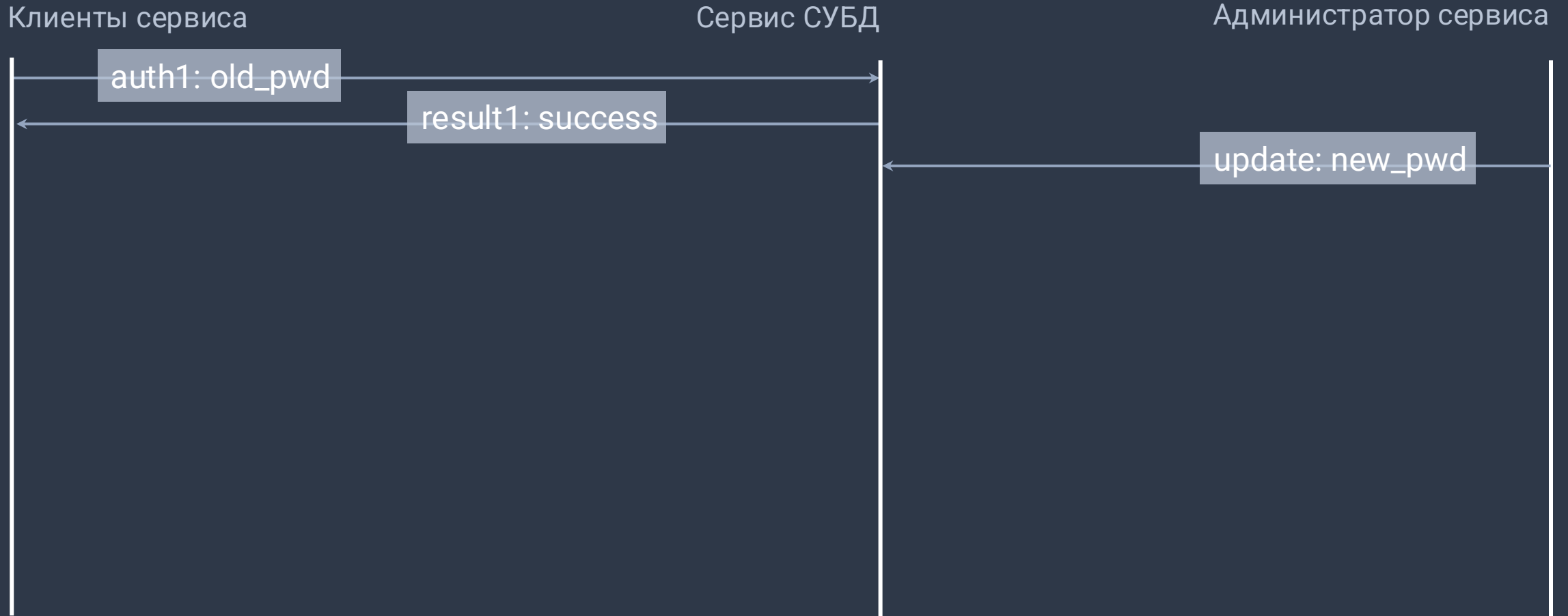
Генеральный директор компании
Postgres Professional
И. Е. Панченко

