РусКрипто

Банк России

infotecs

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

БЕЗОПАСНОСТЬ OPEN API: КОГДА «ОТКРЫТЫЙ» НЕ ЗНАЧИТ «УЯЗВИМЫЙ»

РусКрипто

Банк России

infotecs

К.т.н. Константин Стародубов
Департамент информационной безопасности Банка России

К.ф-м.н. Михаил Грунтович
АО «ИнфоТеКС»

XXVII НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ

Банк России

РусКрипто

Что такое API?

Для чего?

Какие подходы?

Что же в России?

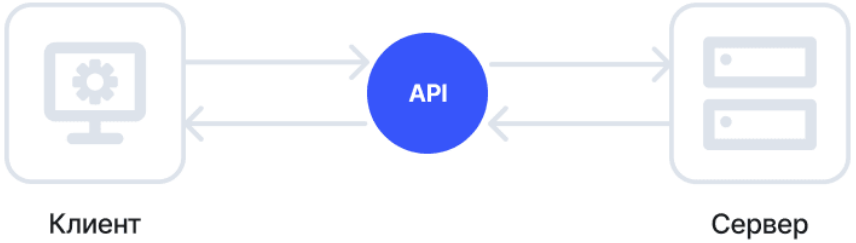
Стандартизация подходов?

Что такое API?

API — набор способов, механизмов и правил, по которым программы общаются между собой и обмениваются данными.

API встречается практически везде:

- В языках программирования, помогает функциям корректно взаимодействовать.
- В ОС, помогает программам получать данные из памяти.
- В Web - сервисы общаются друг с другом через программный интерфейс.

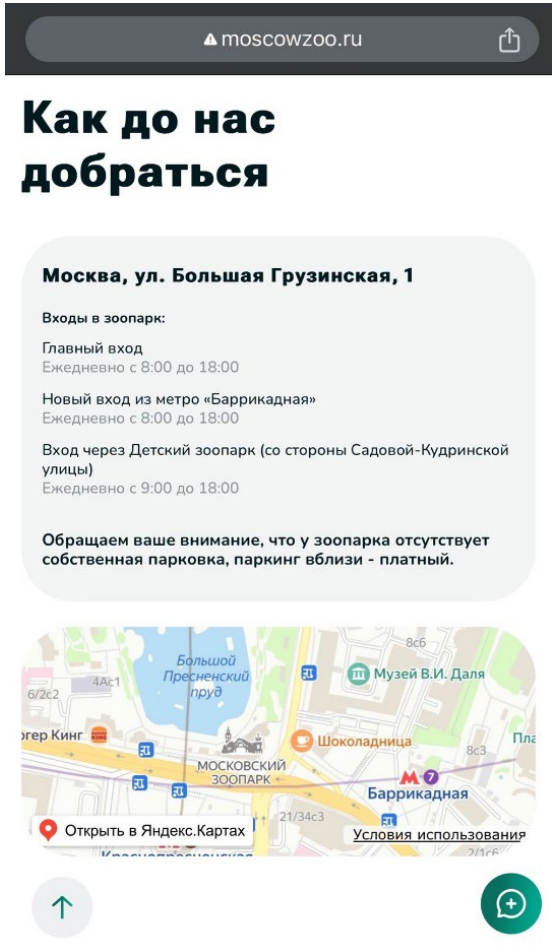


Методы

- **GET** – запрос получения данных
- **POST** – отправка данных
- **DELETE** – удаление данных
- **PUT** – обновление данных

Как использовать API?

Интеграция API — процесс, в рамках которого несколько приложений соединяются между собой с помощью API и обмениваются данными.



GET Resource

С разрешения Владельца данных, открывается возможность использовать его данные на своей странице, интегрируя их с помощью API.

Например у Яндекс можно запросить такие сервисы как:

- новостная лента;
- карта;
- погода;
- курсы валют и т.д.

МОСКОВСКИЙ ЗООПАРК

Яндекс

Пример использования API при проведении платежа

Что насчет Финуслуг?

РусКрипто

ФИН УСЛУГИ от МОСКОВСКОЙ БИРЖИ | Финпродукты | Журнал | О маркетплейсе | Поиск | Вся Россия | Войти

Главная > О финансовой платформе Финуслуги

Финуслуги - маркетплейс дл

Открывайте и пополняйте вклады онлайн, оформляйте к
облигации и электронные полисы ОСАГО на Финуслугах,
любое удобное время.

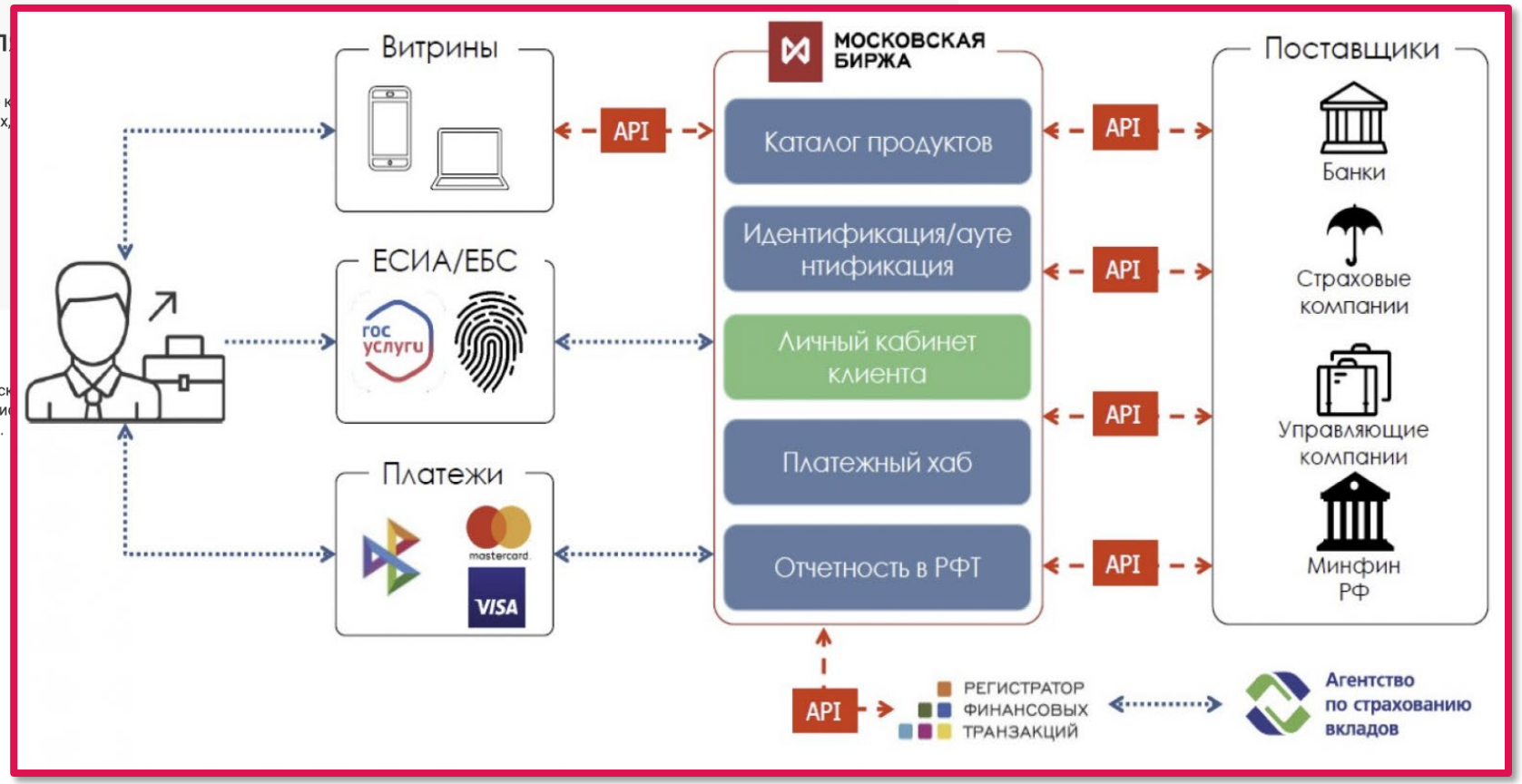
Что такое Финуслуги

Финуслуги - это маркетплейс для денег, созданный Моск
онлайн финансовые продукты, вне зависимости от реги
Финуслуги в реестр операторов финансовых платформ.

Онлайн-вклады от российских банков

Без визита в банк. Выбор, открытие, пополнение и закрытие вклада — в одном личном кабинете.

Подобрать вклад



А как используют API финансовые организации?

Кто использует?

- Кредитные организации
- Страховые организации
- Микрофинансовые организации
- Операторы финансовых платформ
- Маркетплейсы
- Агрегаторы

Какие сервисы?

Предоставление всех банковских услуг. Проведение оплаты через платежный терминал.

Предоставление любых типов данных и статистики.

Предоставление микрофинансовых услуг.

Предоставление всех страховых услуг.

Оптимизация взаимодействия, своих продуктов и услуг.

Финансовые сделки на Маркетплейсах и бирже.

