КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КОД ИБ | Новосибирск

12.10.2023

Владимир Ковалев

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

IdM, PAM и PKI системы

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
- Управление взаимодействием приложений (App2App password management)

PAM система

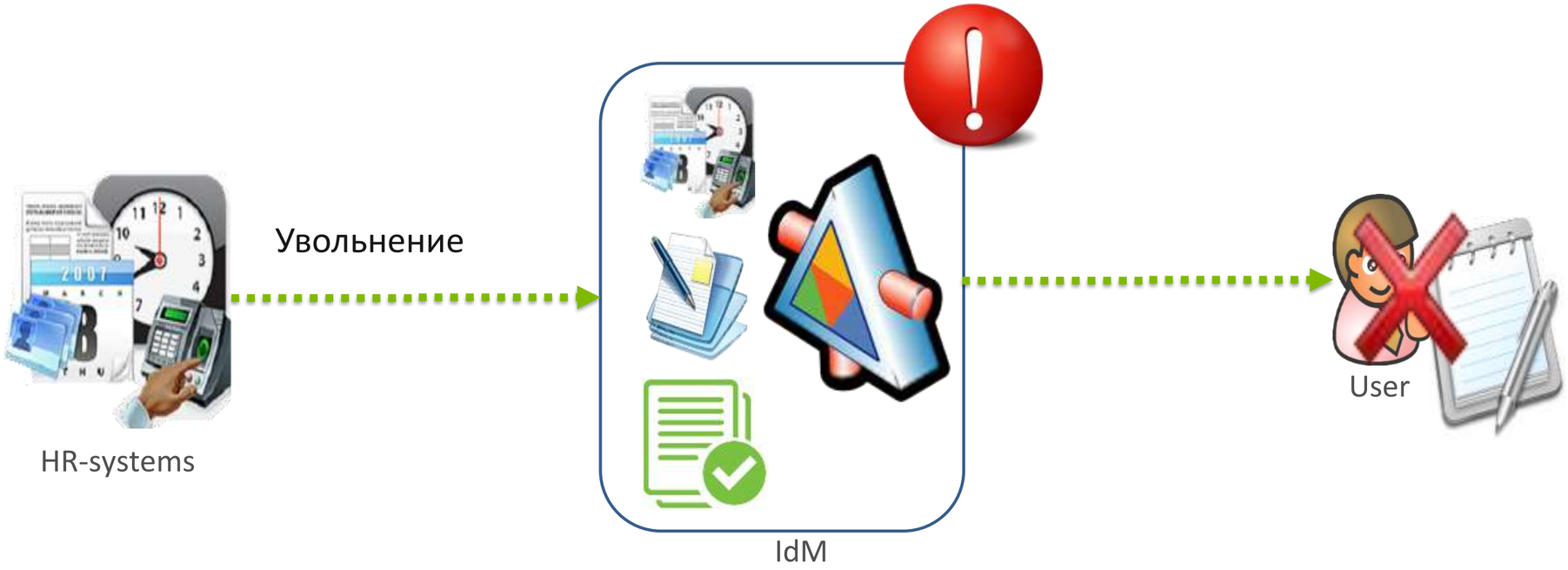
- Большое число привилегированных пользователей, сервисов и оборудования
- Необходимость контроля выполняемых работ со стороны ИТ, ИБ и бизнес-заказчиков