Новые решения для ИБ

2026H1

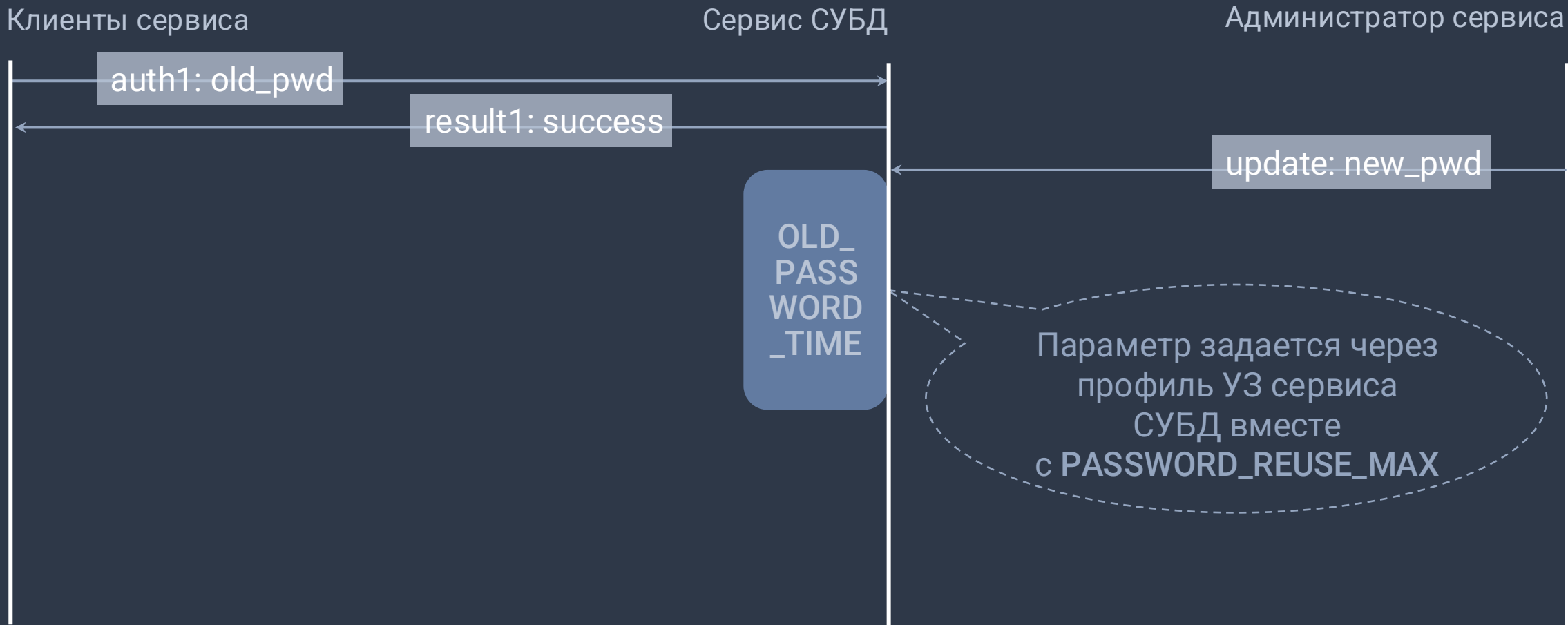
Отложенное изменение пароля

Временное сосуществование старого и нового пароля при смене



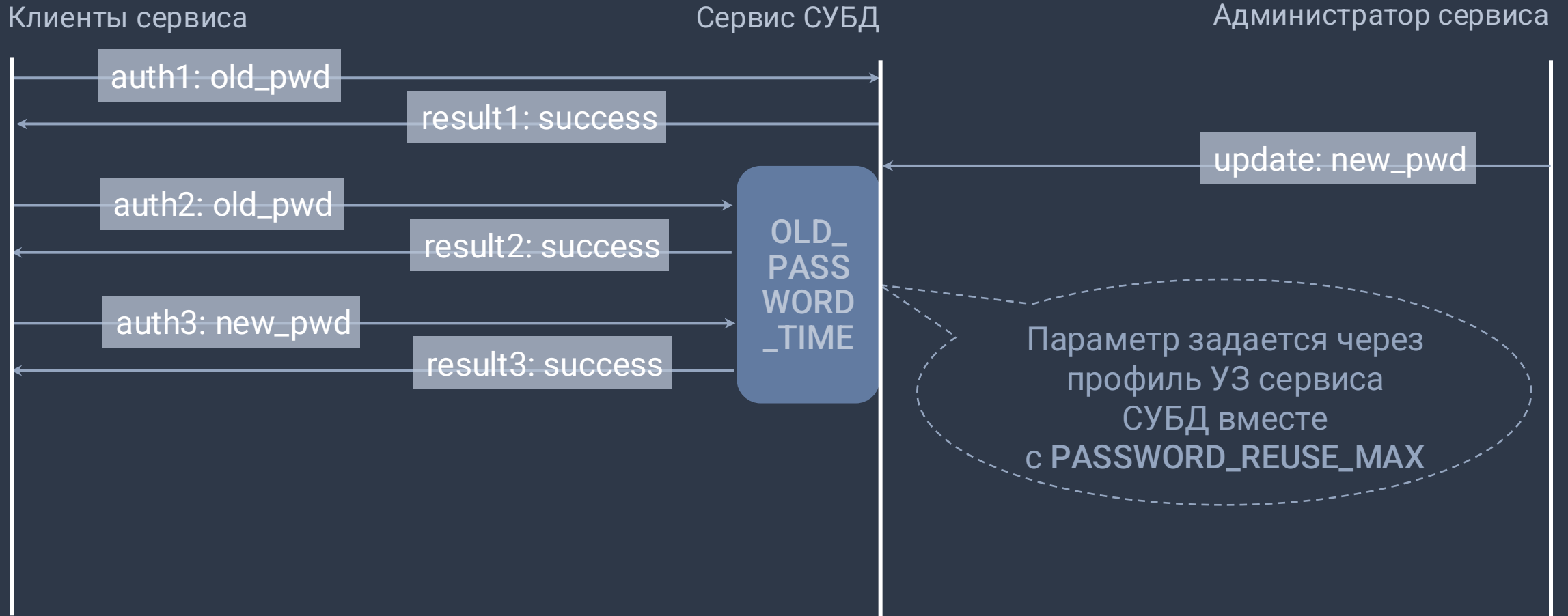
Отложенное изменение пароля

Временное сосуществование старого и нового пароля при смене



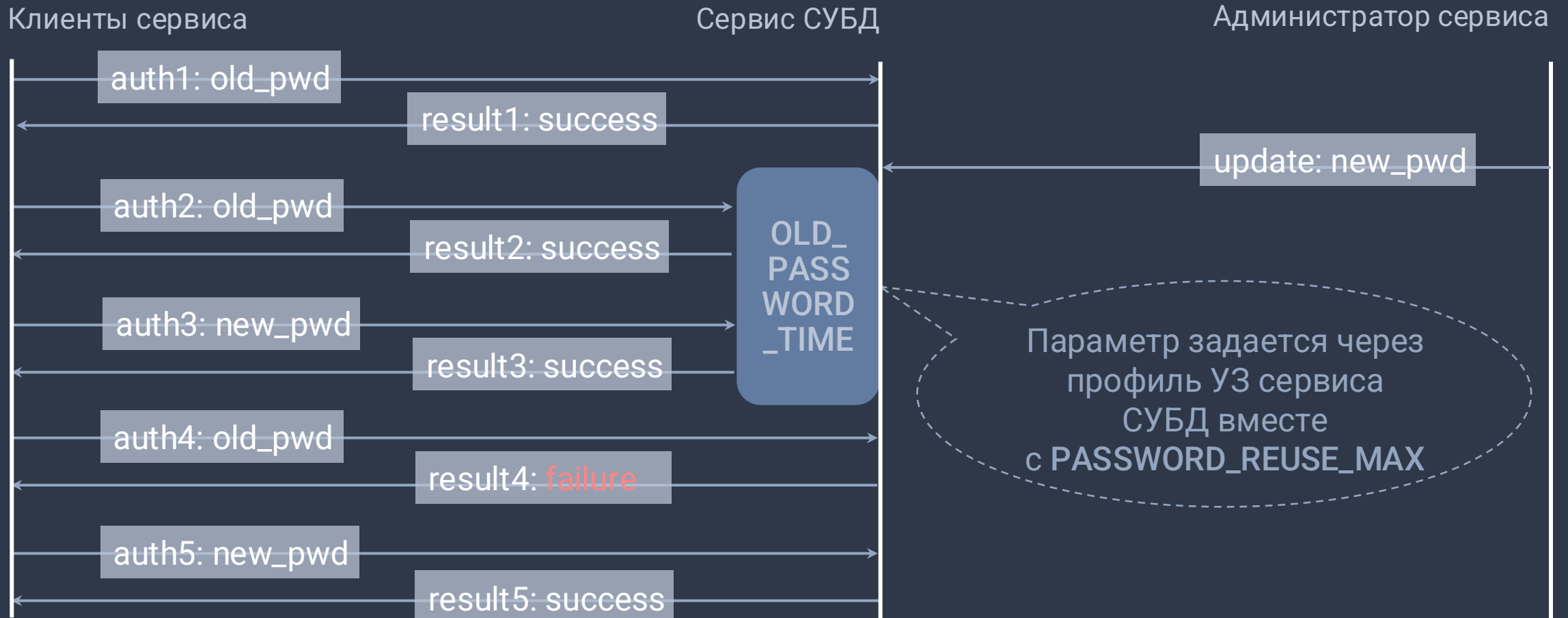
Отложенное изменение пароля

Временное сосуществование старого и нового пароля при смене



Отложенное изменение пароля

Временное сосуществование старого и нового пароля при смене



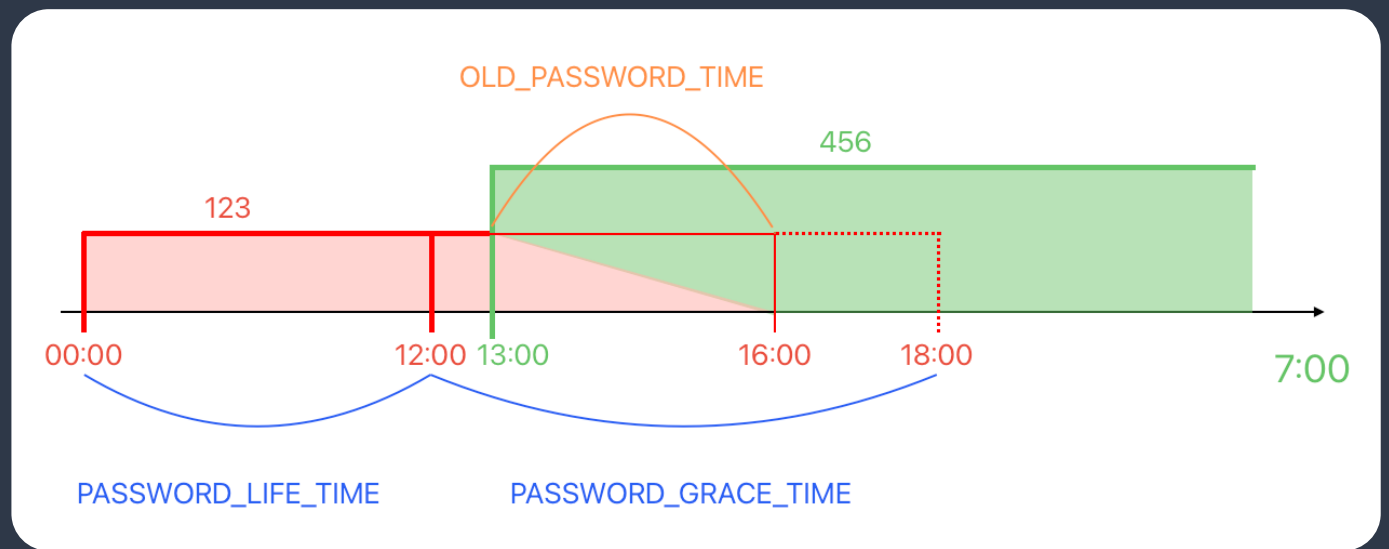
Особенности решения, доступного в 18 версии STD и ENT

- Пароль может стать «старым», только если на момент установки нового пароля он ещё валиден
- В качестве параметров password_encryption поддерживаются md5 и scram-sha-256
- Клиент получает оповещение с предложением сменить пароль на новый
