КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | ИРКУТСК

25.05.2023

Обо мне

Владимир Ковалев

- От админа, до Java разработчика
- От 1С программиста, до начальника отдела ИТ и руководителя проекта внедрения ERP системы Microsoft Axapta
- От замдиректора завода по ИТ и… обратно к администу и руководству проектами

Более 30 лет в ИТ

IdM, PAM и PKI своими руками

Предпосылки

IdM система

- Проблема «мертвых душ»
- Огромное число пользователей и информационных систем, высокая нагрузка на ИТ и длительные сроки выдачи и отзыва ролей и прав в ИС
- Высокая сложность аудита прав пользователей
- Управление специальными, сервисными и привилегированными учетками в ИС

PAM система

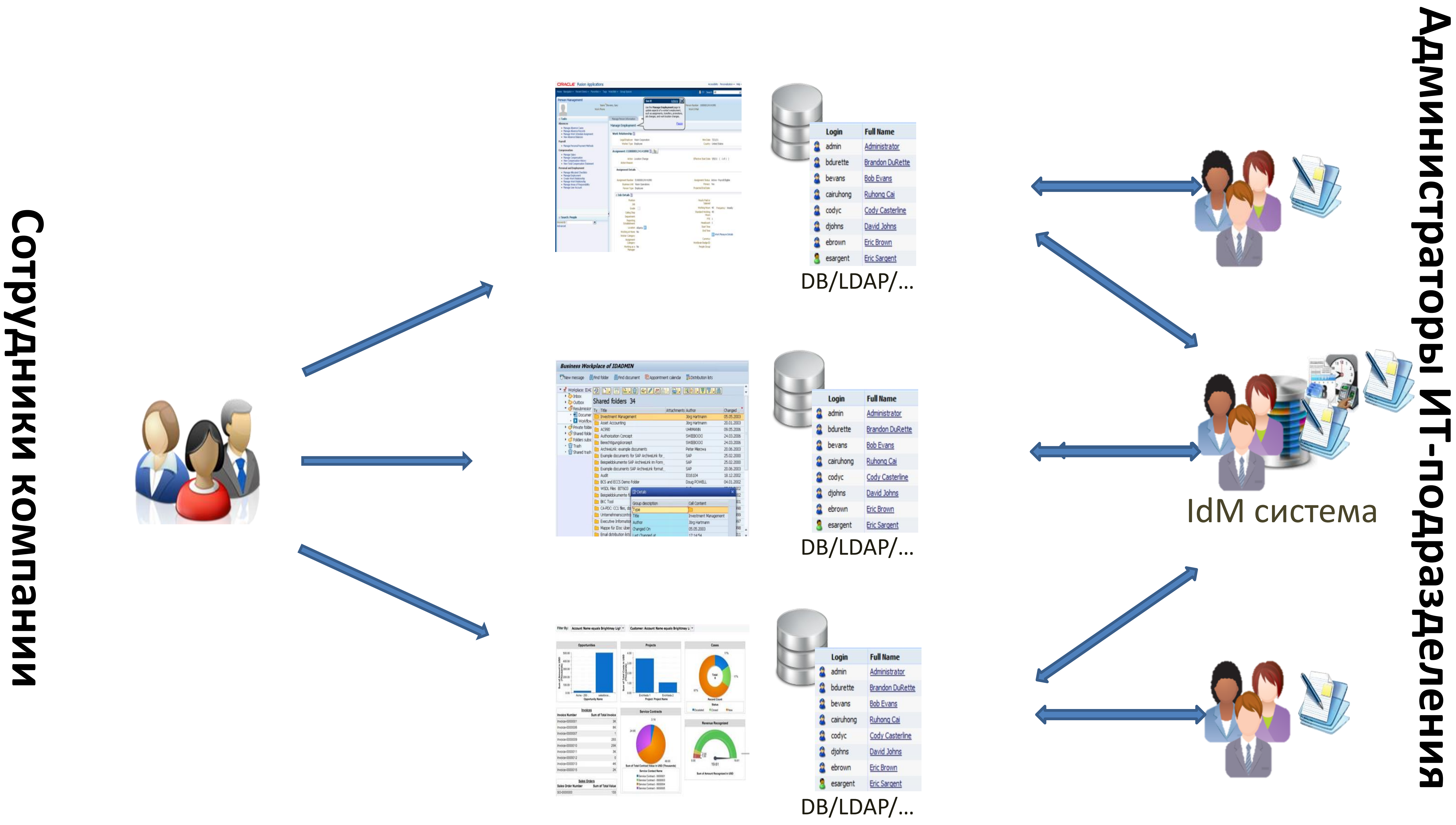
- Большое число привилегированных пользователей и необходимость контроля выполняемых ими работ со стороны ИТ, ИБ и бизнес-заказчиков

