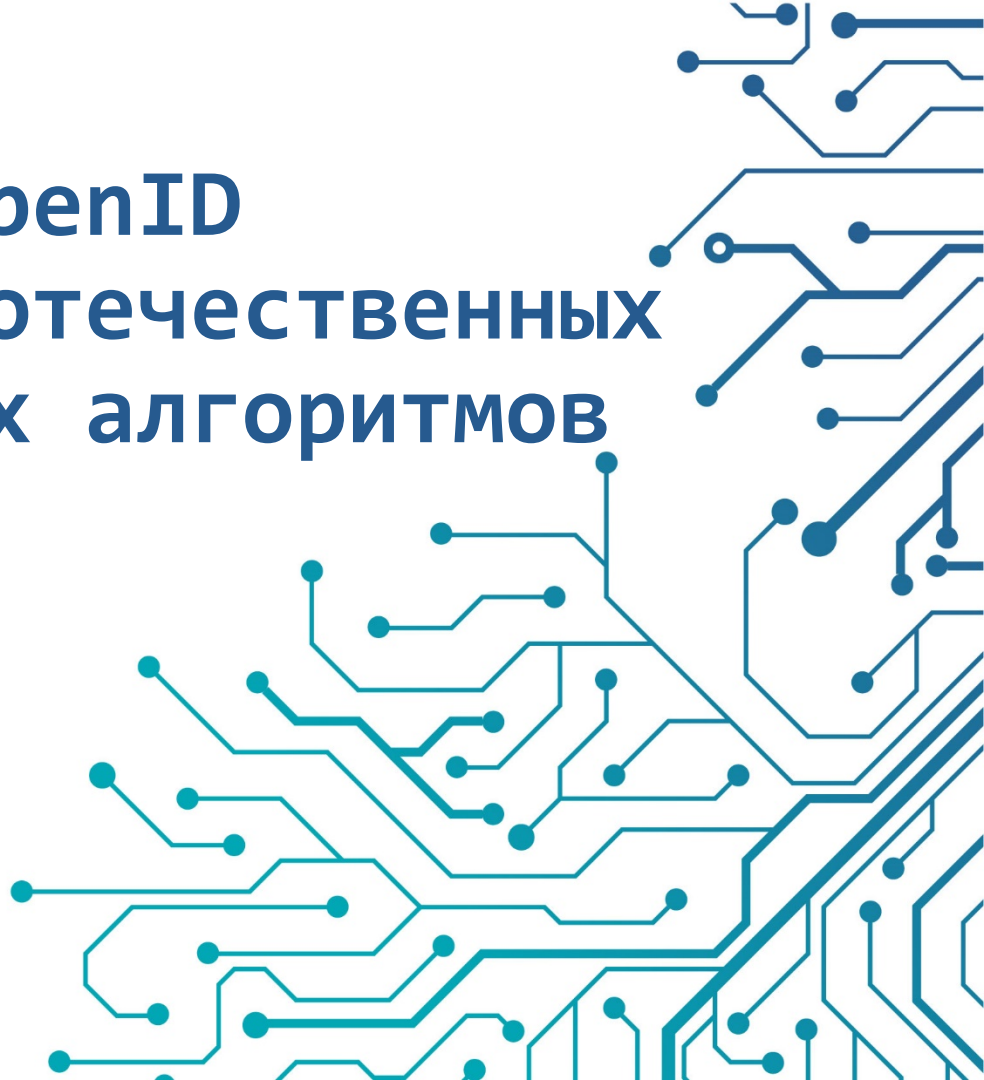
Стандартизация OpenID Connect на базе отечественных криптографических алгоритмов

Грунтович М.М.
Mikhail.Gruntovich@infotecs.ru



infotecs

OpenID Connect

- Единая система идентификации и аутентификации (ЕСИА)
- Единая биометрическая система (ЕБС)
- 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.ПАОК-1.0-2021 Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OPENID CONNECT клиентом потока аутентификации по отдельному каналу. Требования