- Продленное время жизни пароля может быть сокращено новой настройкой

Особенности решения, доступного в 18 версии STD и ENT

- Пароль может стать «старым», только если на момент установки нового пароля он ещё валиден
- В качестве параметров password_encryption поддерживаются md5 и scram-sha-256
- Клиент получает оповещение с предложением сменить пароль на новый
- Продленное время жизни пароля может быть сокращено новой настройкой
- На графике - пример со следующими параметрами:

- PASSWORD_LIFE_TIME
(время жизни пароля) = 12 часов
- PASSWORD_GRACE_TIME
(дополнительное время жизни пароля) = 6 часов
- OLD_PASSWORD_TIME
(время жизни старого пароля)
= 3 часа



Оценка уровня уязвимости СУБД включает в себя в том числе **классификацию** конфиденциальной и персональной информации

Перед применением средств защиты (например – маскирования данных) необходимо:

- Установить, в каких полях каких таблиц содержатся чувствительные данные (т.е. зафиксировать их **размещение**)
- Определить условия применения средств защиты (т.е. **политики**)
- Выбрать **алгоритмы** защиты

Вышеперечисленные действия можно определить как **ведение справочника** чувствительных данных, который может быть создан вручную или автоматически

При создании справочника вручную команда разработчиков на основе знания структуры СУБД может перечислить все поля, содержащие конфиденциальные данные

Но, т.к. в процессе эксплуатации возможно внесение изменений в структуру СУБД, предпочтительным методом является разведка чувствительных данных с автоматическим пополнением справочника

Поиск чувствительной информации

Как найти данные, которые надо защищать?

