Skillbox

Security

Аутентификация и авторизация

Чернухин Максим

Software Architect АО Альфа-Банк

На этом уроке мы узнаем

- Что такое аутентификация
- Где используется авторизация
- Какие бывают способы построения ролевых моделей

Знакомство с пользователем

- **Идентификация** — отождествление анонимного клиента с конкретным именем
- **Аутентификация** — процедура проверки подлинности, например, проверка подлинности пользователя с помощью логина и пароля
- **Авторизация** — предоставление определённому лицу или группе лиц прав на выполнение конкретных действий

Способы аутентификации

- Ввод логина и пароля
- Отправка СМС или почты
- Использование цифровой подписи
- Использование сертификатов
- Биометрическая аутентификация
- Аутентификация с помощью токенов
- Использование одноразовых паролей
- Многофакторная аутентификация и др.

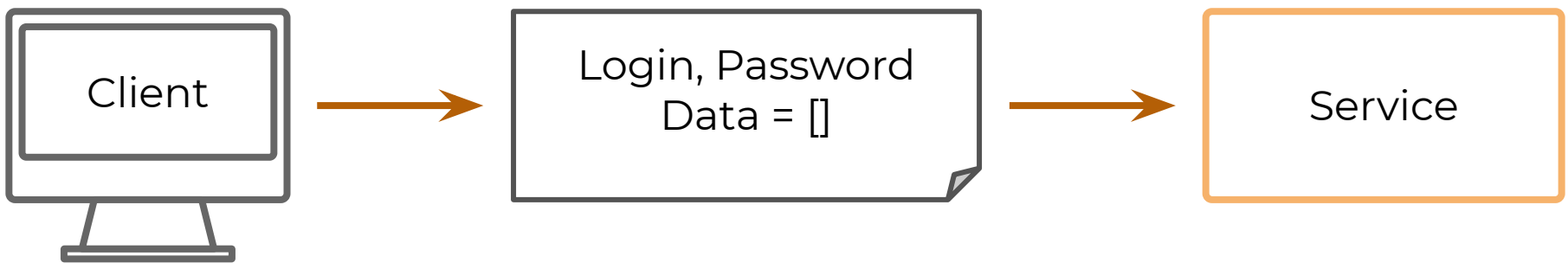
Skillbox

Классификация аутентификации

- Базовая аутентификация
- Дайджест-аутентификация
- С помощью сертификатов: SSL, Kerberos и т. д.
- Децентрализованная аутентификация Single Sign-on (SSO)

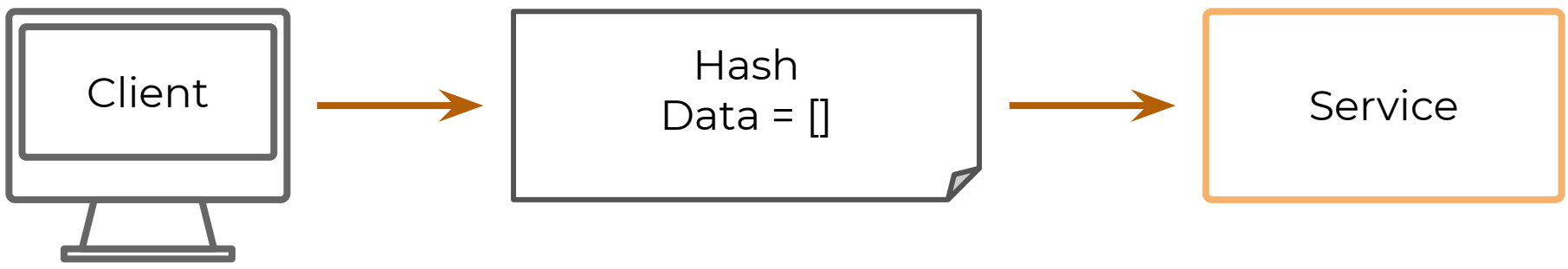
Базовая аутентификация

- В этом случае при каждом запросе передаются логин и пароль
- Простая реализация
- Лёгкий перехват данных
- Необходимость шифрования канала



Дайджест-аутентификация

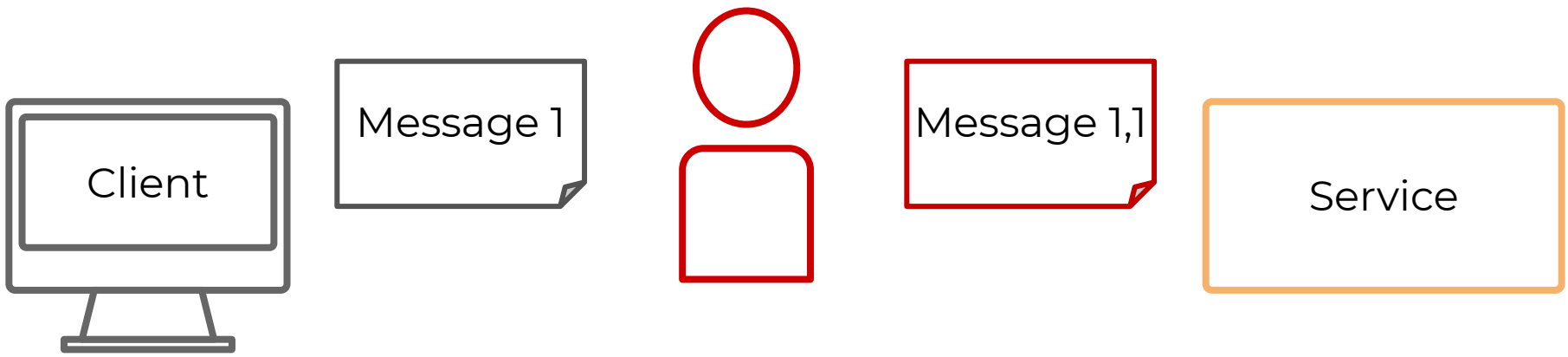
- В этом случае при каждом запросе передаются логин и пароль в хешированном состоянии
- Функция хеширования должна быть сложной



