

Сервис аутентификации, авторизации и единого управления учетными записями



ПЕТРОВ
Андрей Валерьевич

Руководитель департамента
цифровой трансформации

г. Чебоксары.



Функция
родительского
контроля

Контроль и управление пользователями

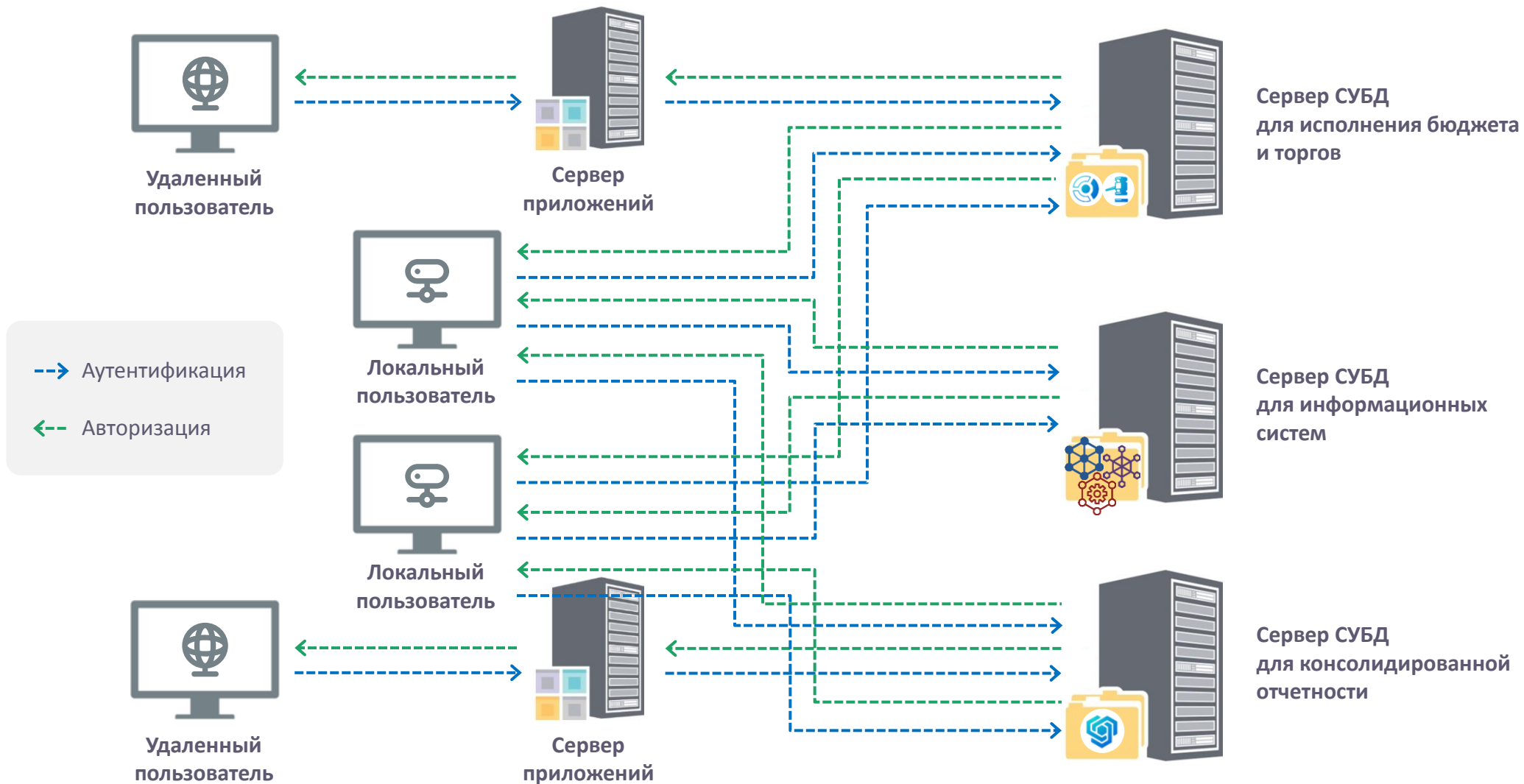


Программный комплекс «Сервис авторизации»

- Позволяет вести централизованное управление учетными записями пользователей для аутентификации и авторизации
- Организовывает доступ через единую точку входа с контролем действий