PKI система

- Необходимость ведения реестра токенов и смарт-карт
- Управление жизненным циклом сертификатов пользователей и сервисов
- Длительные сроки выпуска сертификатов и сложность их доставки пользователям

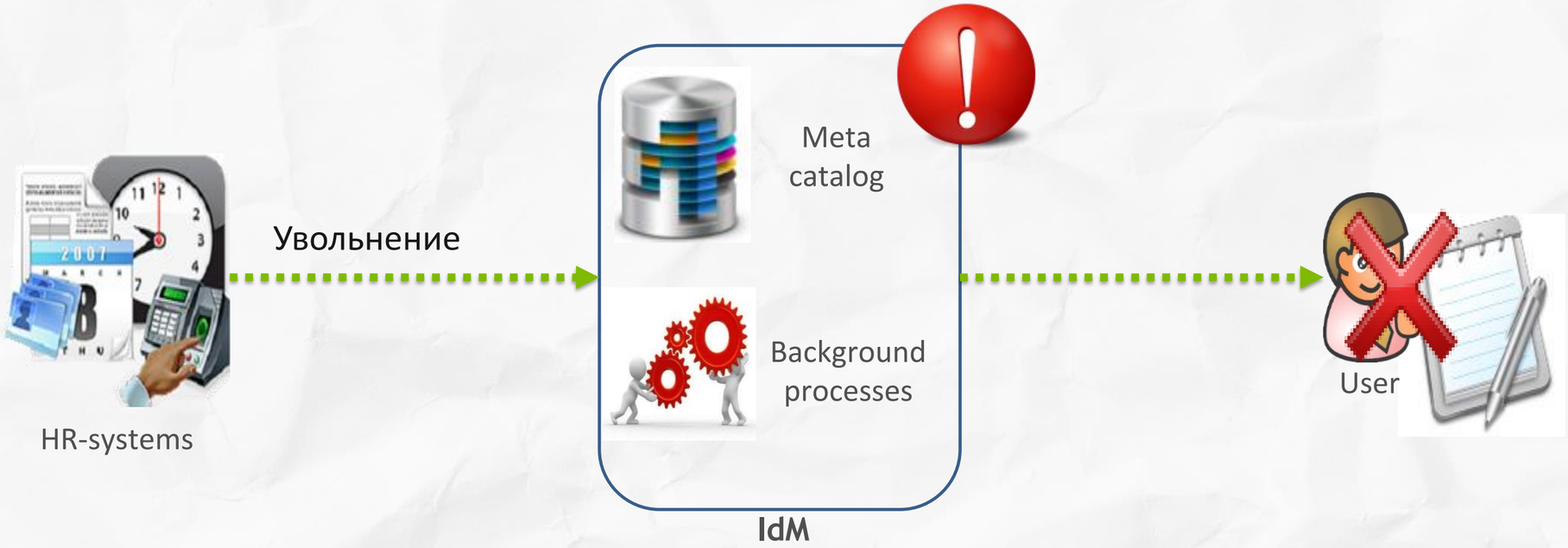
Имеющиеся на рынке решения – не хватает функционала, слабая интеграция продуктов, огромные сроки внедрения и чудовищные деньги