История проекта Открытые API

РусКрипто

Безопасность финансовых (банковских) операций:

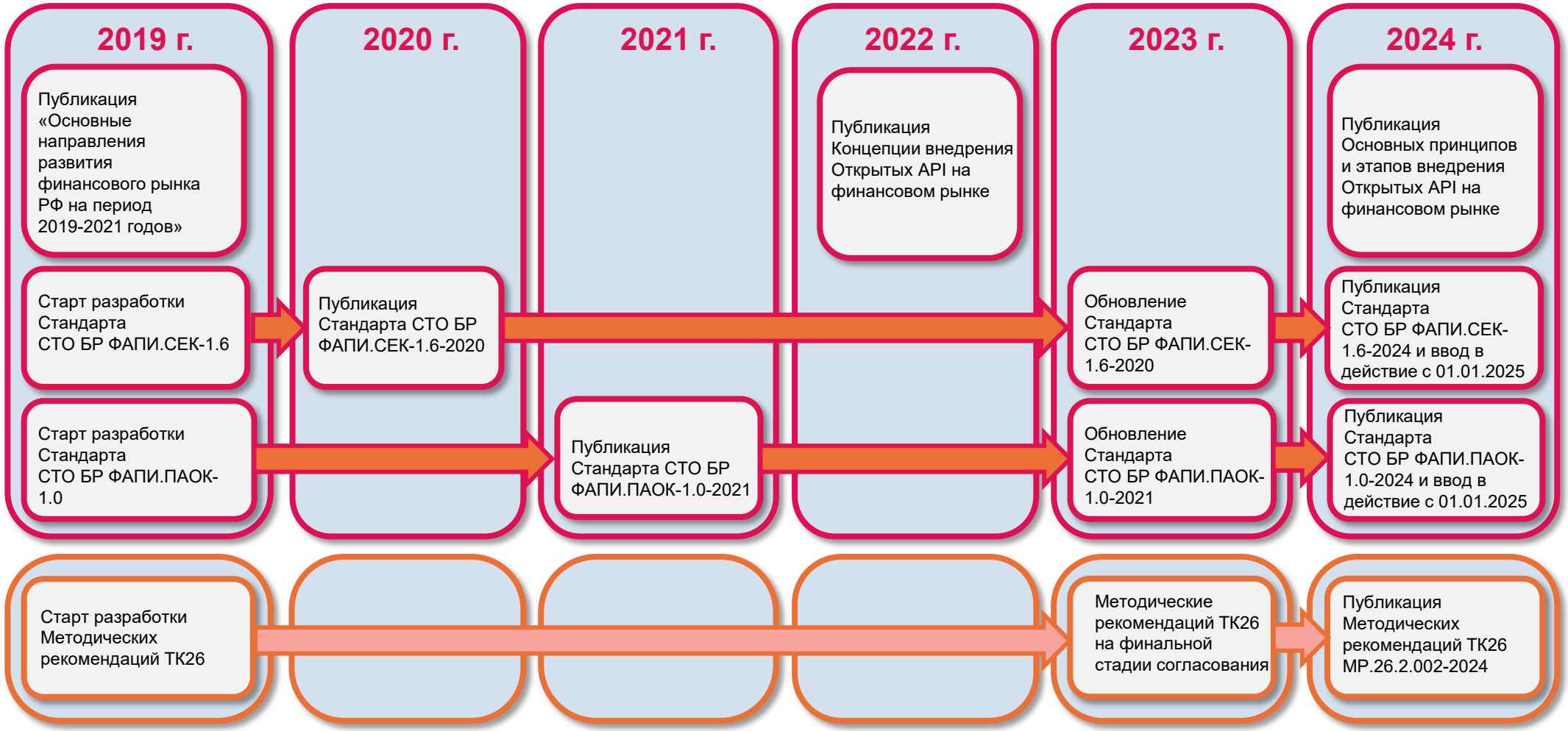
- СТО БР ФАПИ.СЕК-1.6-2020 - Обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect
- СТО БР ФАПИ.ПАОК-1.0-2021- Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу

Стандарты ФАПИ

Открытые банковские интерфейсы:

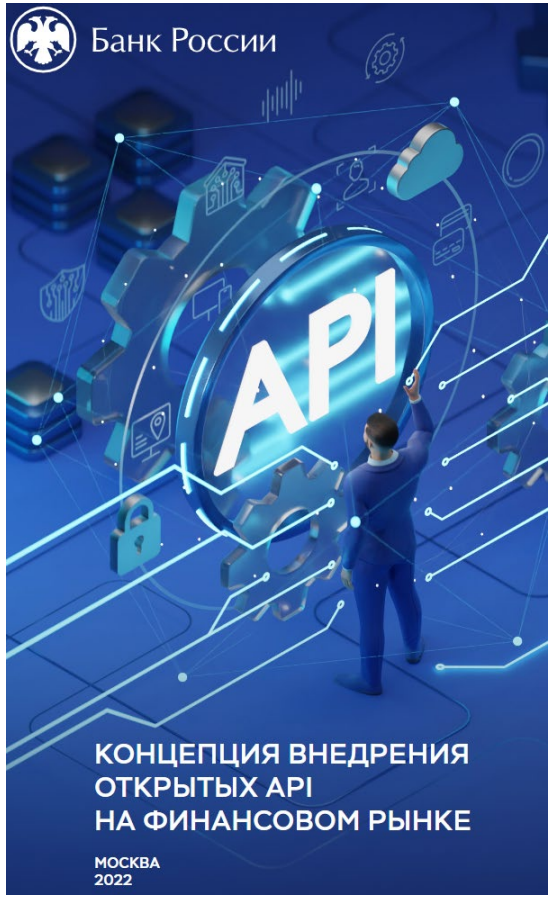
- Общие положения
- Получение информации о счете клиента третьей стороной
- Получение публичной информации о кредитной организации и ее продуктах
- Инициирование перевода денежных средств клиента третьей стороной в валюте РФ

Дорожная карта по стандартизации безопасности Открытых API



Основные направления развития Открытых API в России

РусКрипто



Причины обновления и основные изменения Стандартов ФАПИ

РусКрипто

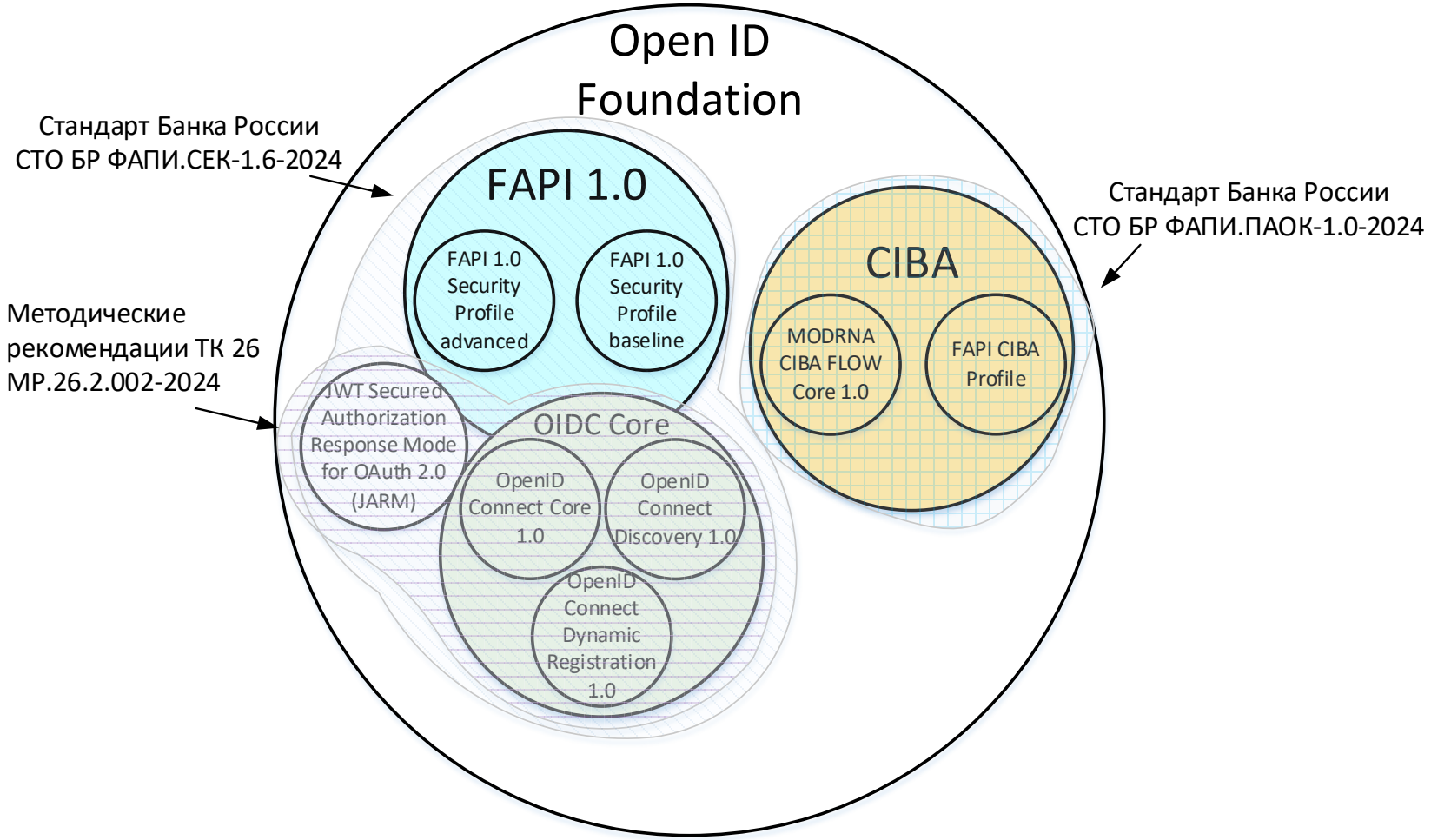
Причины изменений:

- Обновлены международные Стандарты OIDF (OpenID Connect)
- Развитие нормативно-правовой базы по ИБ
- Синхронизация Стандартов ФАПИ и МР ТК26

Внесенные изменения:

- Внесены изменения в профили безопасности API передачи финансовой информации
- Установлены требования к уровню доверия и типу информации
- Актуализированы ссылки на нормативные акты Банка России (821-П, 683-П, 757-П, 802-П, 808-П) и др.
- Учтены положения СТО БР БФБО 1.8-2024 (среда доверия)
- Стандарты ФАПИ синхронизированы с МР ТК26 и применяются совместно
- Обновлены сценарии протокола OpenID Connect
- Удален раздел с криптографией.
- Добавлены ссылки на МР ТК26. МР 26.2.002-2024 на https://tc26.ru

Международные стандарты OIDF, адаптированные в Стандартах ФАПИ



Участники Стандартов ФАПИ (среда доверия)

РусКрипто

Среда доверия

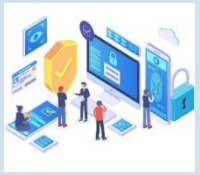
Пользователь

ЮЛ или ФЛ, являющееся владельцем ресурса на сервере ресурсов Поставщика данных

Для обеспечения безопасного взаимодействия все участники должны доверять друг другу.

Агент пользователя

Клиентское приложение, использующее определённый сетевой протокол для доступа к серверу (браузеры, поисковые роботы, почтовые клиенты)



Сервер авторизации (Поставщик данных)

Сервер, выдающий клиенту токены доступа после успешной аутентификации владельца ресурса и прохождения процедуры авторизации

Клиент (Потребитель данных)

Приложение, целью которого является получения доступа к защищенным ресурсам пользователя от его имени после выполнения процедуры авторизации

Сервер ресурсов (Поставщик данных)

Сервер, на котором размещены защищенные ресурсы (обменивает на токен доступа)

СТО БР БФБО-1.8-2024 (среда доверия)

РусКрипто

«Безопасность финансовых (банковских) операций. Обеспечение безопасности финансовых сервисов при проведении дистанционной идентификации и аутентификации. Состав мер защиты информации»

(приказ Банка России от 28 февраля 2024 г. № ОД-326)

Данный стандарт в рамках Открытых API:

Устанавливает требования к результатам:

- идентификация
- аутентификация

Устанавливает состав и содержание мер для обеспечения доверия к:


Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР БФБО-1.8-2024

БЕЗОПАСНОСТЬ ФИНАНСОВЫХ (БАНКОВСКИХ) ОПЕРАЦИЙ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ФИНАНСОВЫХ СЕРВИСОВ ПРИ ПРОВЕДЕНИИ ДИСТАНЦИОННОЙ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

СОСТАВ МЕР ЗАЩИТЫ ИНФОРМАЦИИ

МОСКВА
2024

Синхронизация Стандартов ФАПИ и МР ТК26

РусКрипто

ТК 26
«Криптографическая защита информации»

МР.26.2.002-2024
«Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколах OpenID Connect»

ТК 122
«Стандарты финансовых операций»

СТО БР ФАПИ.СЕК-1.6-2024
«Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования»

СТО БР ФАПИ.ПАОК-1.0-2024
«Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования»

Указ Президента РФ

От 01.05.2022 №250
«О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

СТО БР ФАПИ.СЕК-1.6-2024

РусКрипто

«Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования»

*(приказ Банка России от 07 октября 2024 г. № ОД-1615)**

Целью Стандарта является:

*Применение организациями финансового рынка прикладных программных интерфейсов (**API**), в том числе **Открытых API**, которые определяют **порядок использования модели API** на технологическом участке **аутентификации, идентификации и авторизации**.*
*Стандарт устанавливает состав и содержание требований **к информационной безопасности** при реализации взаимодействия с использованием API, в том числе Открытых API, обеспечивающих необходимый уровень защищенности информации при передаче персональных данных и банковской тайны.*
СТО БР ФАПИ.СЕК-1.6-2024 предоставляет требования и рекомендации для обеспечения безопасного доступа к финансовым данным в финансовых сервисах реального времени с использованием защищенной технологии OAuth, включая профилирующий ее протокол OpenID Connect.

*Взамен СТО БР ФАПИ.СЕК-1.6-2020, вступает в силу с 01.01.2025

СТО БР ФАПИ.ПАОК-1.0-2024

РусКрипто

«Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования»

*(приказ Банка России от 07 октября 2024 г. № ОД-1616)**

Целью Стандарта является:

*Применение организациями финансового рынка прикладных программных интерфейсов (**API**), в том числе **Открытых API**, которые определяют порядок использования модели прикладных программных интерфейсов API, обеспечивающих необходимые уровни защищенности информации при передаче персональных данных, банковской тайны и иной защищаемой информации во исполнение требований Банка России в целях повышения безопасности финансовых технологий для осуществления требуемого уровня доверия к идентификации, аутентификации и авторизации сторонних поставщиков финансовых услуг.*