PKI система

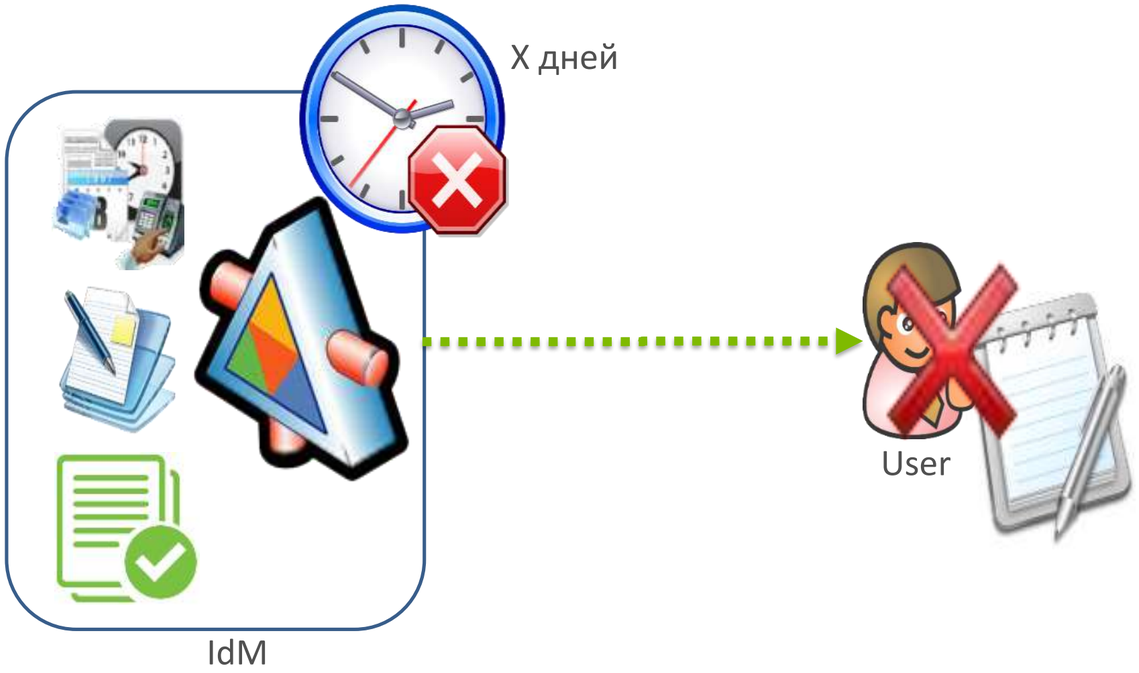
- Необходимость ведения реестра токенов и смарт-карт
- Управление жизненным циклом сертификатов пользователей и сервисов
- Длительные сроки выпуска сертификатов и сложность их доставки пользователям