Skillbox

Аутентификация с помощью сертификатов

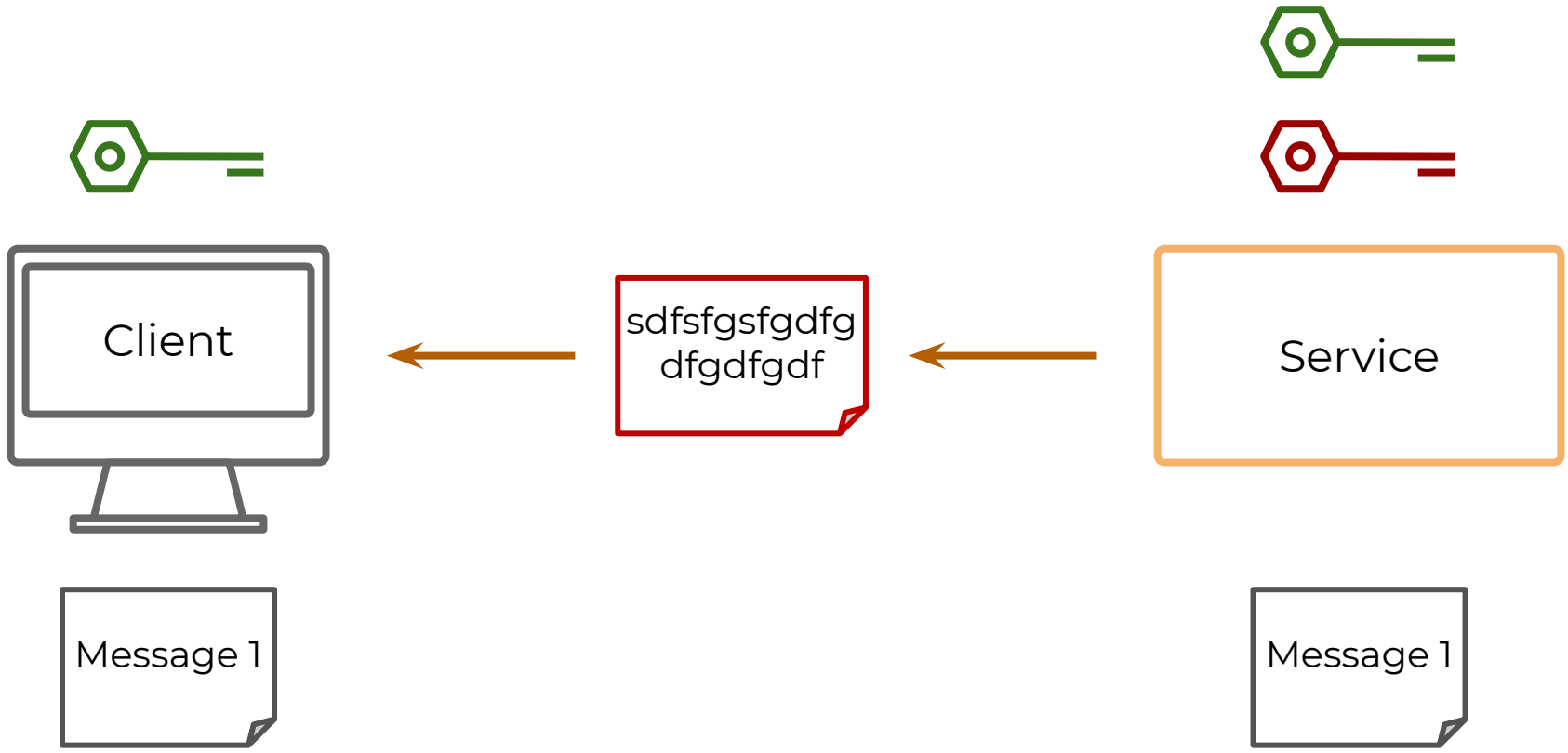
- Аутентификация сервера
- Аутентификация клиента