После внедрения IdM системы

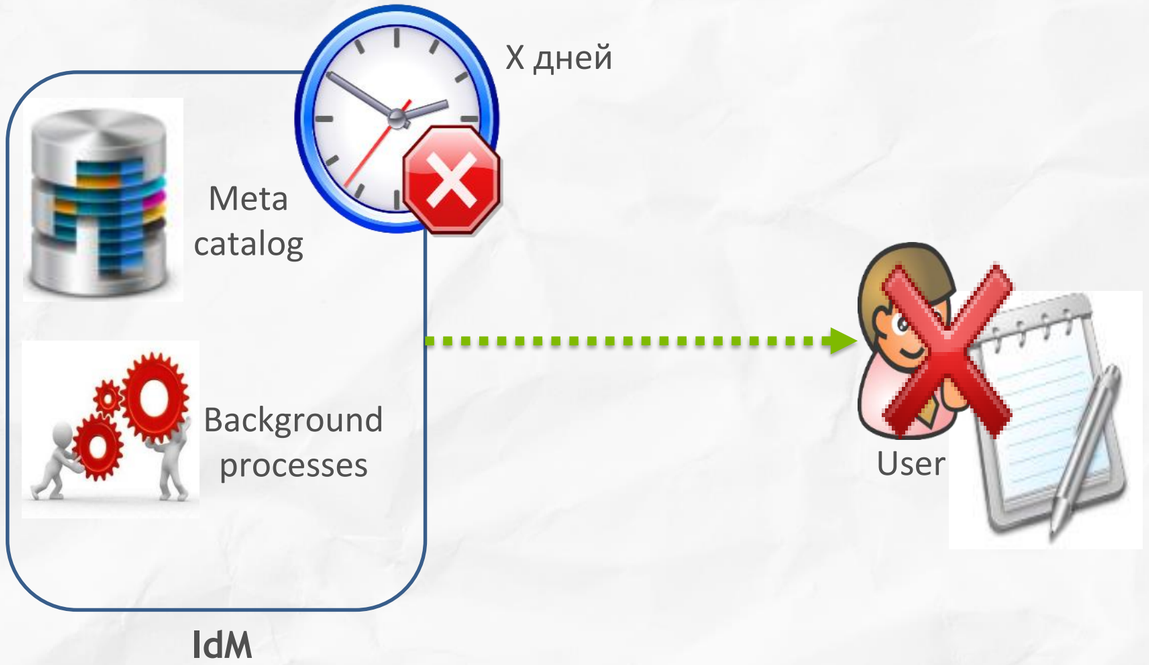


Корпоративные приложения

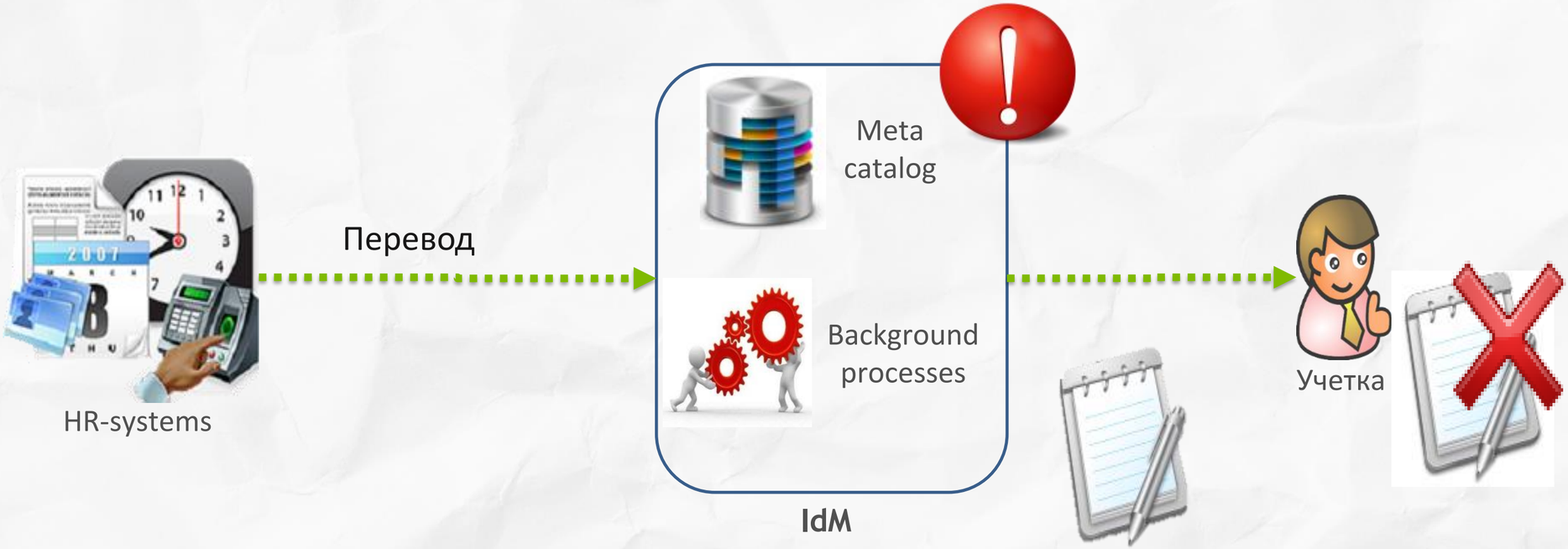
Контроль учеток уволенных сотрудников



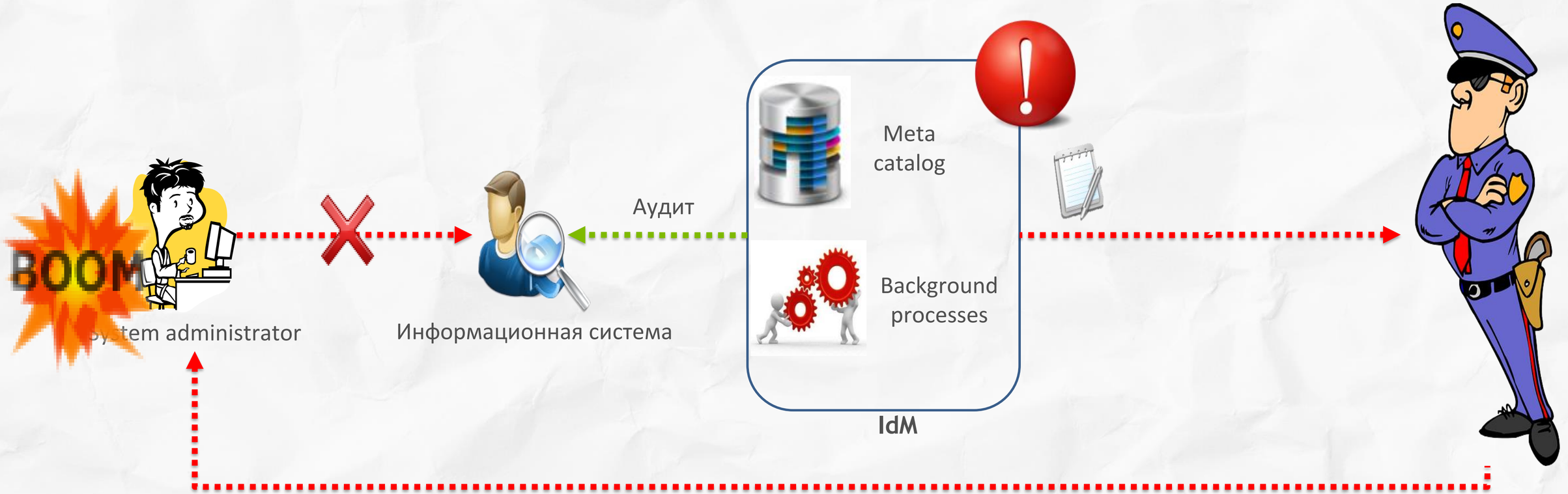
Контроль неактивных учетных записей



Пересмотр прав доступа



Аудит неавторизованных изменений



Ноябрь 2014 – старт проекта IdM

- Microsoft Forefront Identity manager (ныне это Microsoft Identity Manager)
- Консолидируем данные из 14 кадровых источников
- Подключаем одну ИС – MS Active Directory и 4 завода к марту 2015