Как это работает? Без сервиса авторизации



Как это работает? С сервисом авторизации

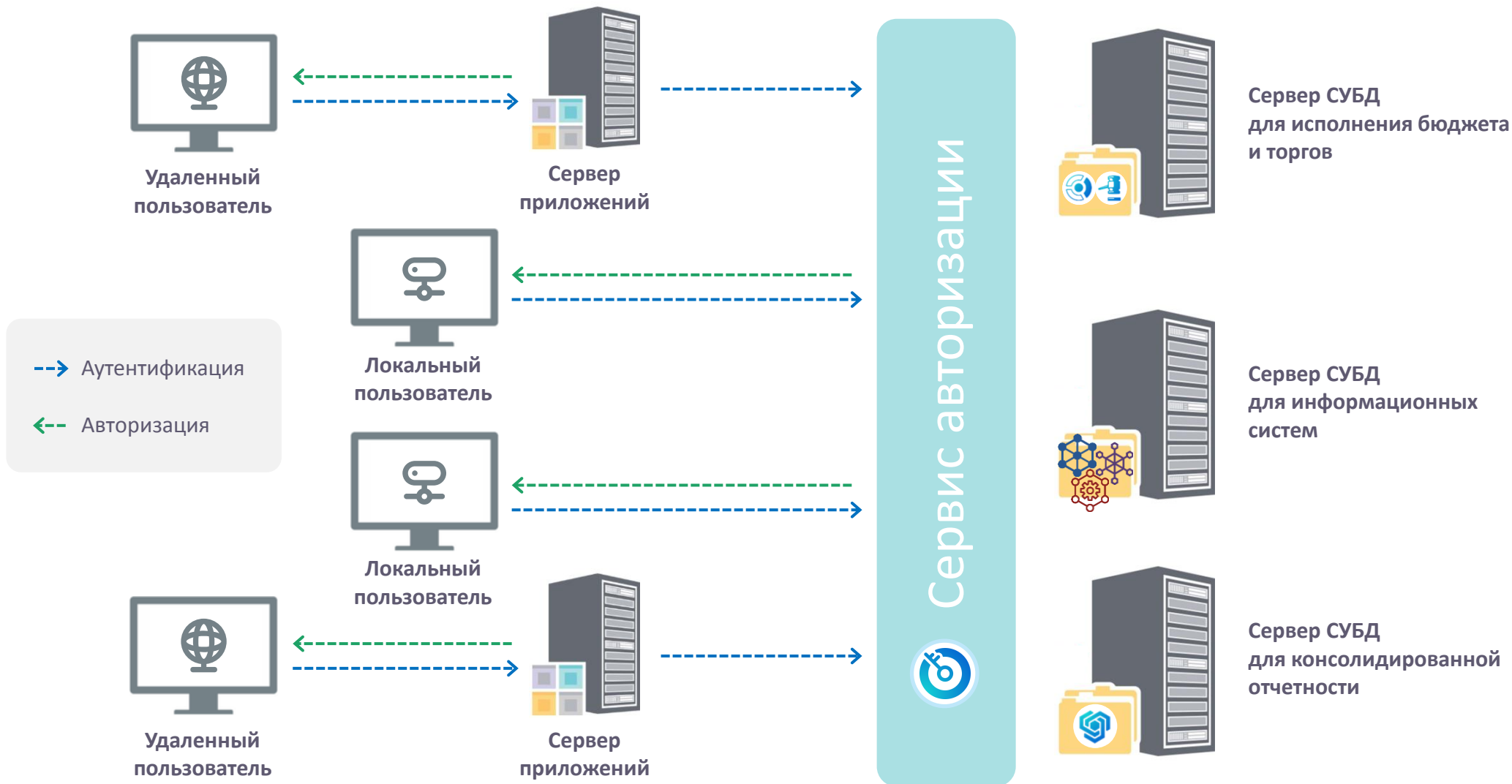


Схема работы программного продукта

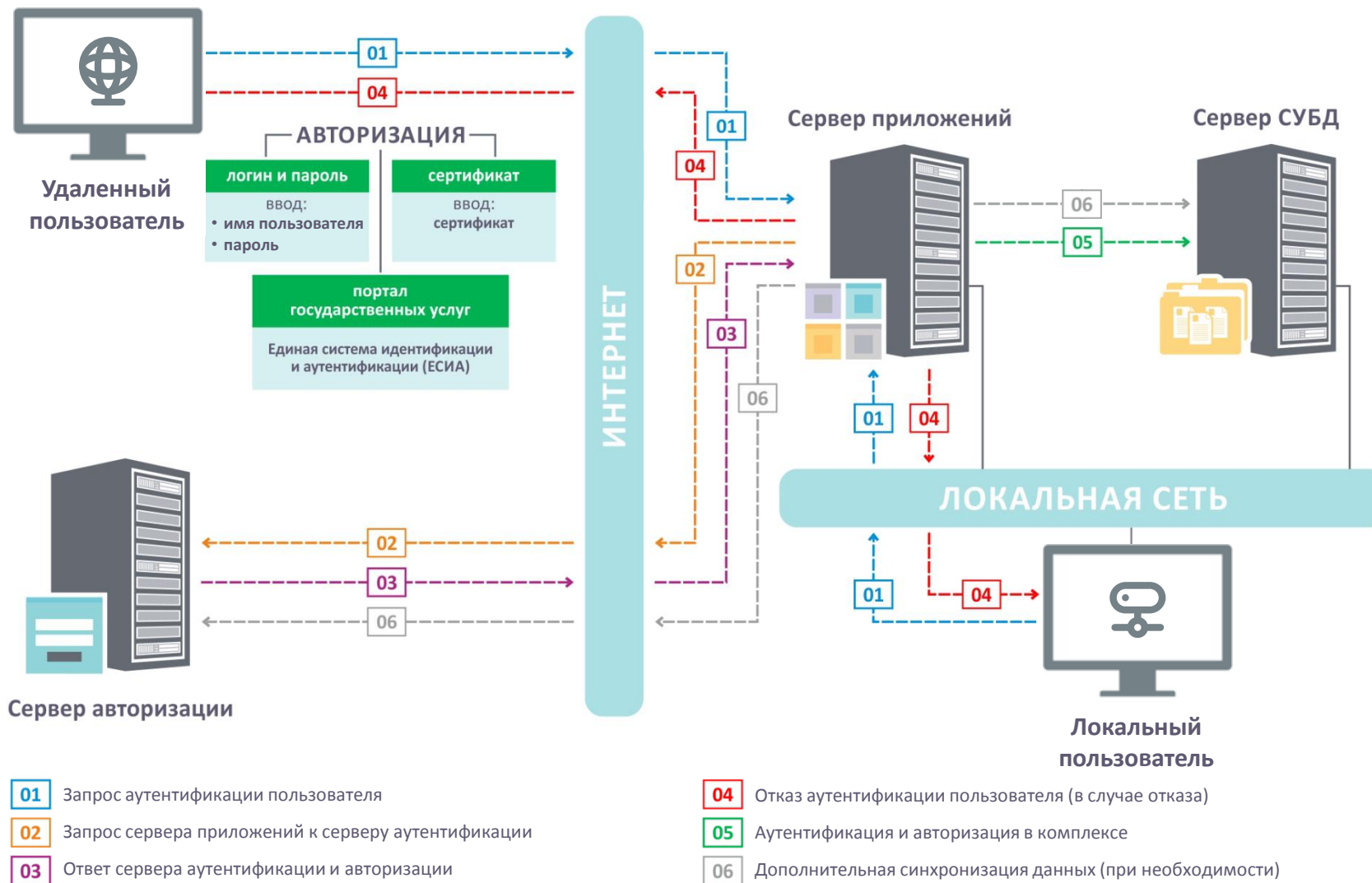
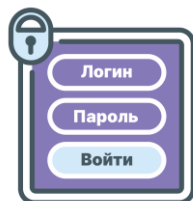


Схема работы программного продукта



Схема работы программного продукта



Аутентификация
(SSO система)

Аутентификация –
подтверждение личности
идентифицированного
пользователя и его подлинности

Схема работы программного продукта



Аутентификация
(SSO система)

Технология единого входа (Single Sign-On, SSO) обеспечивает:

- ✓ использование одного идентификатора для доступа ко всем системам;
- ✓ централизованно хранит все пароли;
- ✓ автоматически обрабатывает запросы аутентификации по требованиям всех систем, подставляя учетные данные пользователя (логин и пароль) и избавляя его таким образом от необходимости запоминать и вручную вводить эти данные несколько раз.

Схема работы программного продукта



Авторизация и контроль
управления доступом
(IDM-система)

Авторизация –
процедура предоставления
пользователю полномочий
и ресурсов

Схема работы программного продукта



Авторизация и контроль
управления доступом
(IDM-система)

Система Identity Management System (IDM)

позволяет:

- ✓ обеспечить управление учетными записями, работая на стыке задач информационной безопасности, управления ИТ-ресурсами и автоматизации бизнес-процессов;
- ✓ предоставить и разграничить доступ к ресурсам;
- ✓ отслеживать неактуальные учетные записи и учетные записи с избыточными полномочиями;
- ✓ оперативно реагировать на прием, увольнение, должностные перемещения персонала, появление новых процессов, модулей.