Man in the middle

Skillbox

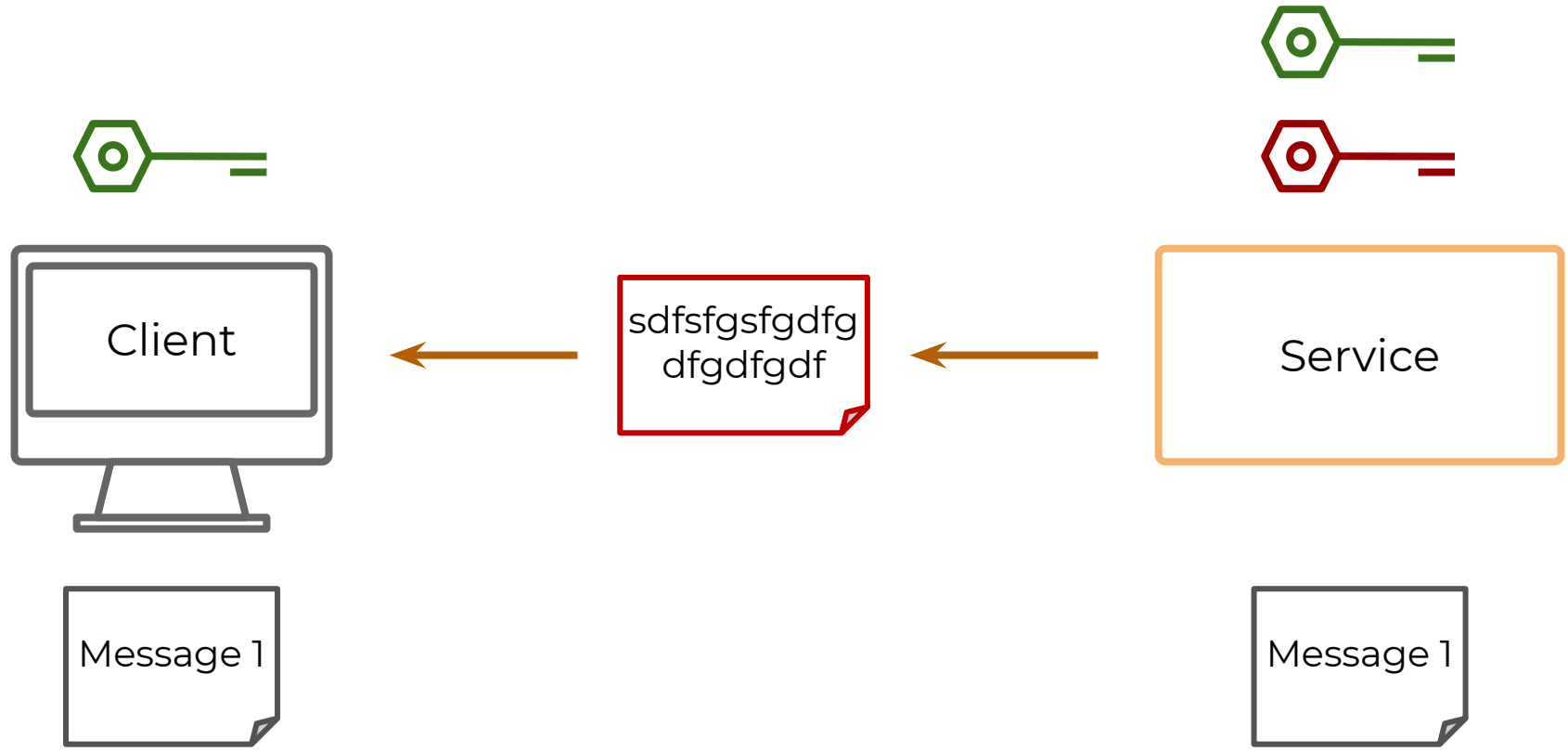
Аутентификация с помощью сертификатов



Skillbox

Аутентификация с помощью сертификатов

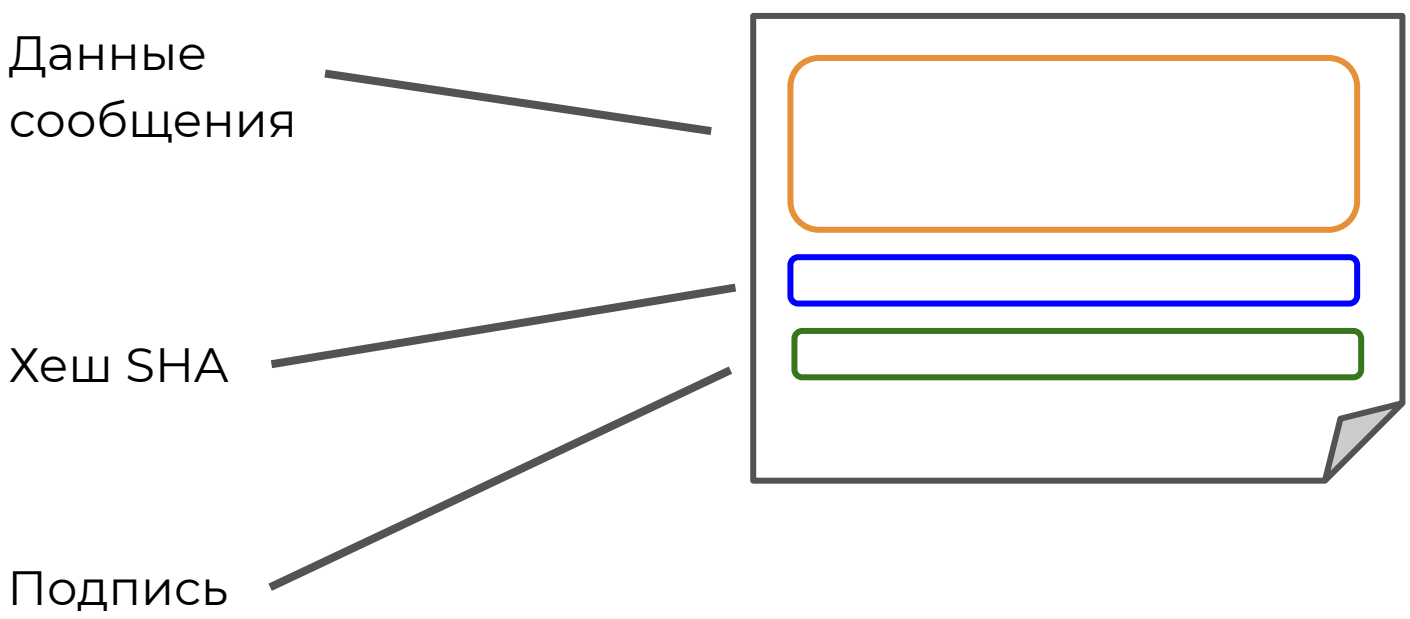
- Какой смысл шифровать сообщения?
- Любой сервер может выпустить сертификат