И тут мы поняли, насколько были неправы

Сентябрь 2015 – рестарт проекта

- Полностью свое ядро
- Полнотекстовый поиск объектов
- API для создания коннекторов к ИС

К декабрю 2016

- Консолидируем данные из 120+ кадровых источников в 17 городах
- Подключаем три ИС:
  - MS Active Directory – 2 шт (суммарно 22.5 тысячи учеток)
  - АСУ ЖДЦ – 1300+ учеток

2017… – подключение прочих систем

- Релиз интеграции с SAP, 1C, Citrix XenApp
- Интеграция с СервисДеск
- Подключение прочих систем
- Атрибутивное управление правами
- SoD контроль
- Управление пользовательскими устройствами и серверами Windows (агент)
- Сбор security логов с DC и прочих приложений
- Конструктор отчетов
- …

Май 2023 – текущее состояние

- Кадровые данные из 252 источников, 113+ тысяч сотрудников и подрядчиков, 158 городов
- 4 домена AD – 92+ тыс учеток
- 237 приложений 1С – 106+ тыс учеток
- 3 SAP/R3 – 19 тыс+ учеток
- 11 прочих приложений, восьми типов
- Более 700 пользователей, 50+ интеграций с другими системами

Время исполнения заявок сократилось с дней до секунд

Октябрь 2021- запуск проекта PAM

- Полностью свое ядро
- Является надстройкой для IdM системы
- Изначально распределенная система, рассчитанная на сотни площадок и тысячи активных пользователей
- Поддержка протоколов RDP/SSH/VNC/Telnet/Kubernetes/Hyper-V
- Кластеризация «из коробки»
- Первая клиентская сессия 05.03.2021, в промышленной эксплуатации с 01.12.2022

Текущее состояние

- 500+ пользователей на 17 площадках
- Более 10тыс сессий, длительностью 20.000+ часов, общим объемом 127Гб

Архитектура PAM

Клиенты (браузер)