OpenID Connect

infotecs

СТО БР ФАПИ.СЕК-1.6-2020:

«Положения настоящего стандарта применяются совместно с документом Технического комитета ТК26 «Использование российских криптографических алгоритмов в протоколах OpenID Connect»

OpenID Connect

Технические спецификации ТК26 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколах OpenID Connect»

OpenID Connect

Технические спецификации ТК26 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколах OpenID Connect»

- Текст
- Контрольные примеры
- Эталонная реализация
- Обоснование

OpenID Connect

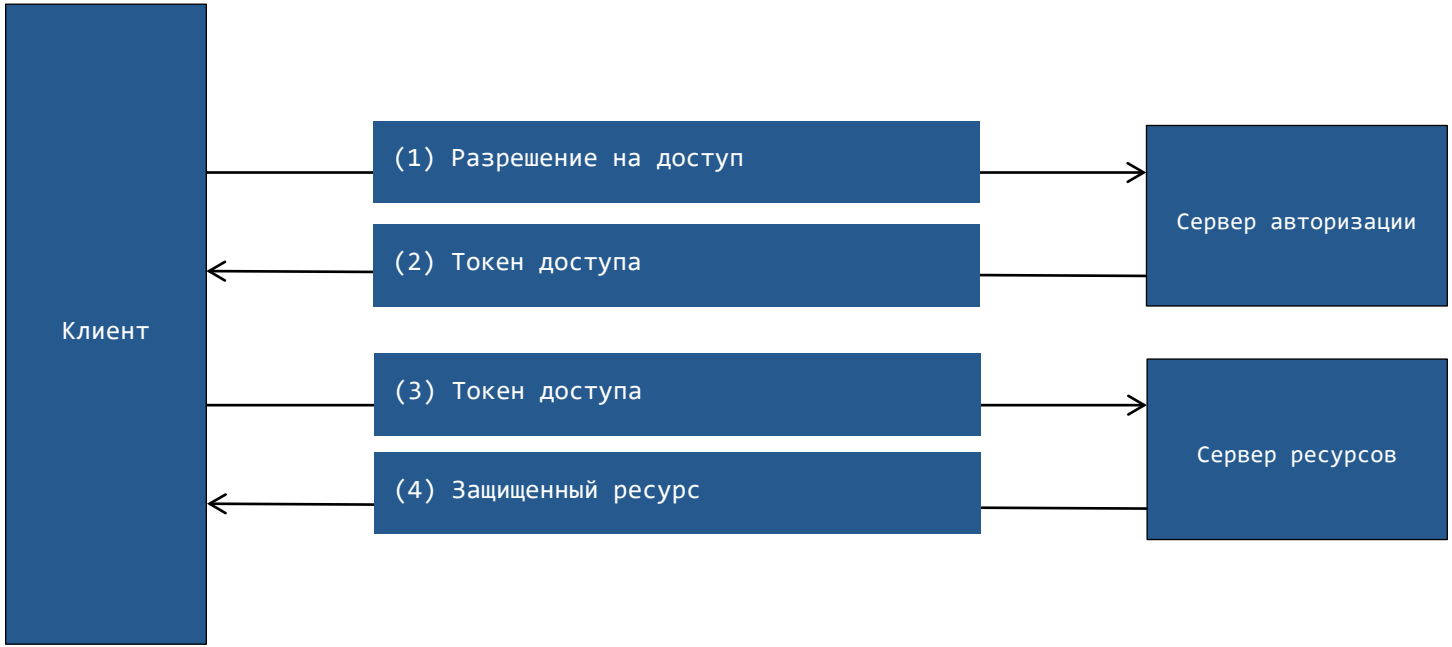
Технические спецификации ТК26 «Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколах OpenID Connect»