Банк России

СТАНДАРТ БАНКА РОССИИ

СТО БР ФАПИ.ПАОК-1.0-2024

Безопасность финансовых (банковских) операций

Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу

Требования

Москва
2024

*Взамен СТО БР ФАПИ.ПАОК-1.0-2021, вступает в силу с 01.01.2025

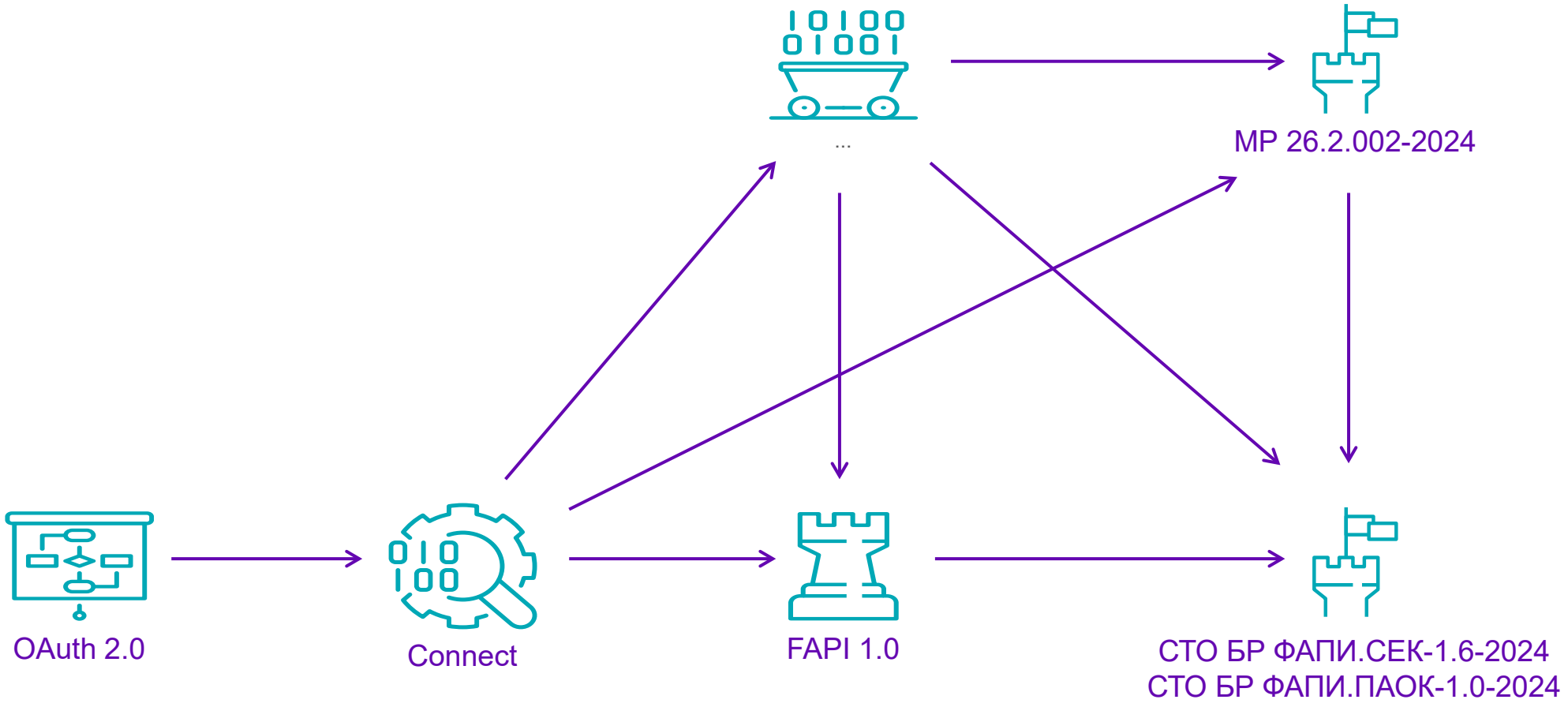
РусКрипто

Технологии безопасности Open API

Развитие технологий безопасности

Технологическая база Open API

РусКрипто

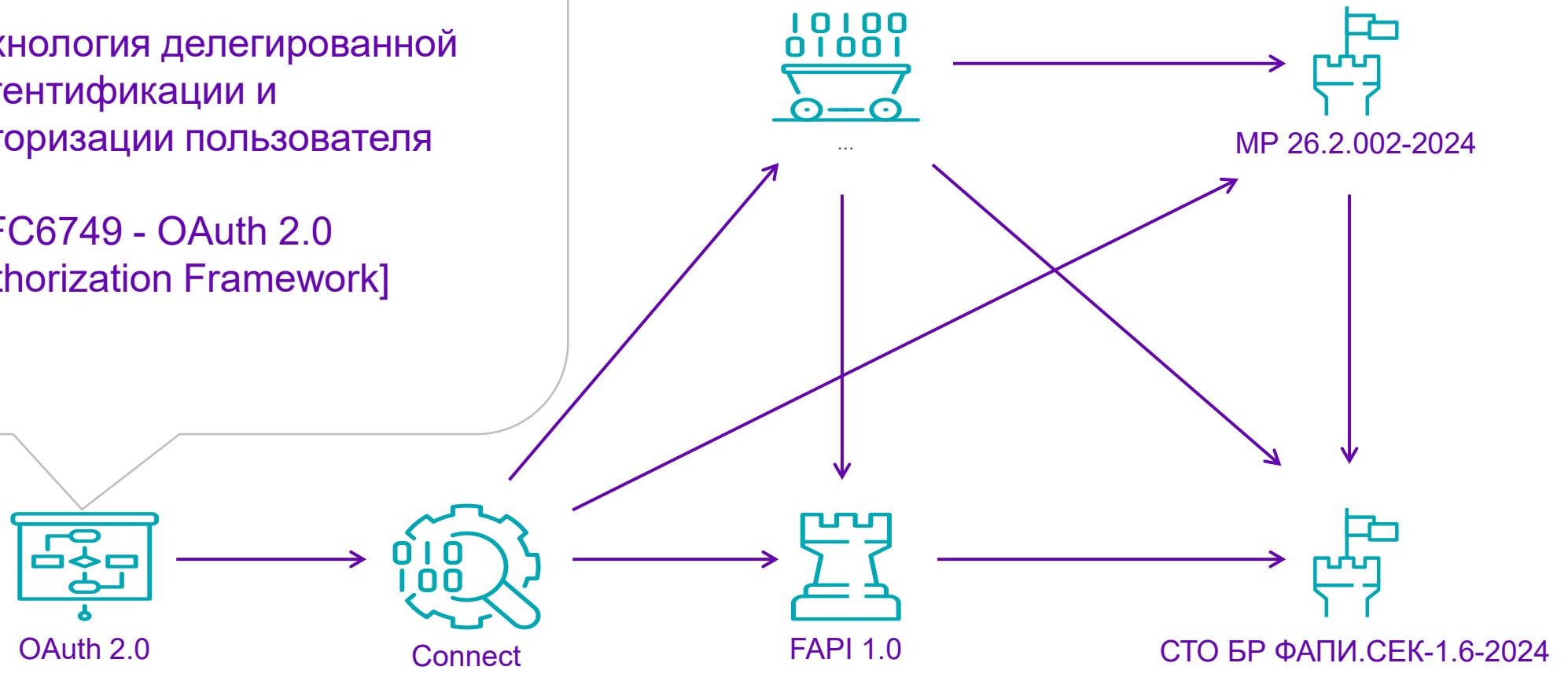


Технологическая база Open API

РусКрипто

Технология делегированной аутентификации и авторизации пользователя

[RFC6749 - OAuth 2.0 Authorization Framework]

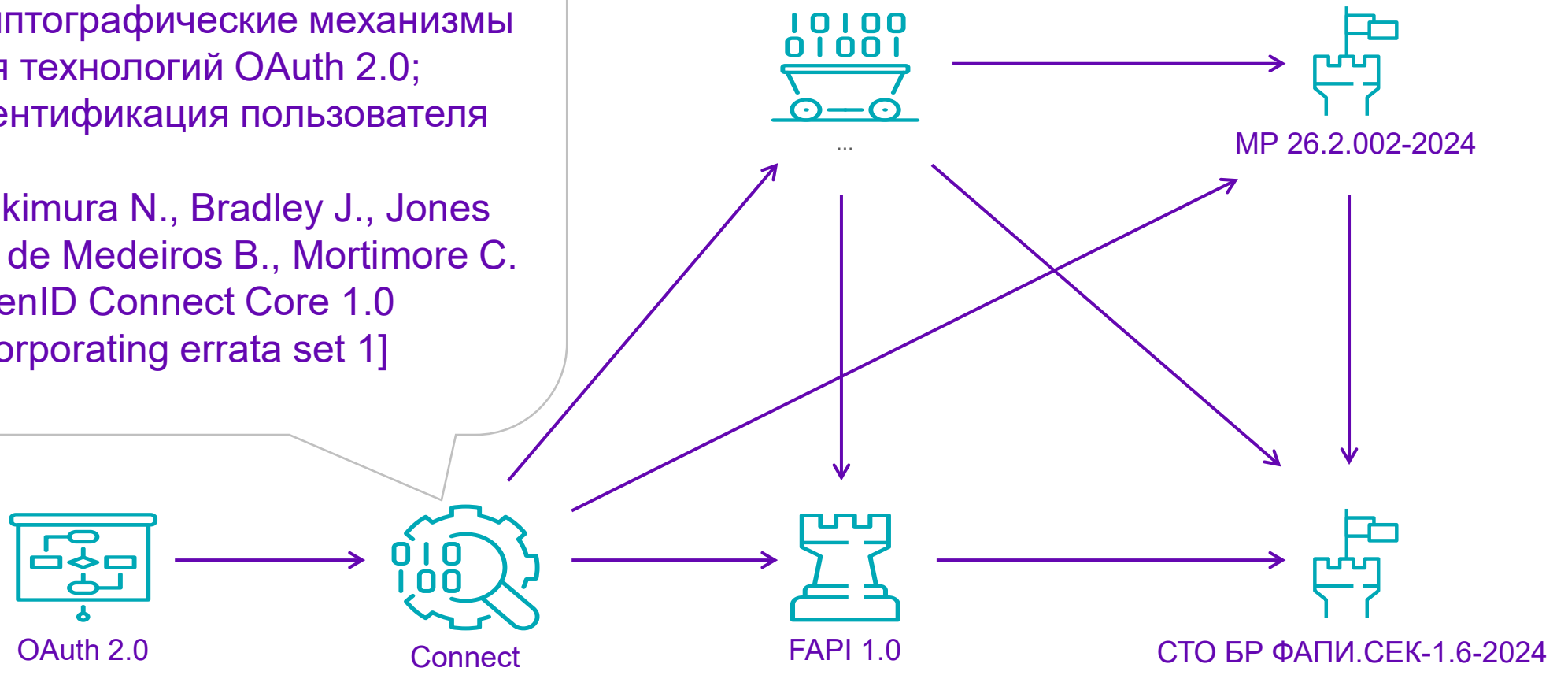


Технологическая база Open API

РусКрипто

Профиль OAuth 2.0;
криптографические механизмы для технологий OAuth 2.0;
идентификация пользователя

[Sakimura N., Bradley J., Jones M., de Medeiros B., Mortimore C. OpenID Connect Core 1.0 incorporating errata set 1]