Схема работы программного продукта



Авторизация и контроль
управления доступом
(IDM-система)

Централизованное управление и разграничение доступа производится на основе ролей (RBAC) и атрибутов (ABAC)

RBAC – предоставление доступа к информационной системе с определением общей роли пользователя.

ABAC – детальный контроль доступа или настройки доступа к информации, доступной для работы при определенных условиях.

Возможности – для администраторов



- Импорт и экспорт конфигураций пользователей из баз данных программных продуктов – отсутствует необходимость повторной настройки разграничения полномочий и прав доступа для каждой информационной системы
- Установка смешанной модели аутентификации - только один вариант или сразу несколько по удобству пользователя
- Возможность сбора и использования сертификатов пользователей для авторизации

Возможности – для администраторов



- ⚙️ Глобальное централизованное управление учётными записями пользователей с последующей синхронизацией изменений в соответствующих базах данных программных продуктов.
- ⚙️ Возможность выбора условий по настройке политики паролей, автоматизированная смена паролей пользователей согласно заданному графику.

Возможности – для администраторов



- ⚙️ Создание и работа с заявками пользователей на администрирование.
- ⚙️ Бизнес-процессы обмена и согласования заявок на администрирование.
- ⚙️ 3-уровневая модель администрирования данных в сервисе авторизации.

Модель администрирования пользователей

Выделено три конфигурации пользователей для работы и упрощения процесса администрирования комплексов:



Администратор сервиса авторизации – осуществляет полное администрирование сервиса.