Логическая схема IdM системы

Контроль учеток уволенных сотрудников

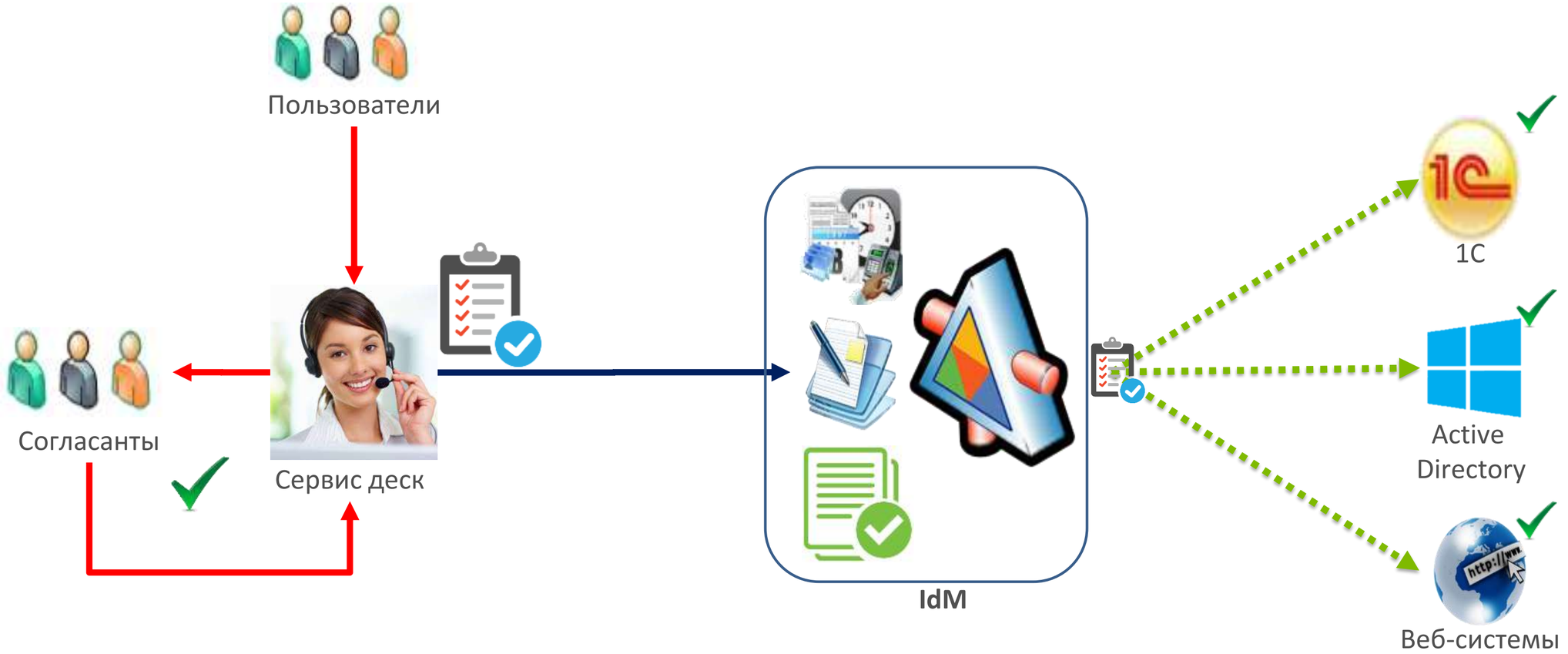


Контроль неактивных учетных записей



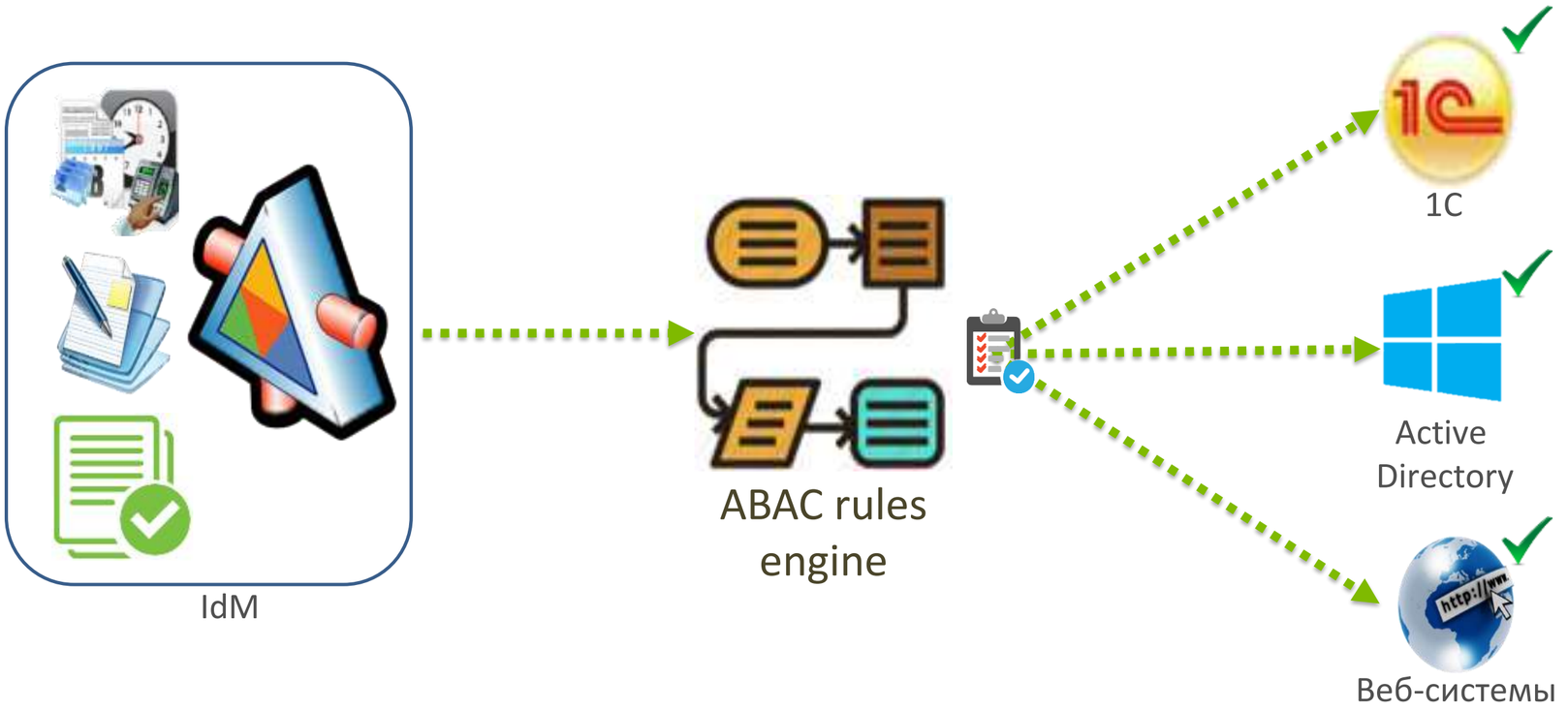
Пересмотр прав доступа

Запрос прав по заявкам



Аудит неавторизованных изменений

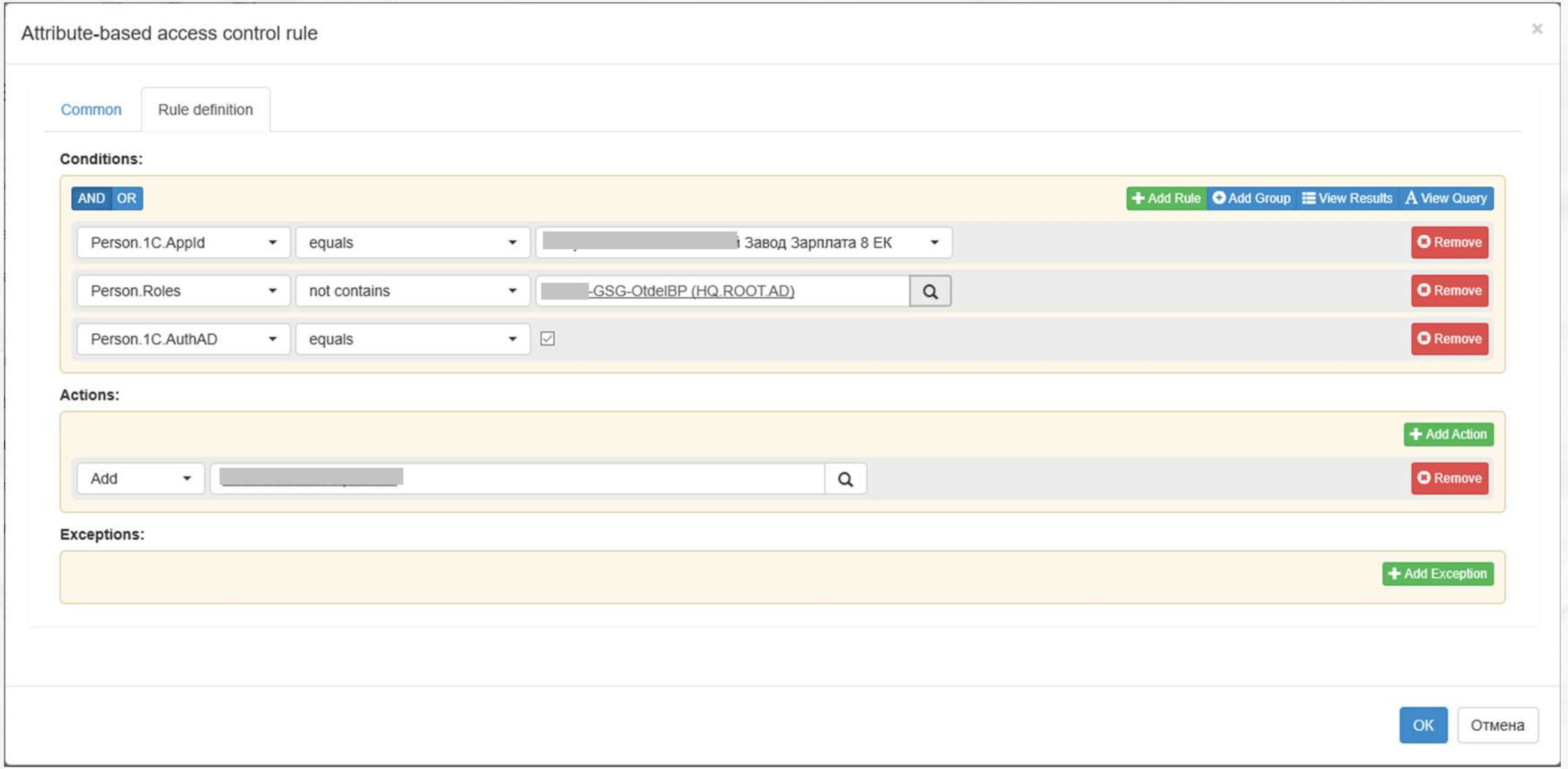
Атрибутивное управление правами



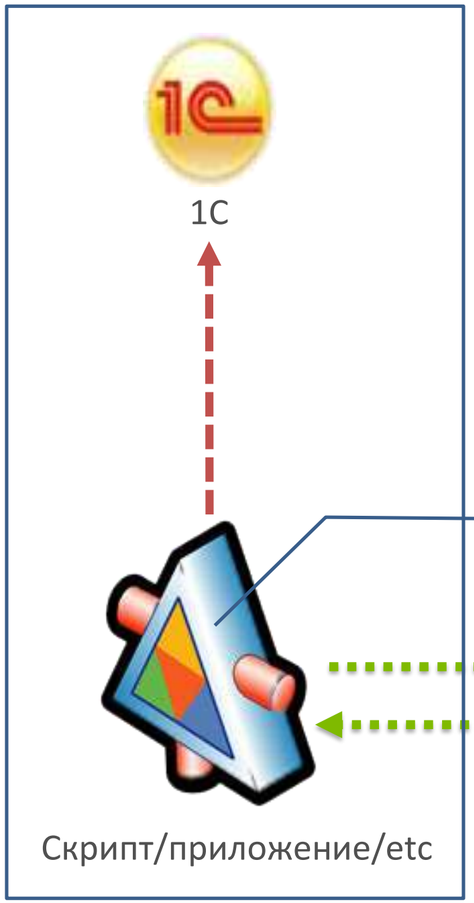
Атрибутивное управление правами

```
IF
   (person.Department -eq ”Finance department” AND
    person.City -eq ”Moscow” AND
    person.AD.HasAccount –eq True AND Person.AD.Enabled = True AND
    person.Roles –contains “somegroup3 (domain.local)”
   )
THEN
{
   KeepState(”somegroup1 (domain.local)”)            // сохранять состояние
   grantRole(”somegroup2 (domain.local)”)            //выдать роль
   revokeRole(” somegroup3 (domain.local)”)          // отозвать роль
   createAccount(“1С Бухгалтерия”)                   // Создание учетной записи в приложении 1С