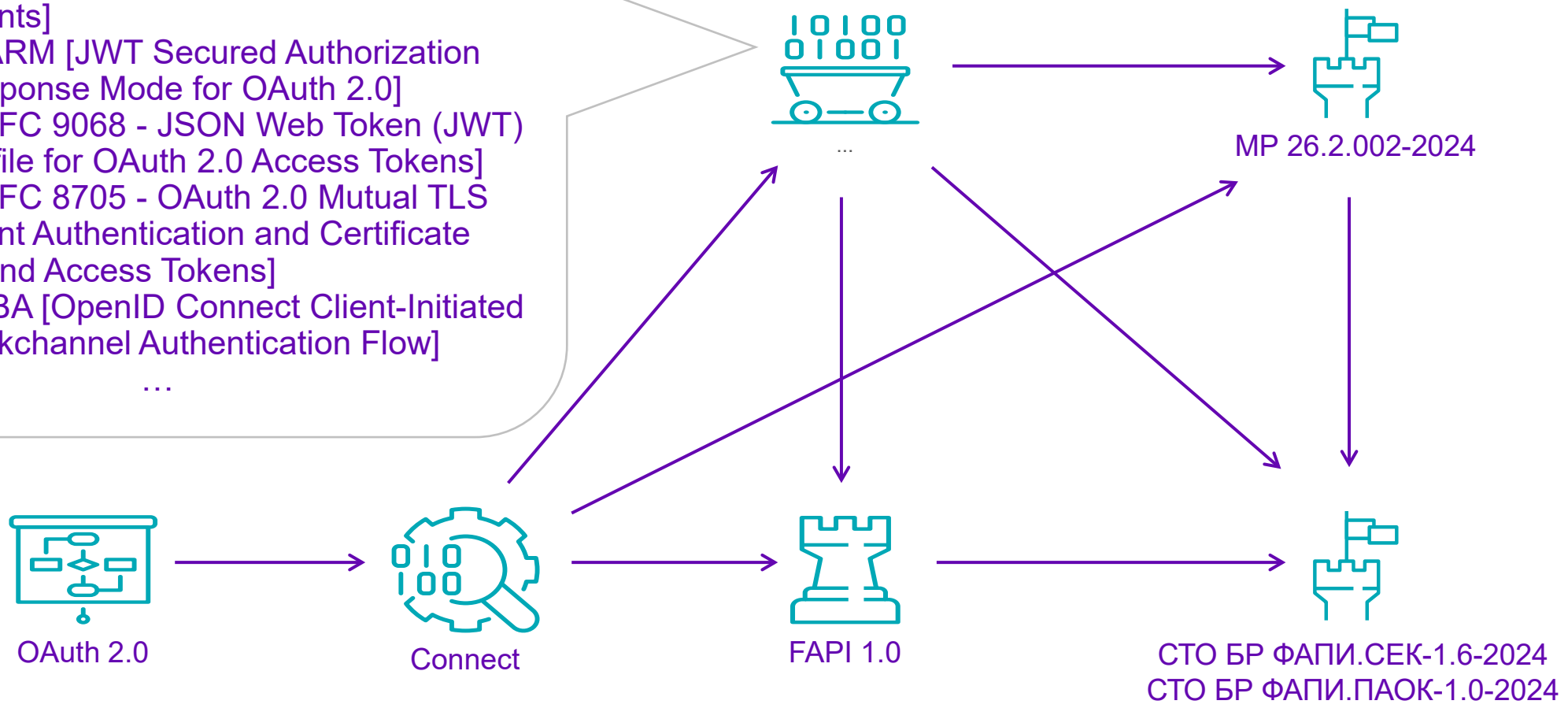


Технологическая база Open API

РусКрипто

- PKCE [RFC 7636 - Proof Key for Code Exchange by OAuth Public Clients]
- JARM [JWT Secured Authorization Response Mode for OAuth 2.0]
- [RFC 9068 - JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens]
- [RFC 8705 - OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens]
- CIBA [OpenID Connect Client-Initiated Backchannel Authentication Flow]

…

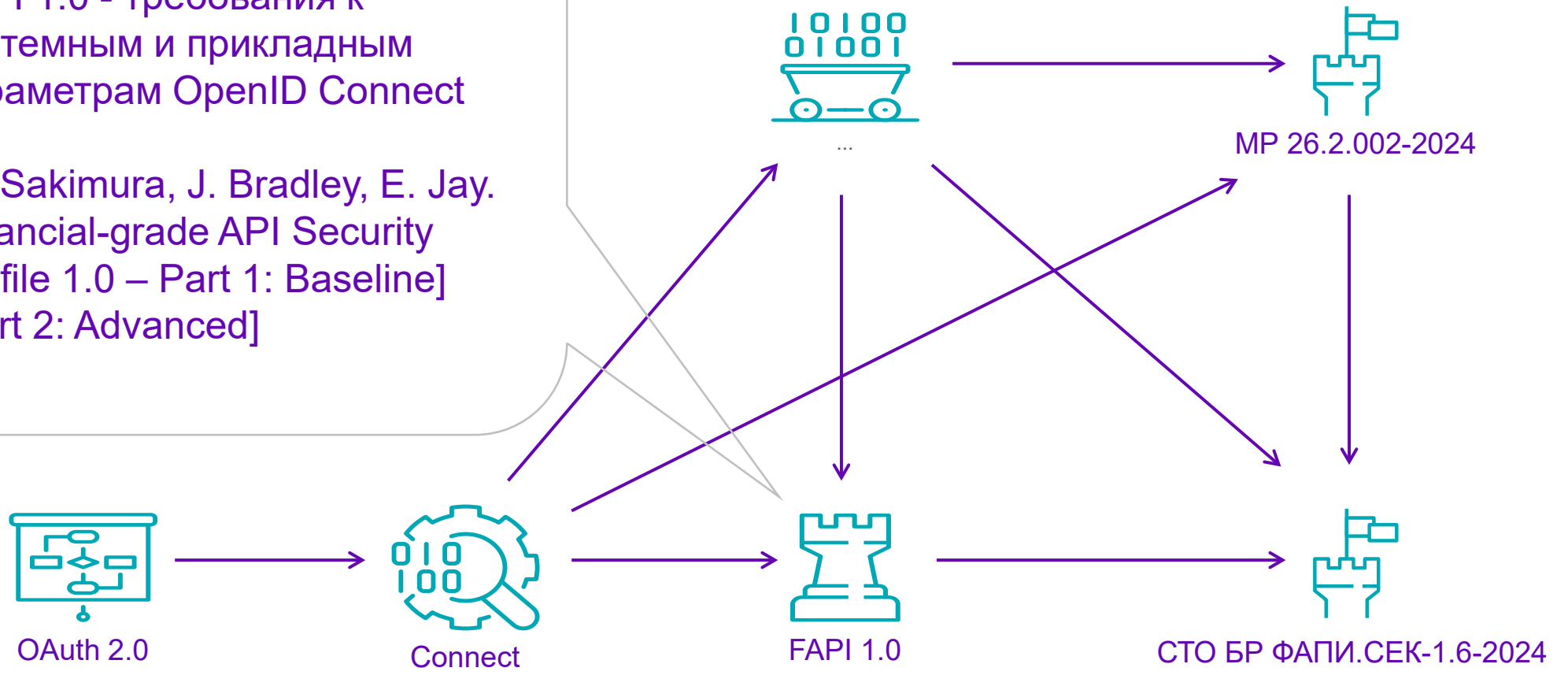


Технологическая база Open API

РусКрипто

FAPI 1.0 - требования к системным и прикладным параметрам OpenID Connect

[N. Sakimura, J. Bradley, E. Jay. Financial-grade API Security Profile 1.0 – Part 1: Baseline]
[Part 2: Advanced]

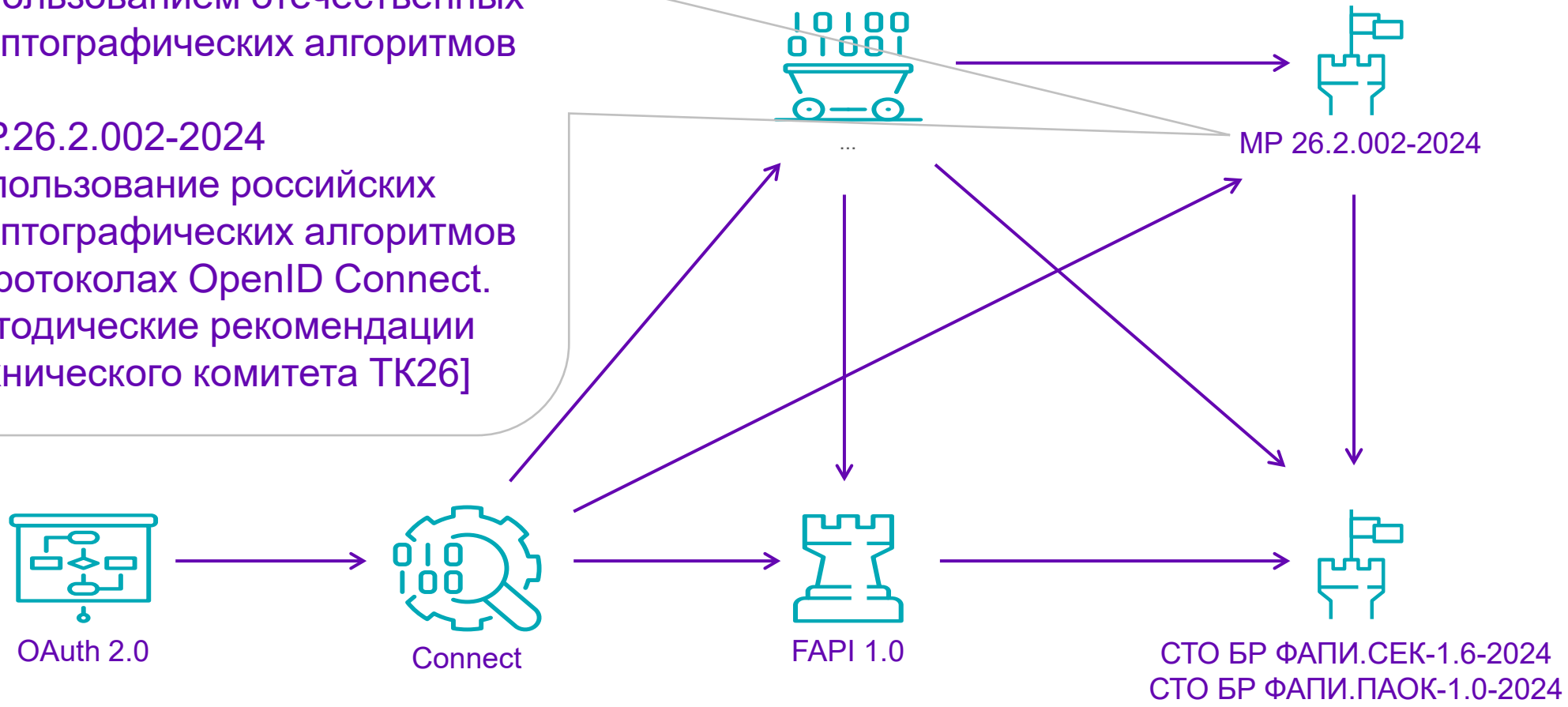


Технологическая база Open API

РусКрипто

OpenID Connect с использованием отечественных криптографических алгоритмов

[МР.26.2.002-2024 Использование российских криптографических алгоритмов в протоколах OpenID Connect. Методические рекомендации Технического комитета ТК26]