HTTPS

HTTPS

Core

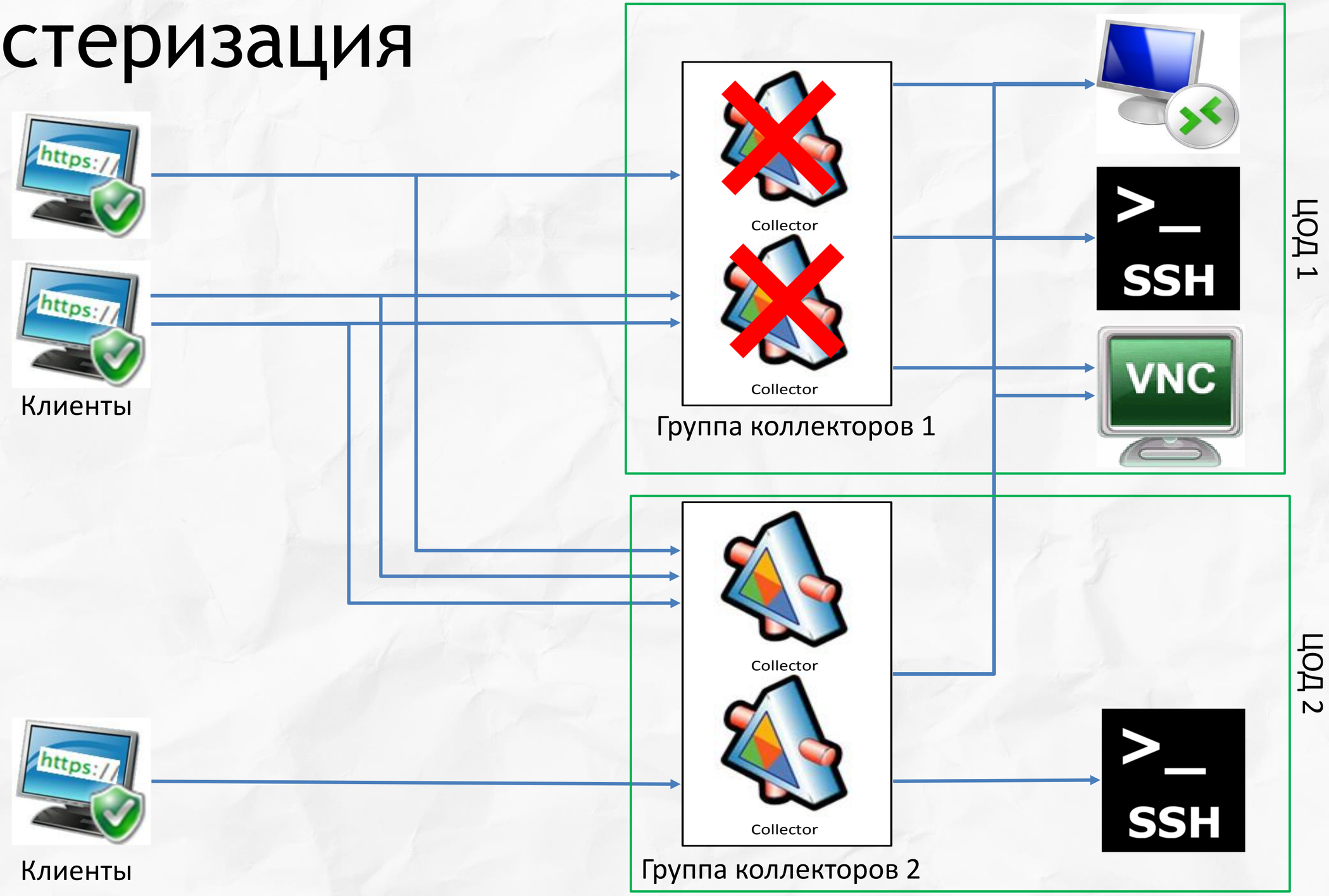
Collector clusters

RDP

SSH

VNC

Кластеризация



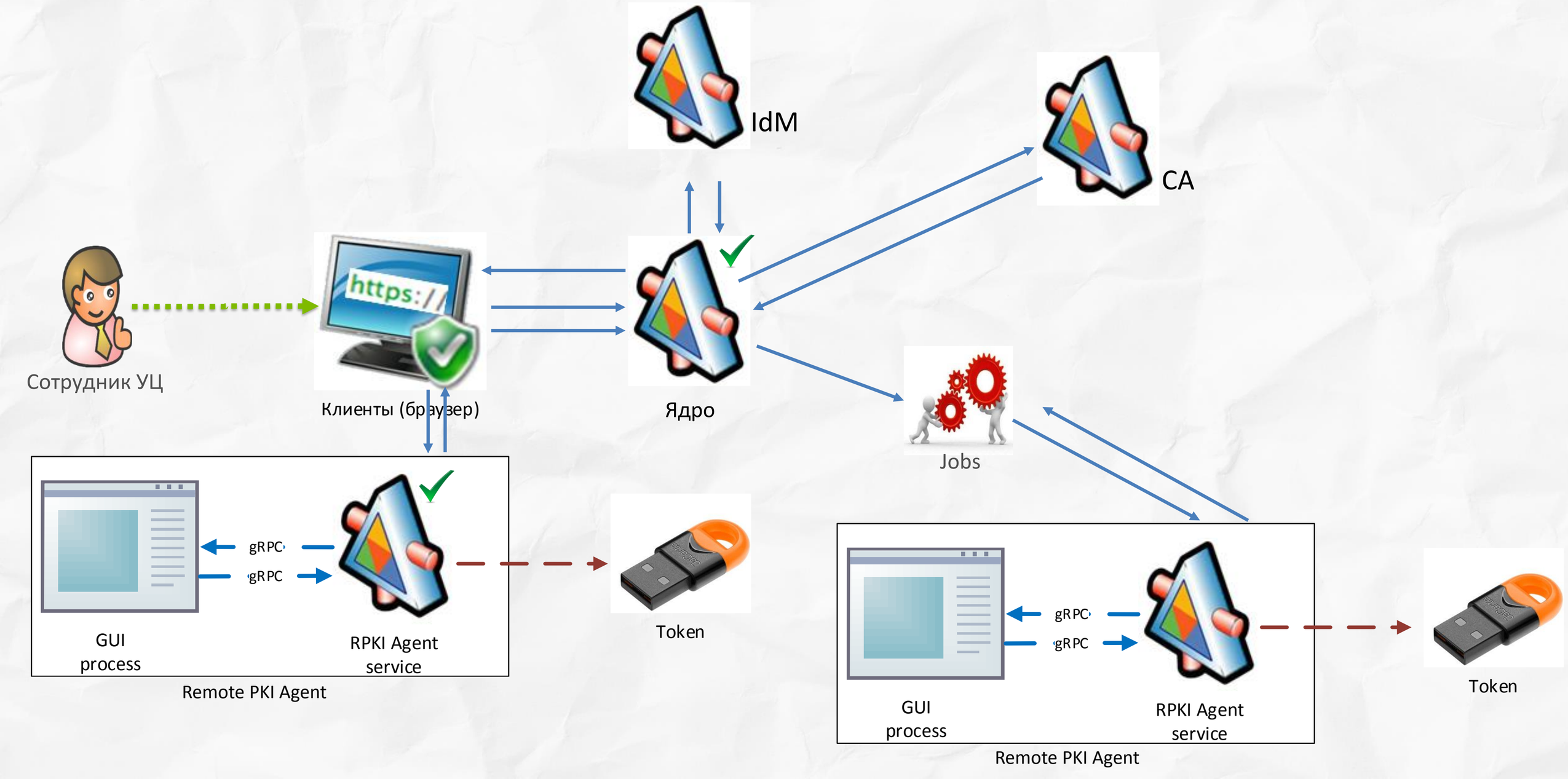
Сентябрь 2022- запуск проекта PKI

- Полностью свое ядро
- Является надстройкой для IdM системы
- Изначально распределенная система, рассчитанная на сотни площадок и десятки тысяч пользователей, тысячи сервисов