   grantRole(”Какая то роль 1(1С Бухгалтерия)”)      //выдать роль в приложении 1С
}
```

Атрибутивное управление правами



App2App password management




```
…
$user = "учетная запись"
$pass = "aGjSAv23jh%agj!^%@"
# использование учетки
…
```

App2App password management

Пример скрипта на PowerShell

Было

```
…
$user = 'учетная запись'
$pass = 'kajsghdjhsagj!^%@^"
# использование учетки
…
```

Стало:

```
…
$apiURI = https://IdM.domain.local/API/App2App/getCredential
$cred = Invoke-RestMethod -Method POST -Uri $apiURI -Body "5cb38847-1bb4-4669-af99-bebbe75f832b"
# получение учетных данных в память по токену
# использование учетки
…
```

Управление устройствами

Инструмент сотрудников техподдержки и администраторов

- Управление жизненным циклом учетных записей типа **Computer** в AD
- Включение/выключение/рестарт устройства
- Удаленные операции ping/tracert/telnet
- Доступ к журналам Windows
- Доступ к локальным файлам
- Управление локальными сервисами (create/delete/start/stop/restart/change account and password)
- Управление локальными учетками и группами
- Инвентаризация железа и софта
- Сбор информации по фактам входа на устройства
- Журналирование всех операций с пользовательским устройством

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, 1С, 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
- …

Октябрь 2023 - текущее состояние

- Кадровые данные из 252 источников, 113+ тысяч сотрудников и подрядчиков, 158 городов
- 4 домена AD – 97+ тыс учеток
- 241 приложение 1С – 114+ тыс учеток
- 3 инстанса SAP/R3 – 20 тыс+ учеток
- 11 прочих приложений, восьми типов
- Более 700 пользователей, 50+ интеграций с другими системами

Время исполнения заявок сократилось с дней до секунд

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
- Управление взаимодействием приложений (App2App password management)