Skillbox

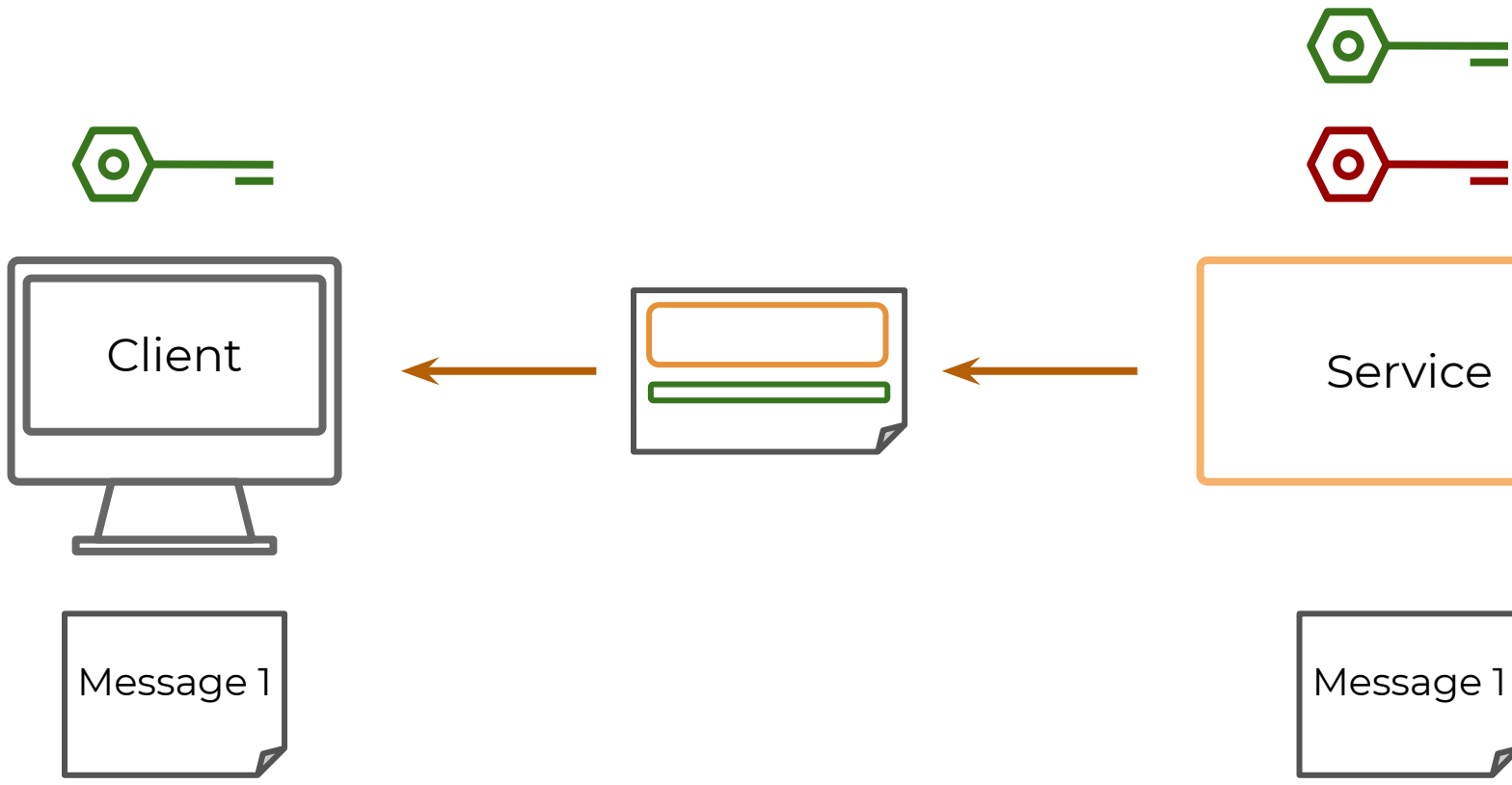
Электронная подпись

- Шифрование хеша сообщения
- Зашифрованный хеш сообщения: электронно-цифровая подпись (ЭЦП)