Для разведки используется мета-словарь, содержащий маски для проверки имен и содержимого полей (в т.ч. JSON) по набору регулярных выражений и константным значениям (названия организаций, фамилии и т. д.)

Поиск чувствительной информации

Как найти данные, которые надо защищать?

Для разведки используется мета-словарь, содержащий маски для проверки имен и содержимого полей (в т.ч. JSON) по набору регулярных выражений и константным значениям (названия организаций, фамилии и т. д.)

```
scout:
  column_names:
    matchers:
      - key: passport
        match_values: [passport, passports]
      - key: namecolumn
        pattern: (name|contact)
    column_values:
      case_sensitive: false
      matchers:
        - key: russian_surnames
          case_sensitive: false # the
option is optional, might be deleted
          pattern: (OVA|EVA|NOV|MOV|KOV)$
        - key: emailfield
          case_sensitive: false
          pattern: (email)
        - key: email_pattern
          case_sensitive: false
          pattern: ([A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.(ru|com))
        - key: phonefield
          case_sensitive: false
          pattern: (phone)
      exclude:
        schemas:
          - pgpro_sfile_data
          - dbms_lob
          - profile
          - information_schema
          - pg_catalog
          - pg_toast
        column_types:
          - dbms_lob.blob
          - dbms_lob.clob
          - sfile
```

Поиск чувствительной информации

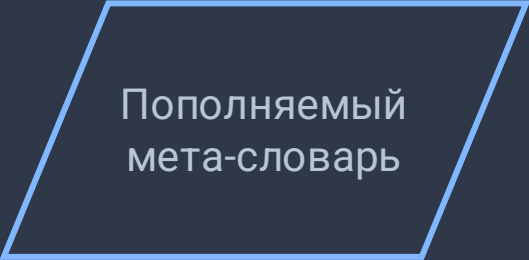
Как найти данные, которые надо защищать?

Для разведки используется мета-словарь, содержащий маски для проверки имен и содержимого полей (в т.ч. JSON) по набору регулярных выражений и константным значениям (названия организаций, фамилии и т. д.)

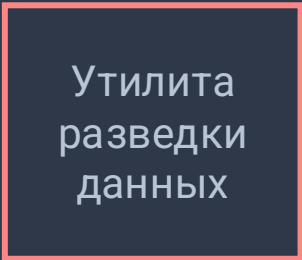
```
scout:
  column_names:
    matchers:
      - key: passport
        match_values: [passport, passports]
      - key: namecolumn
        pattern: (name|contact)
    column_values:
      case_sensitive: false
      matchers:
        - key: russian_surnames
          case_sensitive: false # the
option is optional, might be deleted
          pattern: (OVA|EVA|NOV|MOV|KOV)$
        - key: emailfield
          case_sensitive: false
          pattern: (email)
        - key: email_pattern
          case_sensitive: false
          pattern: {[A-Za-z0-9._%+ ]+@[A-Za-z0-9.-]+\.(ru|com)}
        - key: phonefield
          case_sensitive: false
          pattern: (phone)
      exclude:
        schemas:
          - pgpro_sfile_data
          - dbms_lob
          - profile
          - information_schema
          - pg_catalog
          - pg_toast
        column_types:
          - dbms_lob.blob
          - dbms_lob.clob
          - sfile
```

Утилита для поиска чувствительной информации

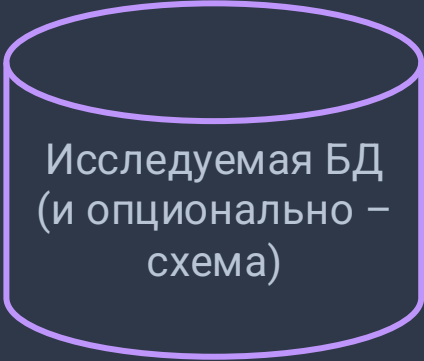
```
./bin/pgpro_scout inspect -f scout.yml -d demo -h localhost -p 5432 -U postgres --search-path=bookings -o report.csv
```



Пополняемый
мета-словарь



Утилита
разведки
данных



Исследуемая БД
(и опционально –
схема)