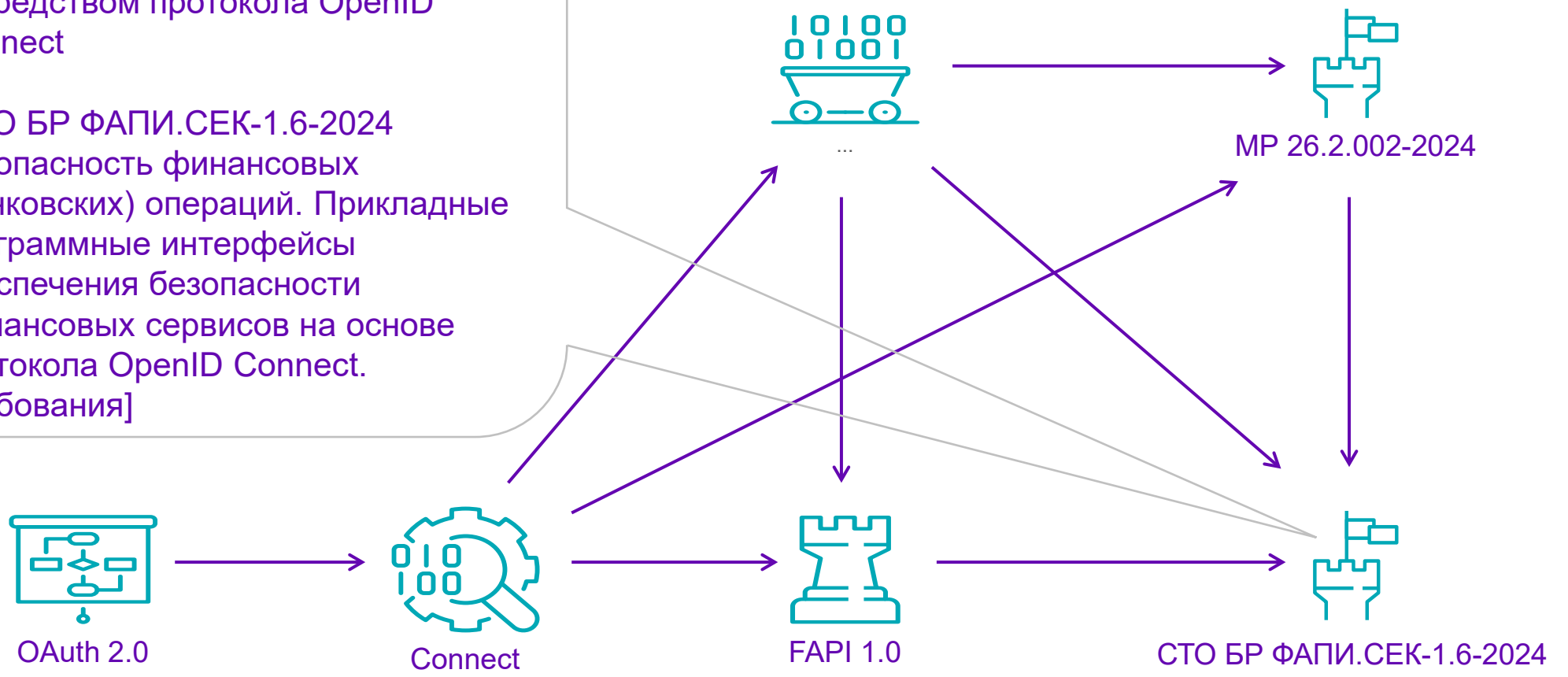


Технологическая база Open API

РусКрипто

Обеспечения безопасного доступа к данным в финансовых сервисах посредством протокола OpenID Connect

[СТО БР ФАПИ.СЕК-1.6-2024 Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID Connect. Требования]

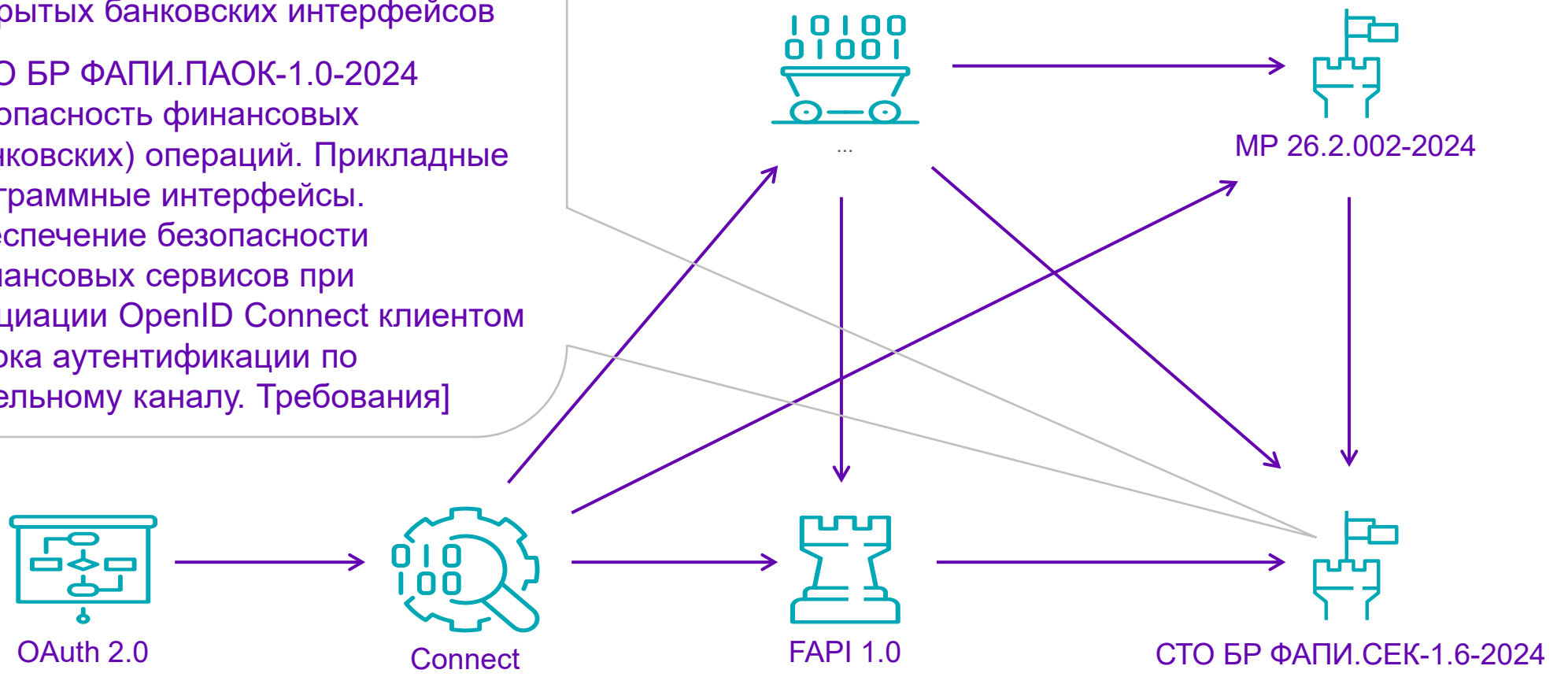


Технологическая база Open API

РусКрипто

Требования к ИБ при передаче защищаемой информации в среде Открытых банковских интерфейсов

[СТО БР ФАПИ.ПАОК-1.0-2024 Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования]