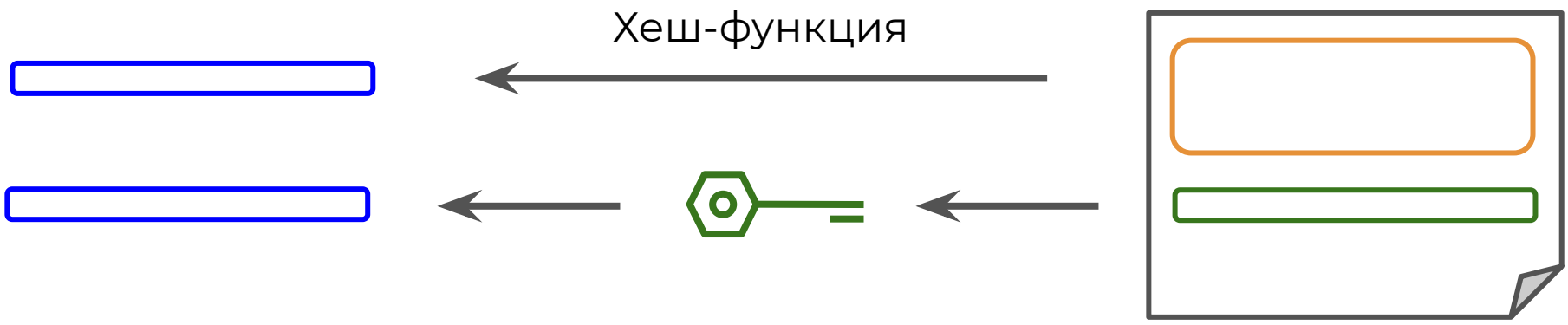


Skillbox

Электронная подпись

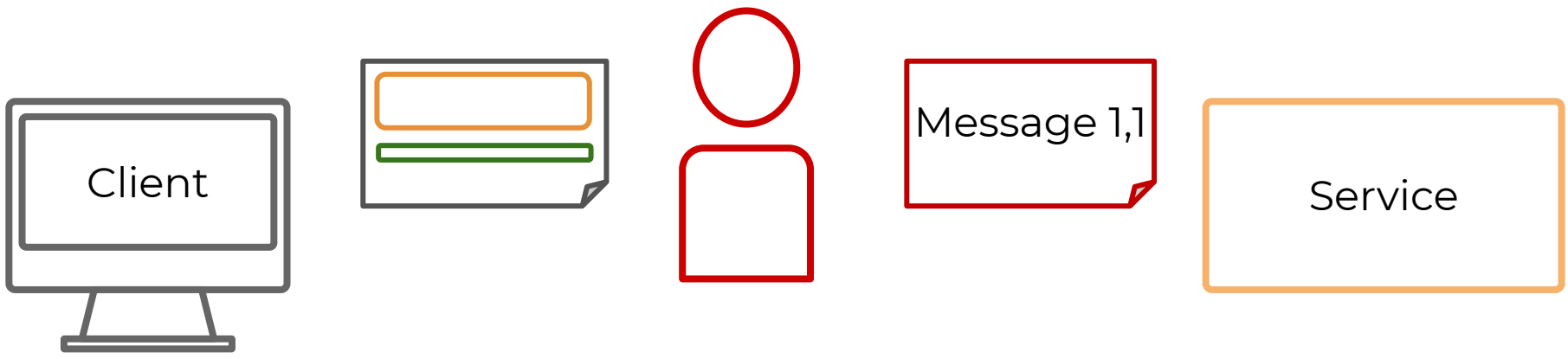


Электронная подпись



Аутентификация с помощью сертификатов

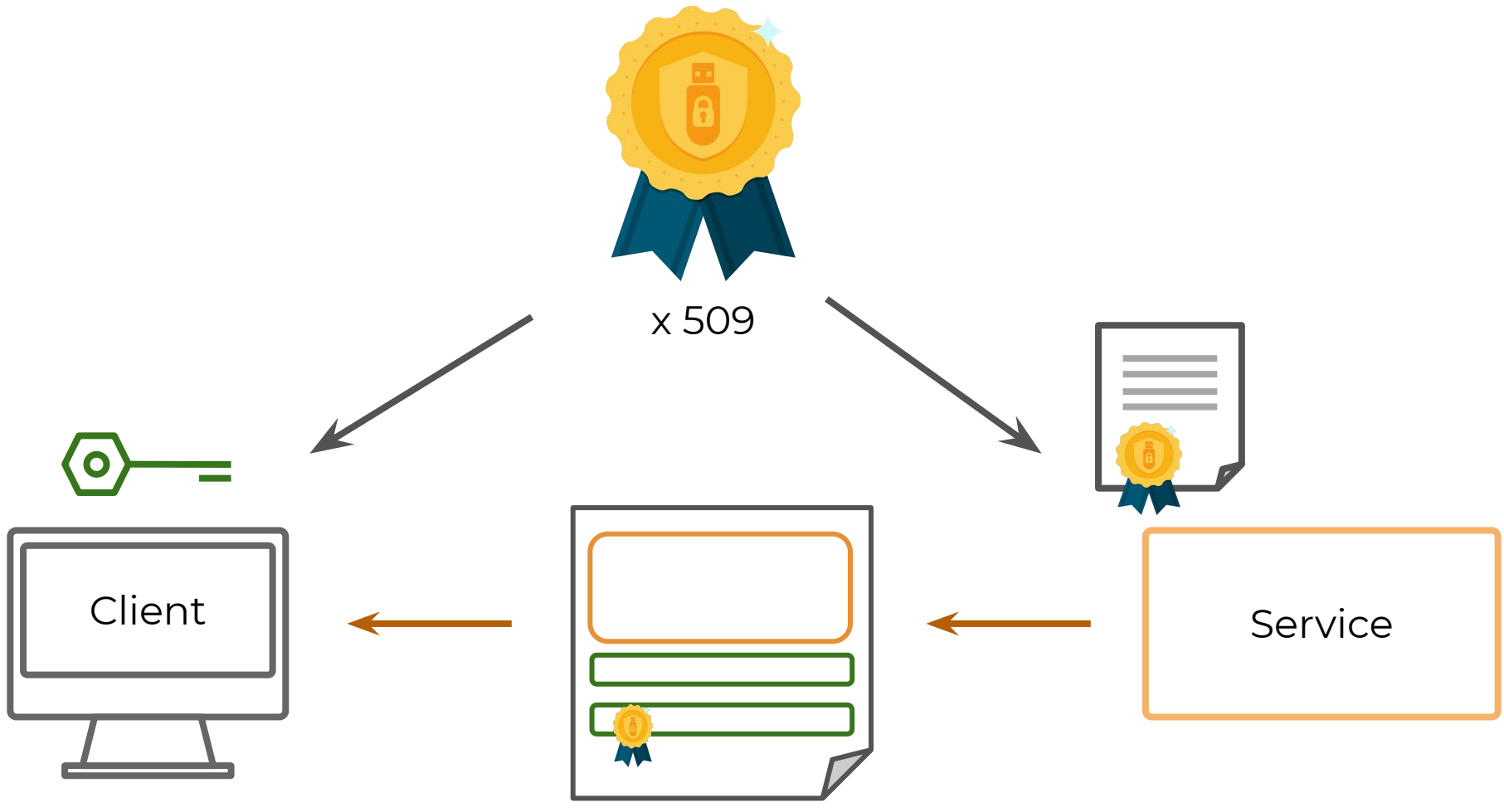
- Как понять, что этот тот самый сервер?
- Кому принадлежит открытый ключ?