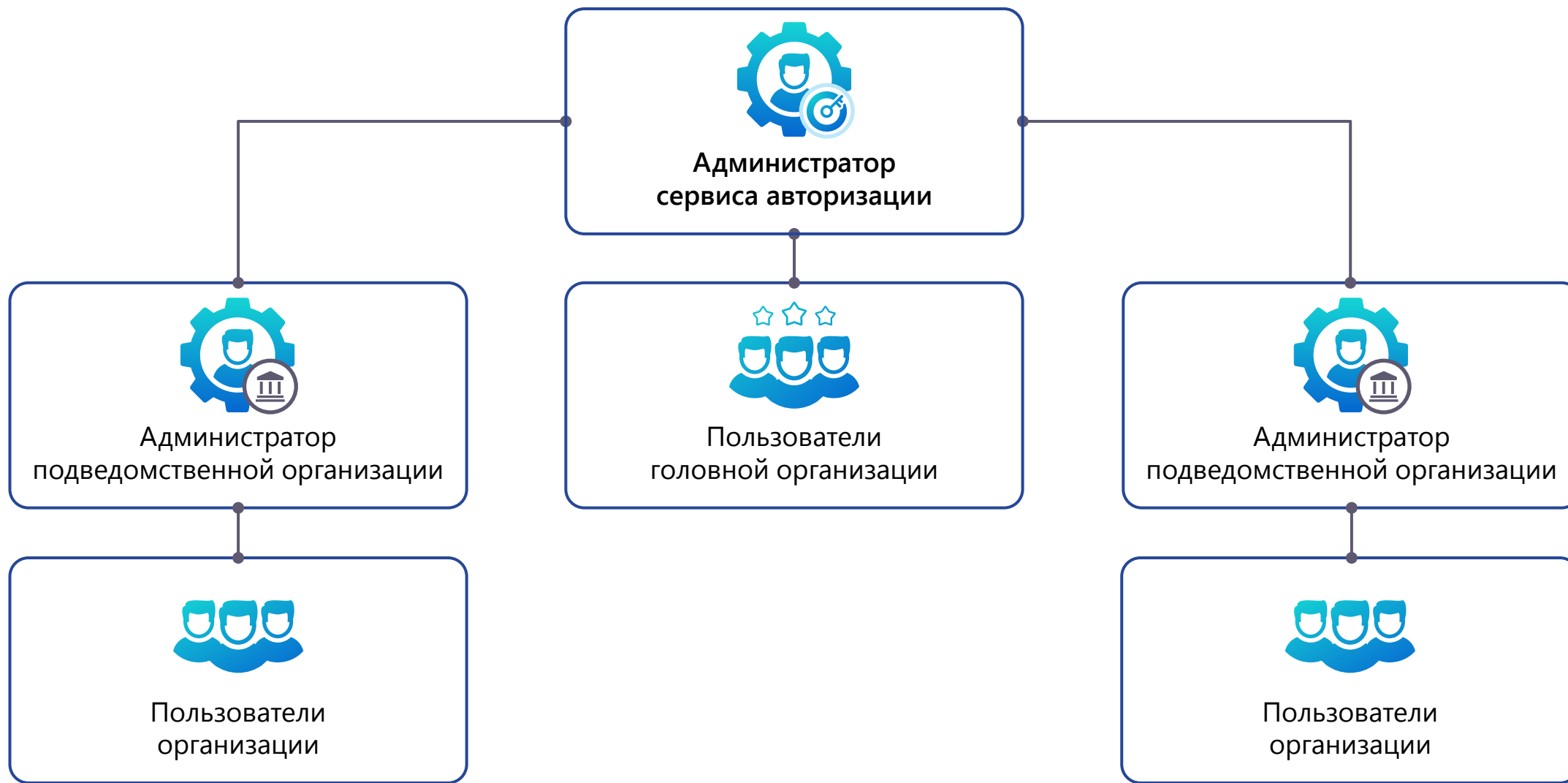


Администратор организации – осуществляет администрирование сервиса авторизации в пределах назначенных ему организаций.



Пользователь – осуществляет администрирование своей учетной записи путем подачи заявок администраторам.

Модель администрирования пользователей



Модель администрирования пользователей

**Администратор
сервиса авторизации**

Администратор организации

Пользователь

Создает:

1. Учетные записи пользователей
2. Организации пользователей
3. Доступные комплексы
4. Конфигураций пользователей

Учетные записи
для пользователей своей организации

Заявки
на администрирование

Утверждает:

Все заявки на администрирование

Заявки на администрирование
организации

Исправляет:

1. Учетные записи
2. Перечень организаций
3. Перечень комплексов
4. Конфигураций пользователей

Учетные записи пользователей своей
организации

*Имеет право на удаление учетных записей
пользователей своей организации

Реквизиты учетной
записи и доступность
комплексов путем
создания заявок

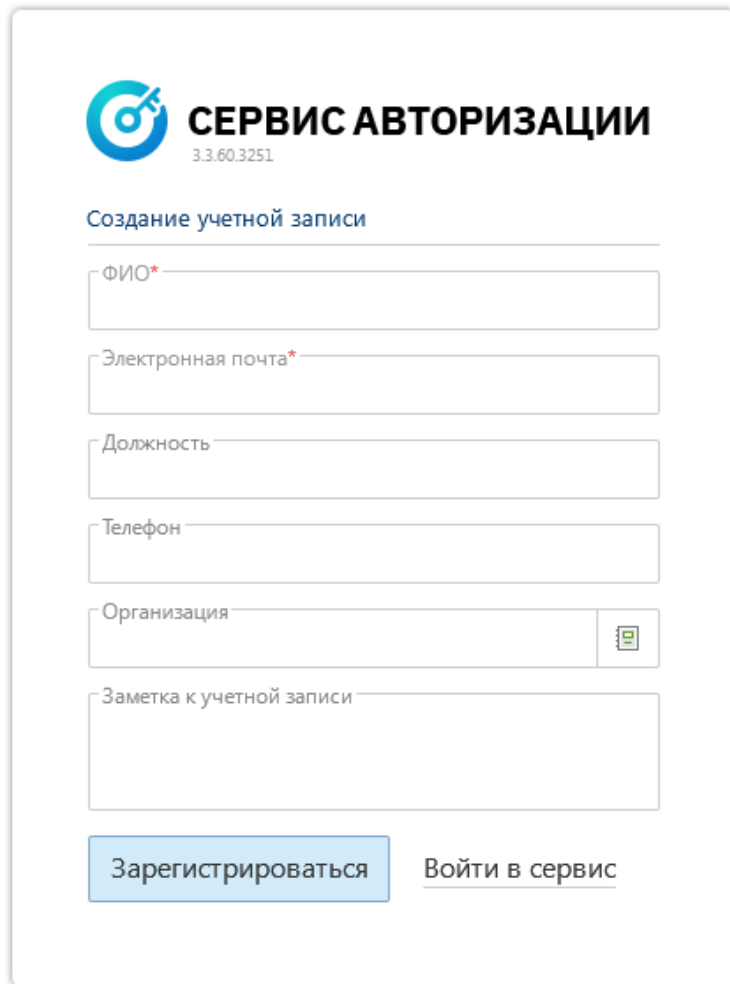
*Устанавливает параметры работы
сервиса


Возможности – для пользователей



- ⚙️ Вход в различные базы данных программных продуктов, указанных пользователю с использованием единой аутентификации через единую точку входа.
- ⚙️ **Работа через личный кабинет пользователя.**