Утилита для поиска чувствительной информации

```
./bin/pgpro_scout inspect -f scout.yml -d demo -h localhost -p 5432 -U postgres --search-path=bookings -o report.csv
```

Пополняемый
мета-словарь

Утилита
разведки
данных

Исследуемая БД
(и опционально –
схема)

Пополняемый
и редактируемый
справочник

Утилита для поиска чувствительной информации

```
./bin/pgpro_scout inspect -f scout.yml -d demo -h localhost -p 5432 -U postgres --search-path=bookings -o report.csv
```

Пополняемый
мета-словарь

Утилита
разведки
данных

Исследуемая БД
(и опционально –
схема)

Пополняемый
и редактируемый
справочник



Сотрудник
отдела ИБ

Утилита для поиска чувствительной информации

```
./bin/pgpro_scout inspect -f scout.yml -d demo -h localhost -p 5432 -U postgres --search-path=bookings -o report.csv
```

Пополняемый
мета-словарь

Утилита
разведки
данных

Исследуемая БД
(и опционально –
схема)

Пополняемый
и редактируемый
справочник

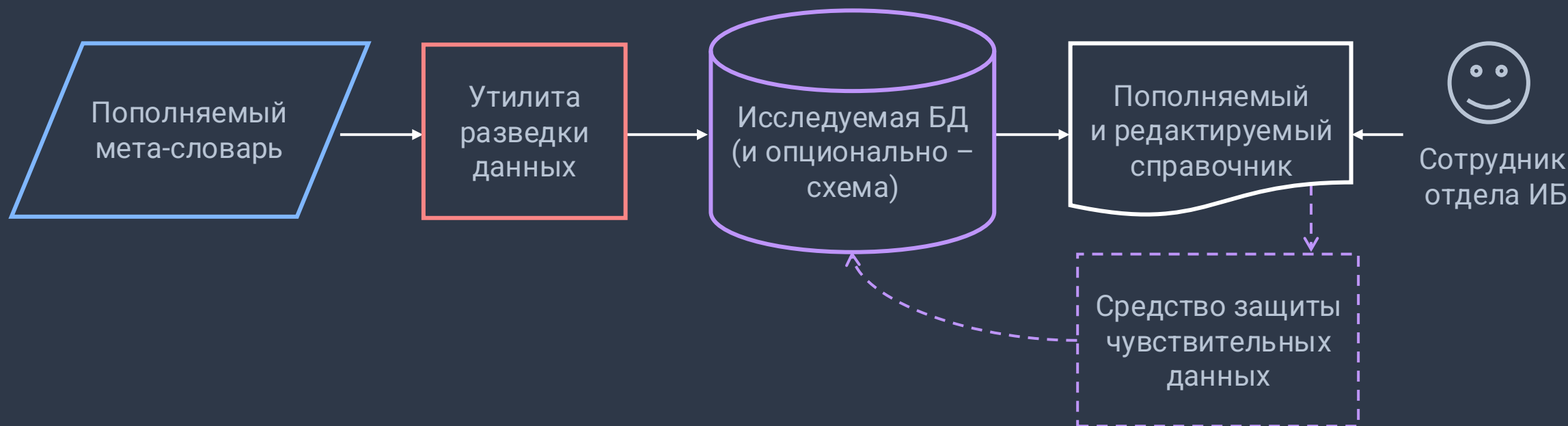


Сотрудник
отдела ИБ

- Результаты разведки в справочнике анализирует сотрудник отдела ИБ, уточняя политики и методы защиты (в отношении каких ролей, статическое или динамическое маскирование, TDE и т.п.)
- Будет бэкпорт, будет доступно в STD

Утилита для поиска чувствительной информации

```
./bin/pgpro_scout inspect -f scout.yml -d demo -h localhost -p 5432 -U postgres --search-path=bookings -o report.csv
```



- Результаты разведки в справочнике анализирует сотрудник отдела ИБ, уточняя политики и методы защиты (в отношении каких ролей, статическое или динамическое маскирование, TDE и т.п.)
- Будет бэкпорт, будет доступно в STD