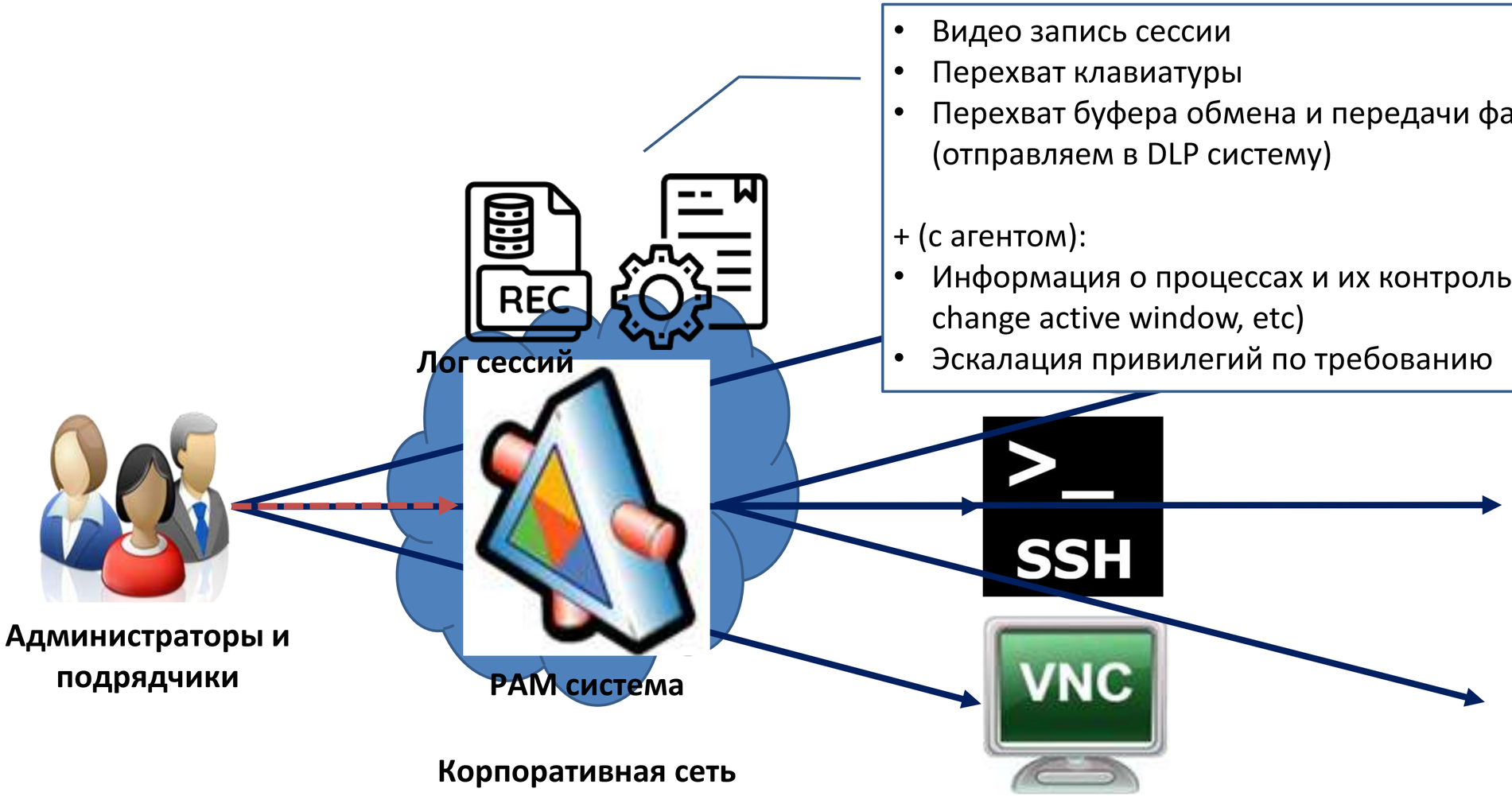
PAM система

- Большое число привилегированных пользователей и оборудования
- Необходимость контроля выполняемых 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