Возможности личного кабинета



 **СЕРВИС АВТОРИЗАЦИИ**
3.3.60.3251


Создание учетной записи

ФИО*

Электронная почта*


Должность

Телефон

Организация 

Заметка к учетной записи

[Зарегистрироваться](#) [Войти в сервис](#)

-  Запрос создания учетной записи пользователем самостоятельно через заявку на администрирование.

Возможности личного кабинета

Сервис авторизации 3.3.60.3251

Петров Андрей


Программные комплексы


Комплексы


Реквизиты


Поддержка

Выйти




 Бюджет-СМАРТ
✓ [bks_auth_serv_test_vv](#)
✓ [bks_auth_serv_test_vv](#)
✓ [bks_auth_serv_test_vv](#)
bks_auth_serv_test_vv
bks_auth_serv_test_vv

 Бюджет-NEXT
✓ [bks_auth_serv_test_vv](#)
bks_auth_serv_test_vv

 Проект-СМАРТ ПРО
✓ [bks_auth_serv_test_vv](#)
bks_auth_serv_test_vv

 Свод-СМАРТ
✓ [bks_auth_serv_test_vv](#)
bks_auth_serv_test_vv

 Администратор-Д
✓ [bks_auth_serv_test_vv](#)


-  Быстрый доступ к комплексам.
-  Отсутствие необходимости вводить пароль повторно при входе в любую информационную систему.
-  Управление списком доступных комплексов.


Возможности личного кабинета

Сервис авторизации 3.3.60.3251

Петров Андрей


 Комплексы



 Реквизиты

 Поддержка

 Выйти

Реквизиты


Логин*	<input type="text" value="cab01"/>
ФИО*	<input type="text" value="Петров Андрей Валерьевич"/>
Электронная почта*	<input type="text" value="petrov_a@keysystems.ru"/>
Должность	<input type="text" value="Руководитель департамента"/>
Телефон	<input type="text" value="8 () _ _ - _ _"/>
Организация	<input type="text"/> 
Сертификат	<input type="button" value="Добавить"/>
Заметка к учетной записи	<input type="text"/>

-  Подача заявки на изменение своих реквизитов.
-  Оперативное внесение изменений в свою учетную запись.


Личный кабинет

Сервис авторизации 3.3.60.3251

Петров Андрей

 Комплексы


 Реквизиты

 **Поддержка**

 Выйти




Поддержка

 Документация
[Руководство пользователя ПК «Сервис авторизации»](#)

 Поддержка пользователей
Подразделение



Электронная почта

Телефон
8 (8352) 323-323, доб. 123

 О сервисе
ПК «Сервис авторизации»  
Версия сервиса: 3.3.60.3251

Сервер: ksdb1\sql2008 (xpks01.dll:110.146)
База данных: razr_164_test8 — admin
Версия базы данных: [16.4.0.2040.0.2040](#)

[Подробнее](#)

-  Постоянное наличие всей пользовательской документации в одном легко доступном месте.
-  Контакты ответственных специалистов по технической поддержке.

Эффекты от внедрения



- ✔ Защищенный изолированный сервис аутентификации.
- ✔ Централизованное управление и разграничение доступа с использованием ролей (RBAC) и атрибутов (ABAC) в информационных системах
- ✔ Единая точка входа и работа через личный кабинет.
- ✔ Снижение нагрузки на системных администраторов.
- ✔ Снижение административных издержек на предоставление/изменение прав доступа.

Эффекты от внедрения



- ✓ Минимизация рисков информационной безопасности.
- ✓ Повышение эффективности расследования инцидентов в области информационной безопасности.
- ✓ Уменьшение затрат на поддержку IT-инфраструктур.
- ✓ Контроль активных учетных записей.
- ✓ Своевременное отключение и блокировка неактивных учетных записей во всех системах.

Программный комплекс «Сервис авторизации»

Делаем с учетом ваших интересов!
Делаем под ваши потребности!



Страница ПК «Сервис авторизации»

По вопросам приобретения,
внедрения, иным вопросам:

Петров Андрей Валерьевич

(8352) 323-323, доб. 269

Petrov-a@keysystems.ru

ICQ: 436823913