Отчет утилиты разведки чувствительных данных

| #report time: 2025-09-23T07:05:12-04:00 | | | | | |
|---|------------------------|----------------|------------------|---------|--|
| matcher | location | column | key | comment | sample |
| column_name | bookings.airports_data | airport_name | namecolumn | | airport_name |
| column_name | bookings.tickets | contact_data | namecolumn | | contact_data |
| column_name | bookings.tickets | passenger_name | namecolumn | | passenger_name |
| column_value | bookings.tickets | contact_data | phonefield | | {"phone": "+70127117011"} |
| column_value | bookings.tickets | passenger_name | russian_surnames | | VALERIY TIKHONOV |
| column_value | bookings.tickets | contact_data | phonefield | | {"phone": "+70378089255"} |
| column_value | bookings.tickets | passenger_name | russian_surnames | | EVGENIYA ALEKSEEVA |
| column_value | bookings.tickets | contact_data | phonefield | | {"phone": "+70760429203"} |
| column_value | bookings.tickets | passenger_name | russian_surnames | | ARTUR GERASIMOV |
| column_value | bookings.tickets | contact_data | emailfield | | {"email": "volkova.alina_03101973@postgrespro.ru", "phone": "+70582584031"} |
| column_value | bookings.tickets | contact_data | email_pattern | | {"email": "volkova.alina_03101973@postgrespro.ru", "phone": "+70582584031"} |
| column_value | bookings.tickets | contact_data | phonefield | | {"email": "volkova.alina_03101973@postgrespro.ru", "phone": "+70582584031"} |
| column_value | bookings.tickets | passenger_name | russian_surnames | | ALINA VOLKOVA |
| column_value | bookings.tickets | contact_data | emailfield | | {"email": "m-zhukov061972@postgrespro.ru", "phone": "+70149562185"} |
| column_value | bookings.tickets | contact_data | email_pattern | | {"email": "m-zhukov061972@postgrespro.ru", "phone": "+70149562185"} |
| column_value | bookings.tickets | contact_data | phonefield | | {"email": "m-zhukov061972@postgrespro.ru", "phone": "+70149562185"} |
| column_value | bookings.tickets | passenger_name | russian_surnames | | MAKSIM ZHUKOV |
| column_value | bookings.tickets | contact_data | emailfield | | {"email": "kuznecova-t-011961@postgrespro.ru", "phone": "+70400736223"} |
| column_value | bookings.tickets | contact_data | email_pattern | | {"email": "kuznecova-t-011961@postgrespro.ru", "phone": "+70400736223"} |
| column_value | bookings.tickets | contact_data | emailfield | | {"email": "antonova.irina04121972@postgrespro.ru", "phone": "+70844502960"} |
| column_value | bookings.tickets | contact_data | email_pattern | | {"email": "antonova.irina04121972@postgrespro.ru", "phone": "+70844502960"} |
| column_value | bookings.tickets | contact_data | emailfield | | {"email": "kuznecova.valentina10101976@postgrespro.ru", "phone": "+70268080457"} |
| column_value | bookings.tickets | contact_data | email_pattern | | {"email": "kuznecova.valentina10101976@postgrespro.ru", "phone": "+70268080457"} |

Обфускация кода хранимых функций и процедур

Что хочется предотвратить:

- Несанкционированные правки кода
- Лишние вопросы о тех или иных решениях в коде

Как добавляется защита:

Encode (convert_to (<текст создания функции или любой произвольный текст>, 'UTF8'), <алгоритм (например, 'base64' или XOR кодирование по фиксированному hardcoded ключу)>) + сжатие

Как СУБД понимает, что код защищен:

- Реализована механика экранирования текста меткой `$_PGPROwrapped_` с двух сторон.
- Экранированный таким образом текст воспринимается, как скрипт в base64. Он сначала декодируется, а затем выполняется.

```
$_PGPROwrapped_ $U0VMRUNUIDE7Cg==$_PGPROwrapped_ $;  
?column? |  
-----+  
1 |
```

Особенности выполнения защищенного кода:

- Реализован вложенный механизм повторного кодирования тел функций, если скрипт их создания был закодирован
- Раскодированная функция обеспечит интерактивное взаимодействие, сообщив например о невозможности выполнения скрипта с синтаксическими ошибками
- Можно использовать вложенные закодированные функции, при этом сначала выделится тело функции и закодируется обратно, а затем будет создана функция с закодированным телом
- Незначительный оверхэд (~10% по сравнению с отсутствием защиты)
- Ожидается в ближайших минорных релизах

**Ответим на ваши
вопросы!**