Логическая схема PAM системы

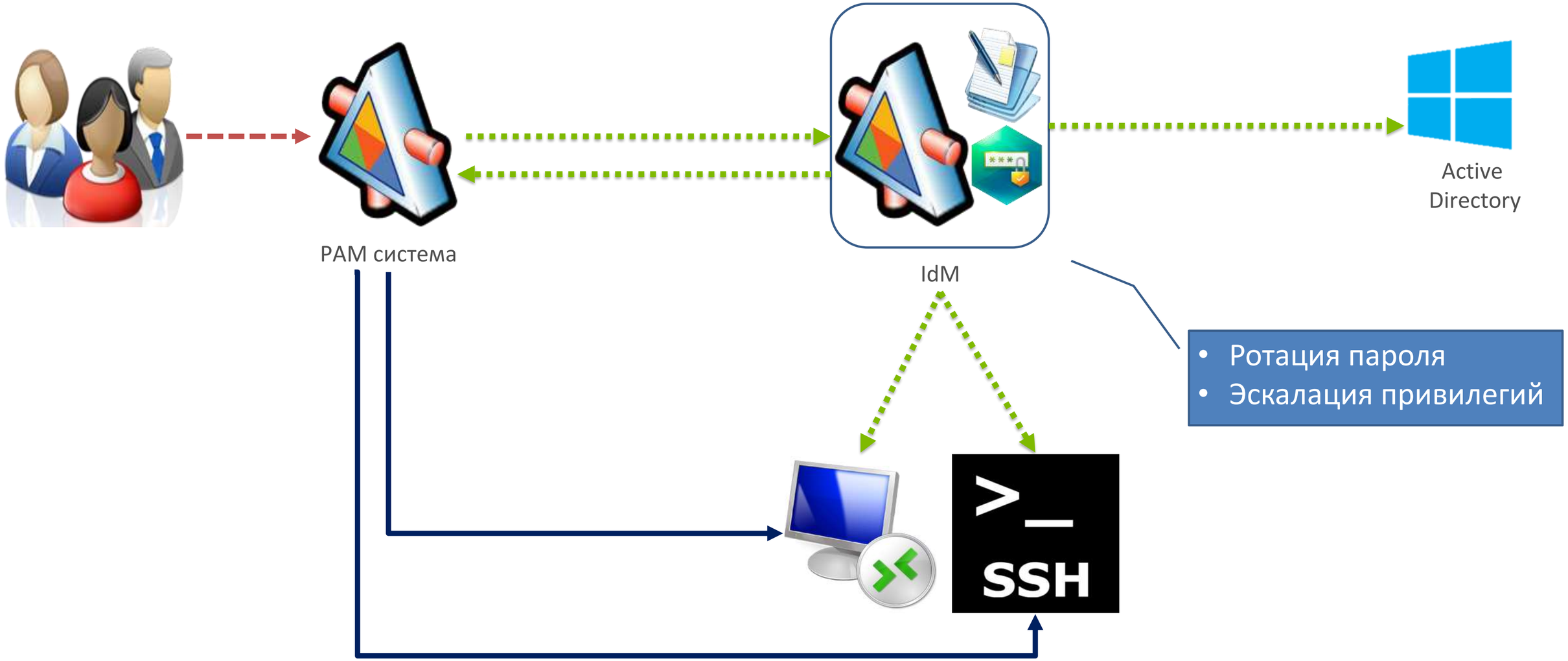


- Видео запись сессии
- Перехват клавиатуры
- Перехват буфера обмена и передачи файлов (отправляем в DLP систему)

+ (с агентом):

- Информация о процессах и их контроль(start process, change active window, etc)
- Эскалация привилегий по требованию

App2App password management



- Ротация пароля
- Эскалация привилегий

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
- Отказоустойчивость и балансировка нагрузки
- Первая клиентская сессия 05.03.2022, в промышленной эксплуатации с 01.12.2022

Текущее состояние

- 500+ пользователей на 17 площадках
- Более 15тыс сессий, длительностью 30.000+ часов, общим объемом 210Гб

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
- Управление взаимодействием приложений (App2App password management)

PAM система

- Большое число привилегированных пользователей и оборудования
- Необходимость контроля выполняемых 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