Man in the middle

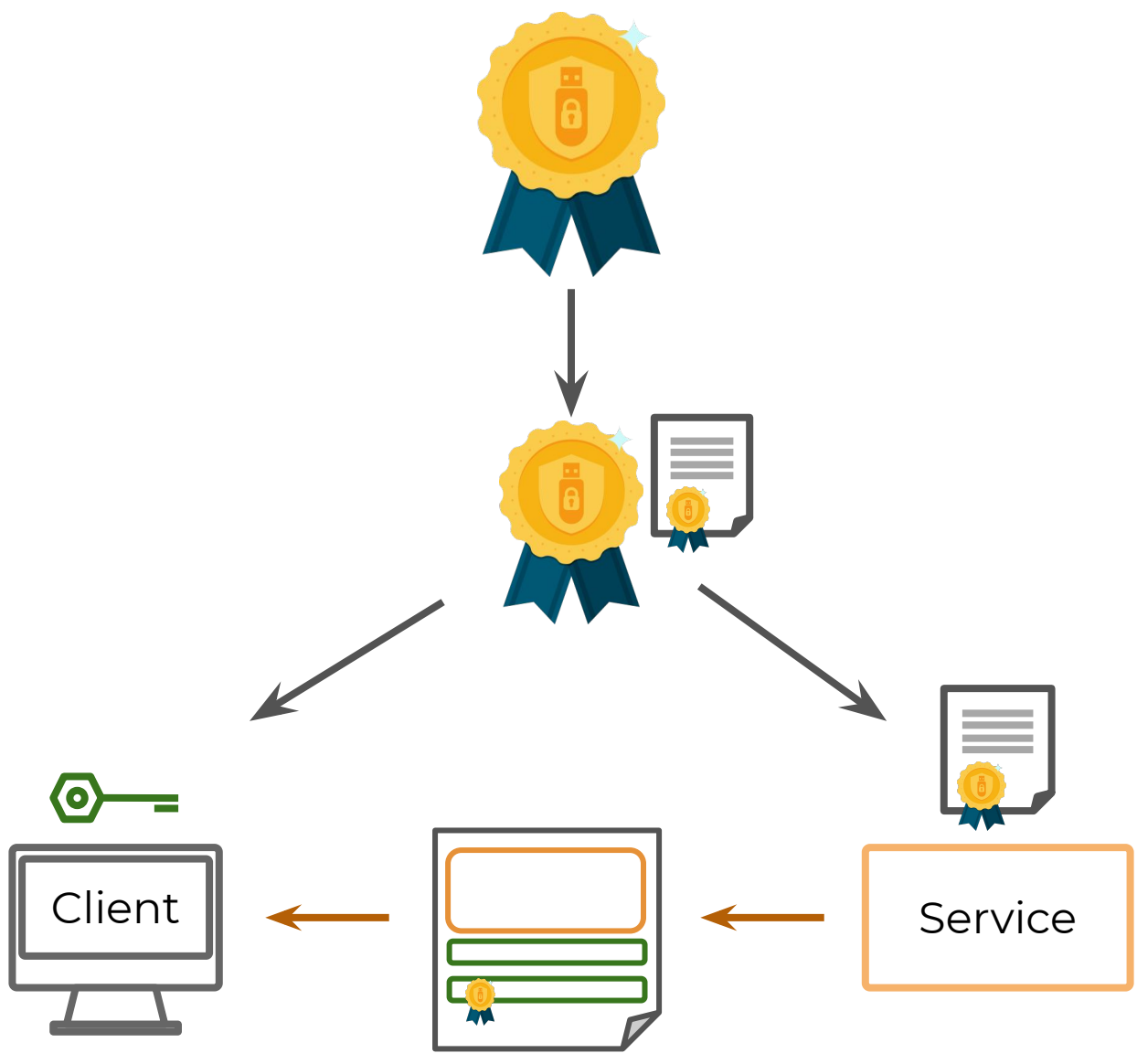
Skillbox

Инфраструктура открытых ключей



Skillbox

Инфраструктура открытых ключей



Авторизация

- **Субъект доступа** — это человек, служба, группа пользователей, которые пытаются получить доступ
- **Объект доступа** — это тот объект, к которому субъект пытается получить доступ