Типовая схема доступа к защищенному ресурсу

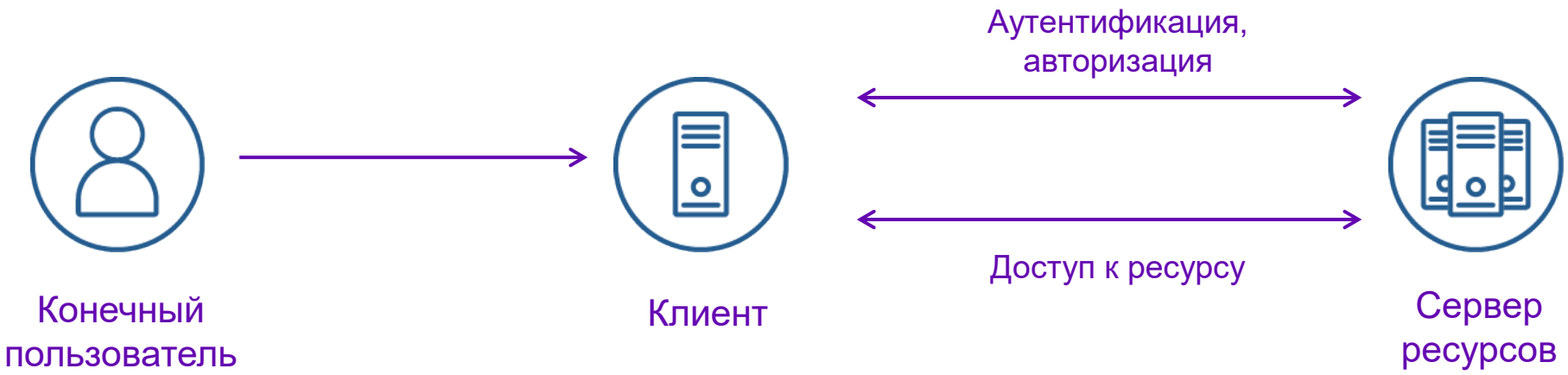


Схема доступа с OpenID Connect. Режим 1

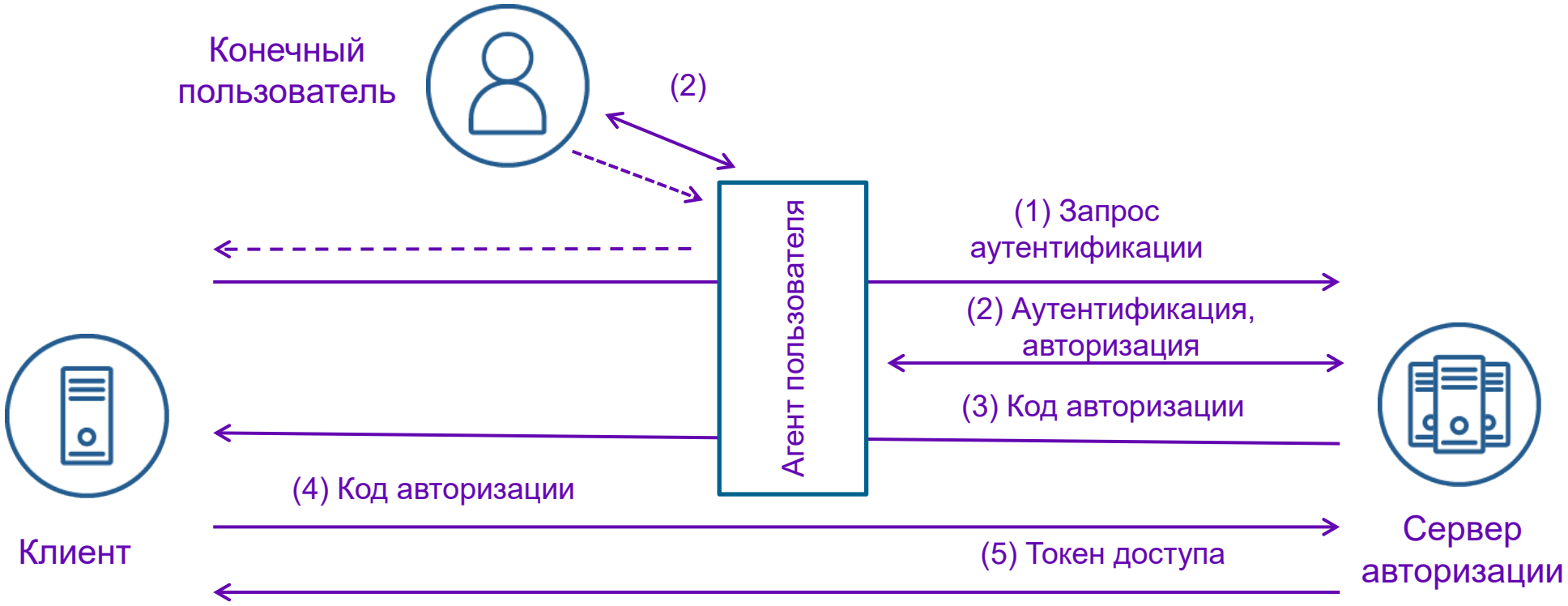


Схема доступа с OpenID Connect. Режим 2

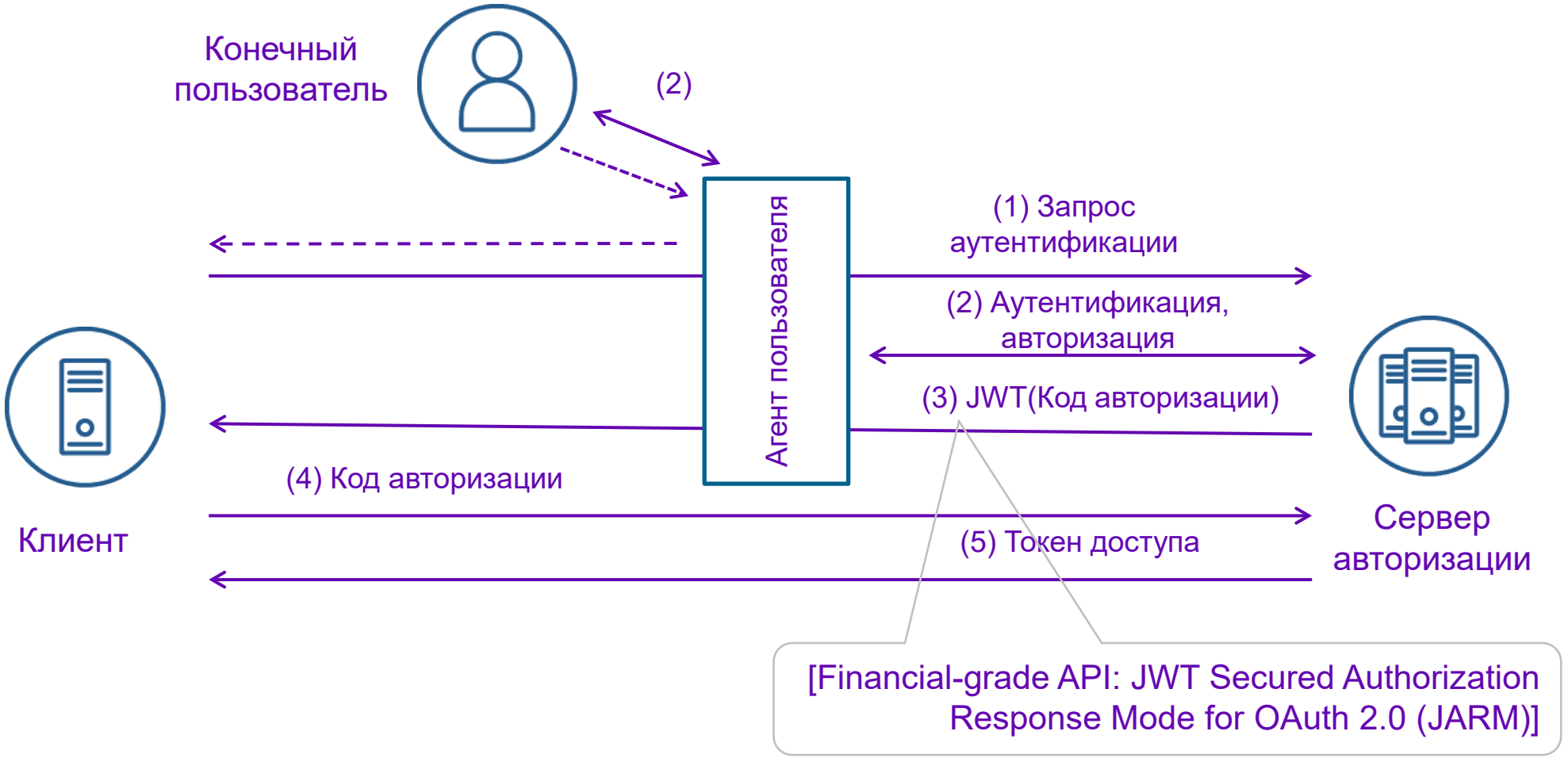


Схема доступа с OpenID Connect. Режим 3

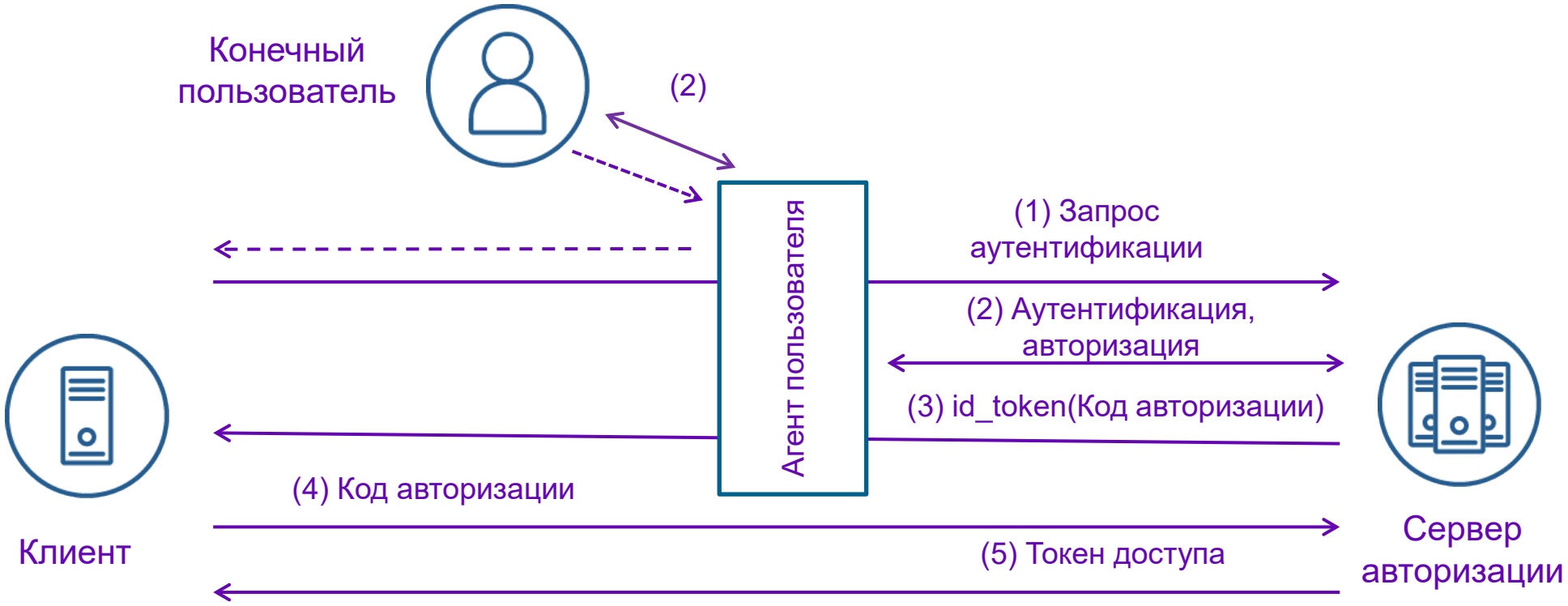
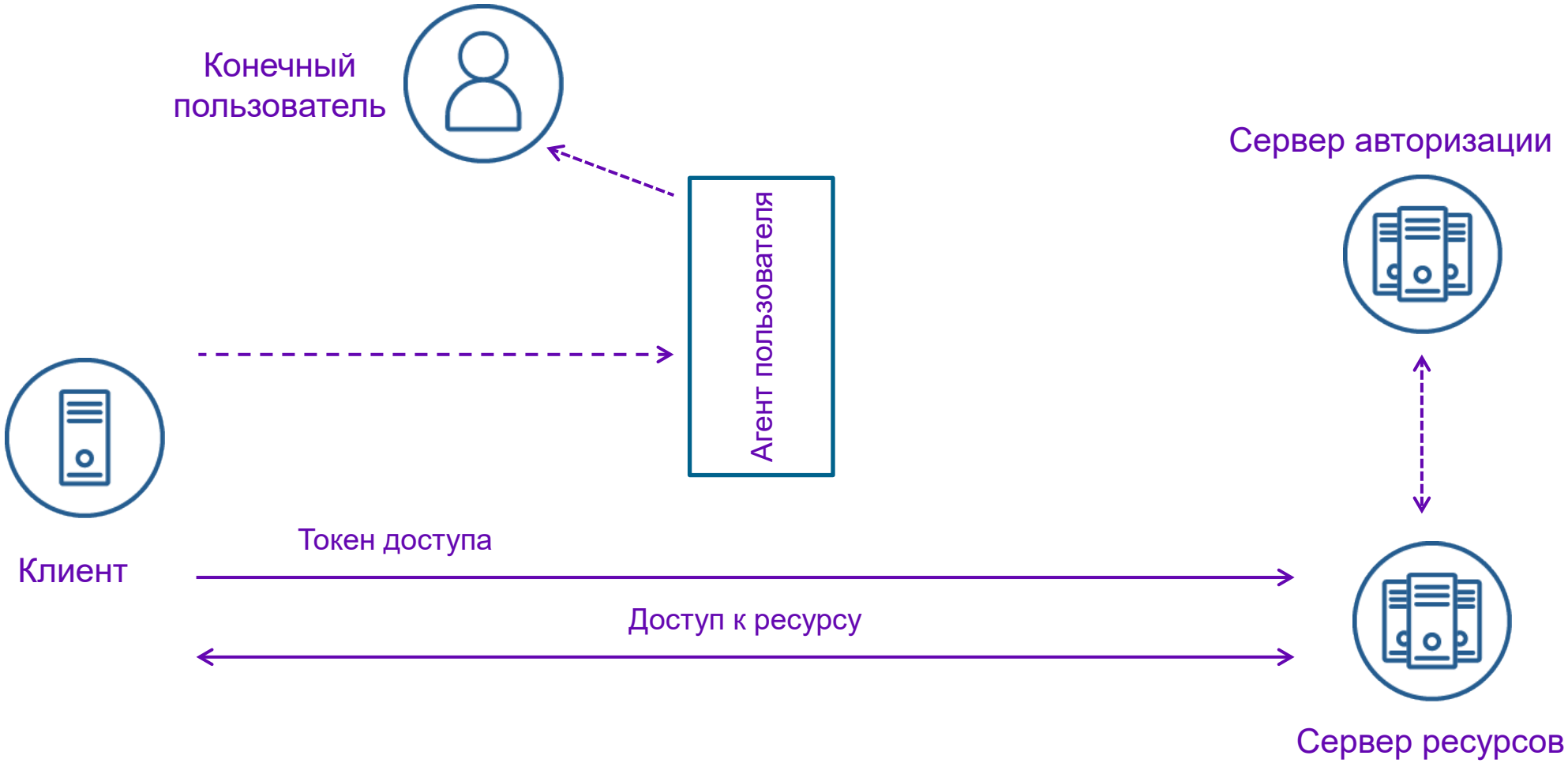


Схема доступа к серверу ресурсов с OpenID Connect



РусКрипто

Протоколы OpenID Connect с использованием российских криптографических алгоритмов:

- ГОСТ Р 34.10-2012
- ГОСТ Р 34.11-2012
- ГОСТ Р 34.12-2015
- Р 1323565.1.026-2019
- Р 1323565.1.020-2020

[МР 26.2.002-2024 на https://tc26.ru]

[Использование российских криптографических алгоритмов в протоколах OpenID Connect. РусКрипто-2022]

Угрозы безопасности

- Маскарад
- Утечки конфиденциальной информации…
- Подделка сообщений, навязывание ложной информации…
- Подмена токенов доступа, перехват и повторное использование токенов и кодов авторизации
- Противодействие ряду не криптографических кибератак
- …

РусКрипто

ISO серия Information technology - OpenID connect:

- ISO/IEC 26131:2024 OpenID connect core 1.0 incorporating errata set 2
- ISO/IEC 26132:2024 OpenID connect discovery 1.0 incorporating errata set 2
- ISO/IEC 26133:2024 OpenID connect dynamic client registration 1.0 incorporating errata set 2
- ISO/IEC 26134:2024 OpenID connect RP-initiated logout 1.0
- ISO/IEC 26135:2024 OpenID connect session management 1.0
- ISO/IEC 26136:2024 OpenID connect front-channel logout 1.0
- ISO/IEC 26137:2024 OpenID connect backchannel logout 1.0 incorporating errata set 1