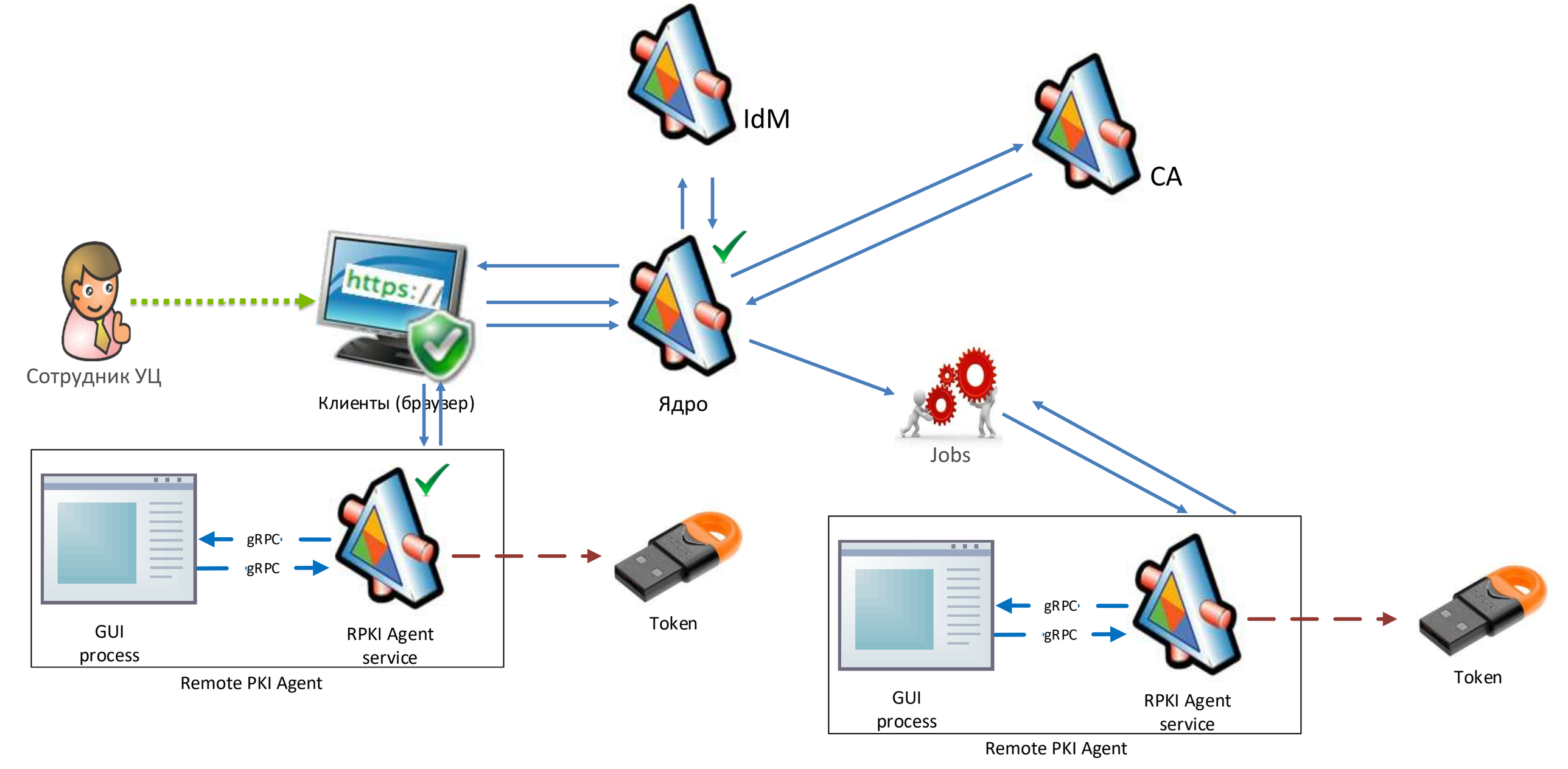
Сентябрь 2022- запуск проекта PKI

- Полностью своя разработка
- Является надстройкой для IdM системы
- Распределенная система, рассчитанная на сотни площадок и десятки тысяч пользователей, тысячи сервисов
- Первая клиентская операция 28.10.2022

Текущее состояние

- 25тыс+ пользователей по всему миру
- Среднее время выпуска и доставки сертификата – менее минуты

Архитектура PKI – выпуск сертификата



Что было самым сложным

- Консолидация кадровых данных. 252(!) кадровых источника
- Обучение пользователей
- Тестирование приложений
- Оптимизация производительности
- Удаленная запись сертификатов на токен

Команда проекта




Готов ответить
на ваши вопросы

E-mail: Vladimir.kovalev2@gmail.com