- **Авторизатор** — это компонент, который разрешает либо запрещает доступ субъекта к объекту

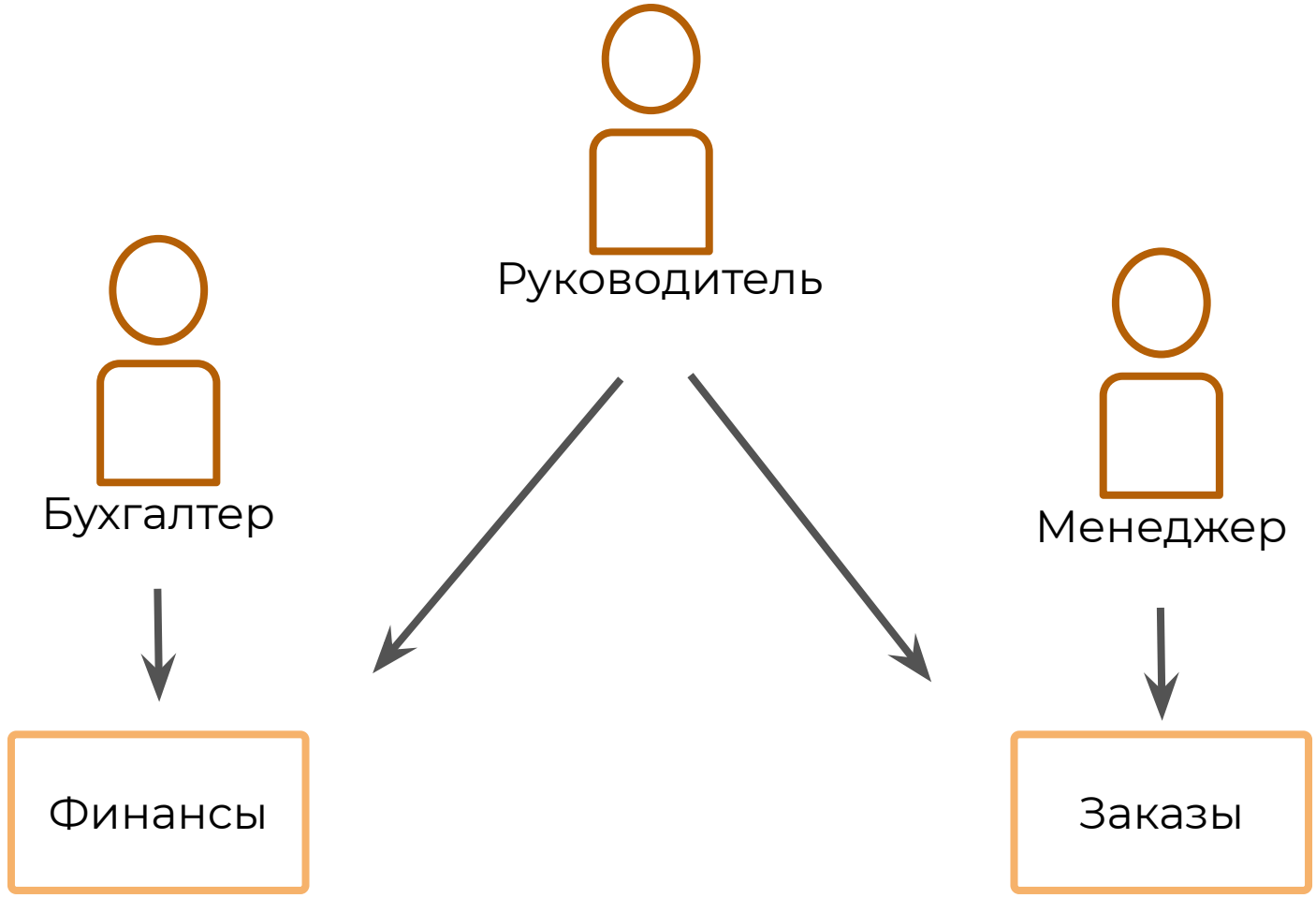
Skillbox

Авторизация RBAC vs ABAC

- **Role-based access control** — авторизация, основанная на бизнес-ролях
- **Attribute-based access control** — авторизация, основанная на атрибутах, которыми надо будет управлять