- Первая клиентская операция 28.10.2022

Текущее состояние

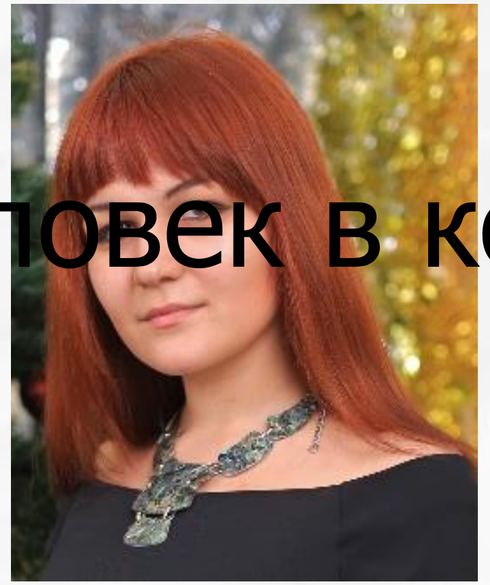
- 25тыс+ пользователей, на всех континентах
- Среднее время выпуска и доставки сертификата – менее минуты

Архитектура PKI - выпуск сертификата



Команда проекта

Сколько человек в команде ?



Готов ответить
на ваши вопросы

E-mail: Vladimir.kovalev2@gmail.com