infotecs

Об отдельных направлениях стандартизации в области PKI

infotecs

СТО БР ФАПИ.СЕК-1.6-2020

Безопасность финансовых (банковских) операций (ФАПИ.СЕК).

Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Требования

СТО БР ФАПИ.СЕК-1.6-2020

infotecs

Разработан на базе рекомендаций **OpenID FAPI** по инициативе Ассоциации ФинТех

Утвержден в ТК 122
Согласован с ТК26

СТО БР ФАПИ.СЕК-1.6-2020

Рекомендован к использованию в программных средствах для безопасного обмена финансовыми сообщениями, связанными с:

- получением информации о банковском счете
- переводом денежных средств в валюте Российской Федерации

СТО БР ФАПИ.СЕК-1.6-2020

Предназначен для организаций:

- участников получения информации о банковском счете (банки, клиенты, сторонние поставщики)
- участников перевода денежных средств (банки, клиенты, сторонние поставщики)
- разработчиков программного обеспечения, информационных систем

СТО БР ФАПИ.СЕК-1.6-2020

Содержит **требования и рекомендации** для обеспечения безопасного доступа к финансовым данным в финансовых сервисах реального времени с использованием модели обмена данными **REST/JSON**, защищенной технологией **OAuth 2.0**, включая протокол **OpenID Connect**

Не устанавливает конкретных требований к криптографическим алгоритмам
Применяется совместно с требованиями технической спецификации ТК26 «Использование российских криптографических алгоритмов в протоколах OpenID Connect» (разрабатывается)

СТО БР ФАПИ.СЕК-1.6-2020

infotecs

Состав:

- нормативные требования
- общие сведения о протоколах авторизации OAuth 2.0 и аутентификации OpenID Connect, регистрации сервера доступа и клиента
- профиль безопасности OpenID API для доступа к сервисам в режиме только для чтения
- профиль безопасности OpenID API для доступа к сервисам в режиме чтения и записи,
- защищенный с использованием JWT режим ответа на запрос авторизации OAuth 2.0 (JARM)

СТО БР ФАПИ.СЕК-1.6-2020

Нормативные требования:

- СКЗИ соответствует требованиям Регулятора
- безопасность персональных данных в соответствии с законодательными и нормативными актами РФ
- анализ уязвимостей прикладного финансового ПО по требованиям Положений БР 382-П, 683-П и 684-П
- безопасность разработки ПО согласно ГОСТ Р 56939

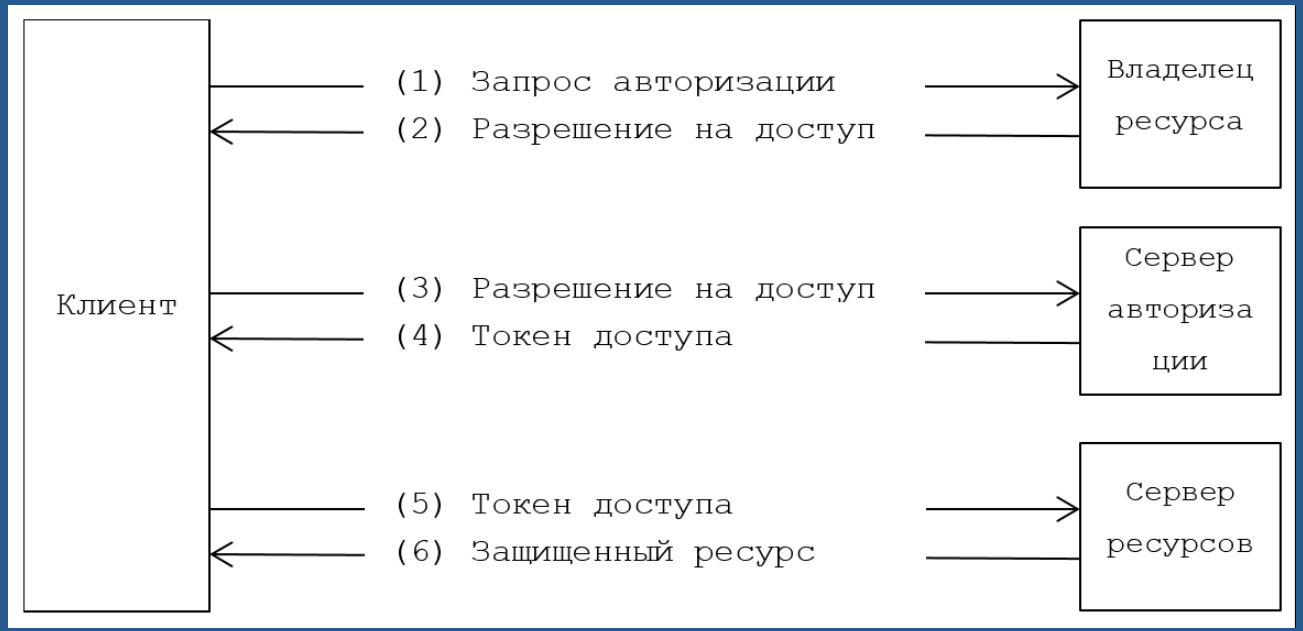
OpenID FAPI:

- Financial-grade API – Part 1: Read Only API Security Profile (Implementer's Draft). OpenID Foundation, Financial-grade API (FAPI) WG, 2019
- Financial-grade API – Part 2: Read & Write API Security Profile (Implementer's Draft). OpenID Foundation, Financial-grade API (FAPI) WG, 2019
- Financial-grade API – JWT Secured Authorization Response Mode for OAuth 2.0 (JARM) (Implementer's Draft). OpenID Foundation, Financial-grade API (FAPI) WG, 2019

OpenID OAuth 2.0:

- Hardt D. The OAuth 2.0 Authorization Framework. RFC 6749
- Jones M., Hardt D. The OAuth 2.0 Authorization Framework: Bearer Token Usage. RFC 6750
- OAuth 2.0 Token Introspection. RFC 7662

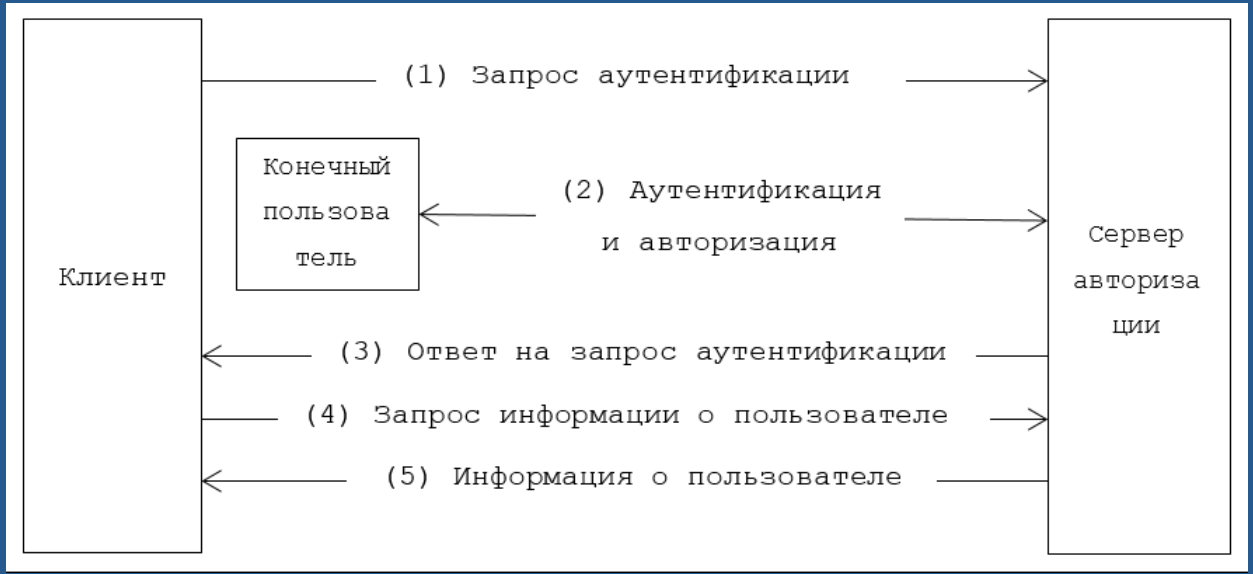
Протокол авторизаци OAuth 2.0:



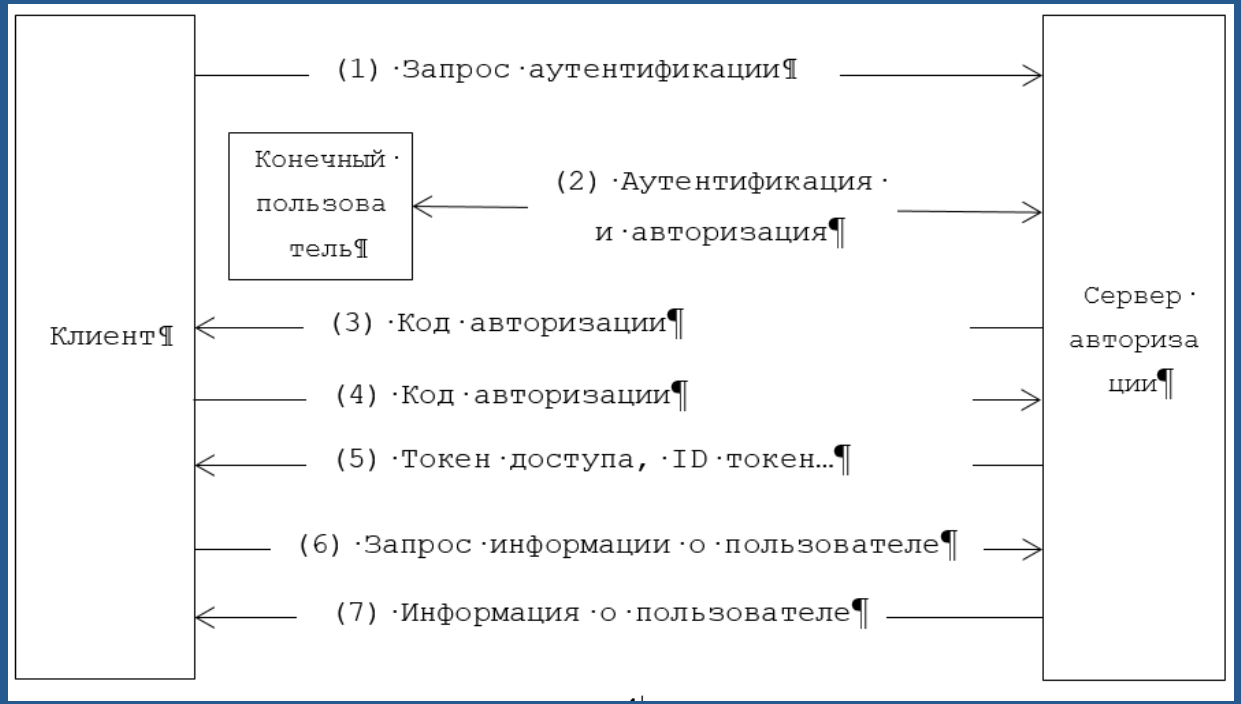
OpenID Connect:

- Sakimura N., Bradley J., Jones M., de Medeiros B., Mortimore C. OpenID Connect Core 1.0 incorporating errata set 1. November 8, 2014
- Sakimura N., Bradley J., Jones M., Jay E. OpenID Connect Discovery 1.0 incorporating errata set 1. November 8, 2014
- Sakimura N., Bradley J., Jones M. OpenID Connect Dynamic Client Registration 1.0 incorporating errata set 1. November 8, 2014

Протокол аутентификации OpenID Connect:



Протокол OpenID Connect с кодом авторизации:



СТО БР ФАПИ.СЕК-1.6-2020

infotecs

ФАПИ.СЕК наследует от FAPI:

- OpenID OAuth 2.0 и Connect
- токены доступа
- токены обновления
- ID токены в формате JWT (JSON Web Token) по RFC 7519
- цифровая подпись и MAC в формате JWS по RFC 7515
- шифрование в формате JWE по RFC 7516
- структура ключевой информации в формате JWK по RFC 7517
- TLS для защиты всех транзакций
- MTLS для аутентификации клиента по RFC 8705

СТО БР ФАПИ.СЕК-1.6-2020

infotecs

Отличие от FAPI:

- не использует публичных клиентов (только конфиденциальные)
- не поддерживает неявный (implicit) сценарий авторизации
- использует только один тип разрешения на доступ: authorization grant
- отечественная криптография согласно технической спецификации ТК26 «Использование российских криптографических алгоритмов в протоколах OpenID Connect» (JWT, JWS, JWE, JWK на отечественных стандартах криптоалгоритмов)
- TLS 1.2 по МР 26.2.001–2013 и Р 1323565.1.020-2018
- отсутствуют требования доверия к аутентификации конечного пользователя

Доверие к идентификации и аутентификации

Идентификация и аутентификация

Доверие к аутентификации объектов:

- X.1254/ISO 29115 «Information technology — Security techniques — Entity authentication assurance framework»: 4 уровня доверия к аутентификации объекта: LoA1 – LoA4

Идентификация и аутентификация

Доверие к аутентификации объектов:

- X.1254/ISO 29115 «Information technology — Security techniques — Entity authentication assurance framework»: 4 уровня доверия к аутентификации объекта: LoA1 – LoA4
- проект ГОСТ Р «Защита информации. Идентификация и аутентификация. Уровни доверия к результатам аутентификации»

Идентификация и аутентификация

infotecs

Доверие к аутентификации среды:

- Целостность программно-аппаратной среды проверяет отправитель (АМДЗ, TPM)
- Целостность программно-аппаратной среды не проверяет получатель
- Некоторые дистанционные сервисы передают параметры среды вычислений (ДБО…) на уровне приложения
- Требуется: на уровне средств защиты информации с передачей результатов в составе сообщений криптографического протокола

О стандартизации сервисов доверия в ТК26

Выпущены ТК26 – 66 (tc26.ru):

- ГОСТов - 4
- Рекомендаций по стандартизации (Р) - 31
- Методических рекомендаций (МР) - 24
- Технических спецификаций (ТС) - 7

По сервисам криптографии:

- Аутентификация - 40
- Целостность - 39
- Конфиденциальность - 35
- Управление ключами - 34
- TLS - 5
- ДСЧ - 3
- Методология - 2

По области применения:

- Общего назначения - 21
- PKI - 20
- IoT - 8
- Платежные карты - 16
- Распределенный реестр - 1

infotecs

Инициативная разработка!

Причины:

- Отсутствие спроса у потребителей (импортируемые решения)
- Отсутствие большого числа специалистов (ТК26)

infotecs

Потребители криптографии должны быть заинтересованы в международной и отечественной стандартизации криптографии

TK26

- TK26?

ТК26

- ТК26
- Лаборатория в АК?

ТК26

- ТК26
- Лаборатория в АК
- НТЦ ВМСК?

ТК26

- ТК26
- Лаборатория в АК
- НТЦ ВМСК

Что делать:

- Анализ потребности в новых криптографических механизмах (АК)
- Синтез отечественных стандартов криптографических механизмов (ТК26)
- Продвижение отечественных криптографических стандартов в международных организациях по стандартизации
- Контроль отраслевых отечественных и международных стандартов, использующих криптографические механизмы

infotecs

Потребители криптографии должны быть заинтересованы в международной и отечественной стандартизации криптографии!

Спасибо!

Mikhail.Gruntovich@infotecs.ru