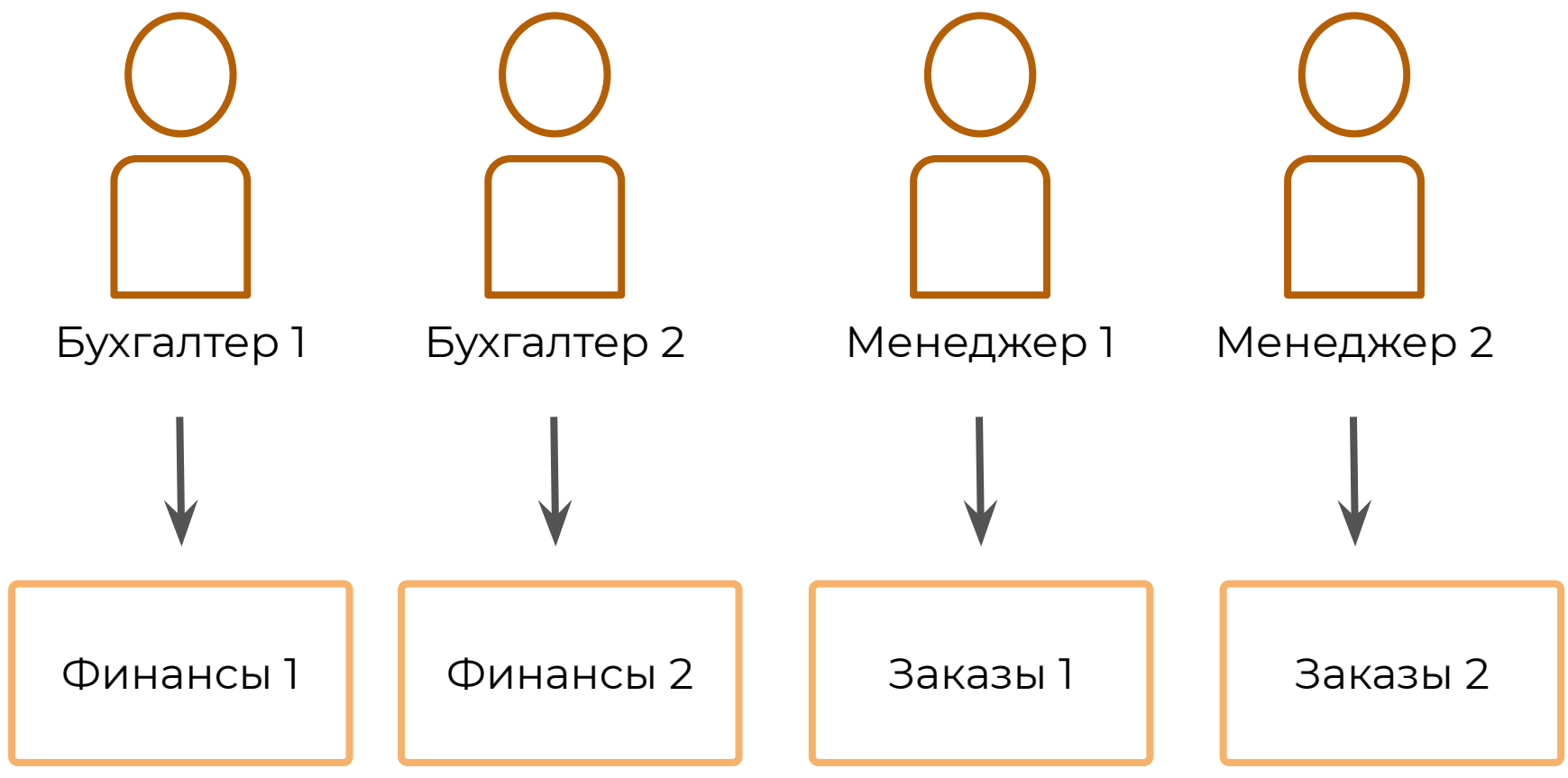
Skillbox

Role-based access control RBAC



Skillbox

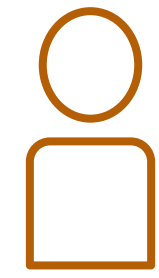
Role-based access control RBAC



Skillbox

Attribute-based access control ABAC

- Имя филиала
- Гео привязка
- Головной офис
- Наличие своих бухгалтеров
- Цена



- Имя филиала
- Головной офис

Skillbox

Attribute-based access control ABAC

Менеджер может управлять заказами в своём филиале, стоимость которых меньше 100 000.

Роль менеджера:

- Субъект.должность = «Менеджер»
- Объект.Филиал = Субъект.Филиал
- Объект.цена <= 100 000 руб.
- Объект.тип = «Заказ»

Skillbox

Авторизация RBAC vs ABAC

- Role-based access control:
  - быстрый старт
  - сложности при масштабировании
- Attribute-based access control:
  - долгий старт
  - лёгкое масштабирование

Итоги

- Мы познакомились с типами и способами аутентификации
- Узнали, что такое инфраструктура открытых ключей и сертификат x509
- Разобрались, что такое авторизация
- Изучили различные подходы, применяемые при авторизации

Что дальше?

- Что такое OAuth 2.0?
- Чем он отличается от OpenID Connect?
- Зачем нужен JWT?
- Как использовать SSO?

Skillbox

Спасибо за внимание!