- ISO/IEC 26138:2024 OAuth 2.0 multiple response type encoding practices
- ISO/IEC 26139:2024 OAuth 2.0 form post response mode

РусКрипто

Стандартизация в IETF (BCP):

- RFC 9700, BCP 240 - Best Current Practice for OAuth 2.0 Security. 2025

РусКрипто

OAuth 2.1:

- PKCE для всех клиентов, использующих сценарий с кодом авторизации
- Implicit grant (response_type = token) исключено из этой спецификации
- Предоставление учетных данных пароля владельца ресурса в этой спецификации исключено
- Исключается использование токенов на предъявителя в строке запроса URI
- Токены обновления для общедоступных клиентов должны быть ограничены отправителем или использоваться один раз
- …

[The OAuth 2.1 Authorization Framework. IETF, 2024. draft-ietf-oauth-v2-1-12]

РусКрипто

GNAP:

- Не требуется обязательное наличие веб браузера у пользователя
- Конечный пользователь, инициировавший операции клиента, не обязательно совпадает с владельцем ресурса
- Токены привязываются к конкретному клиенту. Минимизируется использование токенов на предъявителя
- Механизм интроспекции токена более богатый
- Отсутствует понятие «public client», предполагается использование криптографии
- Более гибкая технология, позволяет ее расширять

[RFC9635 Grant Negotiation and Authorization Protocol (GNAP). IETF, 2024]

Развитие FAPI 1.0

Фиксация FAPI 1.0:

- ISO/IEC DIS 25791-1 Information technology - OpenID Connect FAPI Security Profile 1.0 - Part 1: Baseline
- ISO/IEC DIS 25791-2 Information technology - OpenID Connect FAPI Security Profile 1.0 - Part 2: Advanced

Развитие: FAPI 2.0

- FAPI 2.0 Security Profile. OpenID Foundation, 2025

РусКрипто

Банк России

infotecs

СПАСИБО
ЗА ВНИМАНИЕ