- Получены замечания экспертной организации
- Работаем над устранением замечаний

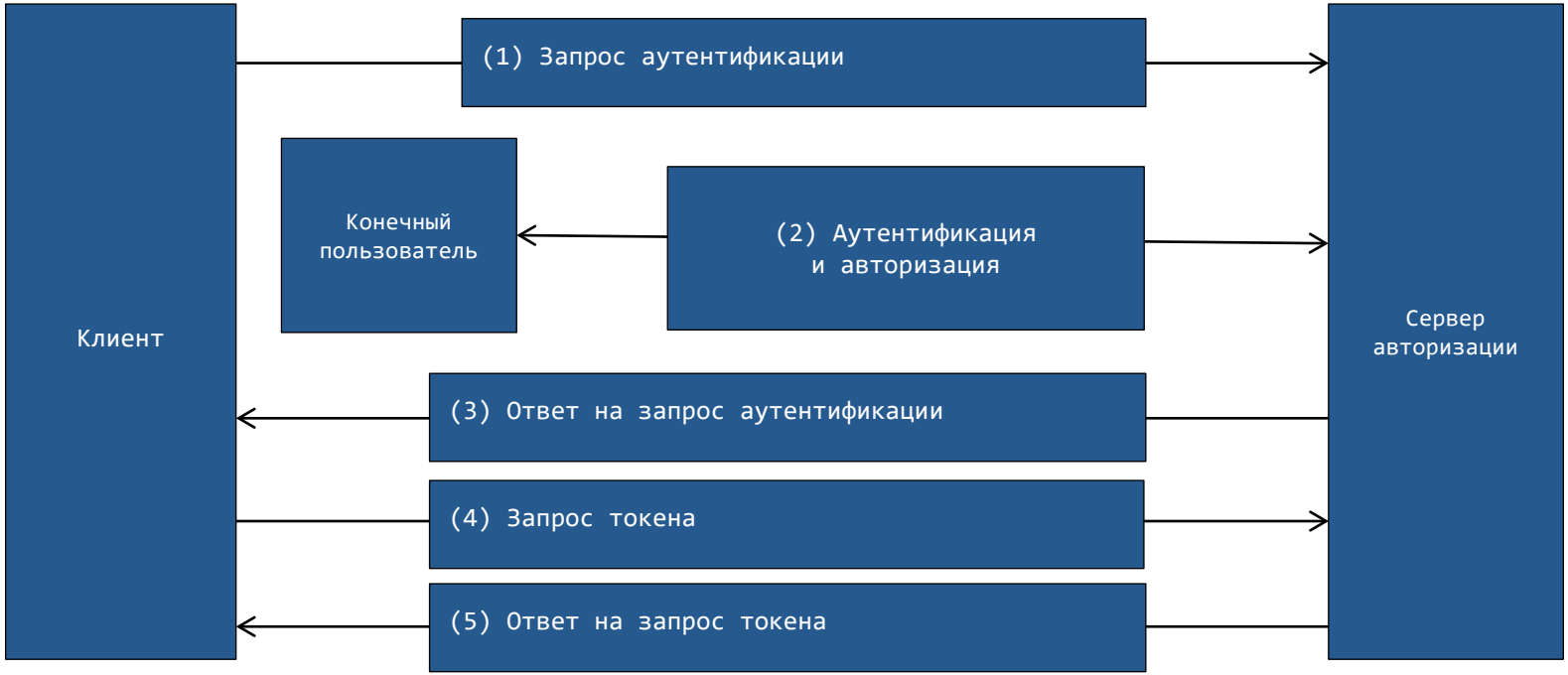
Протокол OpenID Connect

OpenID Connect позволяет приложению – клиенту получить доступ к защищенным данным приложения – сервера ресурсов

Протокол OpenID Connect



Протокол OpenID Connect



Режимы OpenID Connect

- Режим 1: базовый протокол OpenID Connect с генерацией кода авторизации
- Режим 2: протокол OpenID Connect с генерацией кода авторизации и передачей ответа на запрос аутентификации с цифровой подписью сервера авторизации в формате JARM
- Режим 3: протокол OpenID Connect с генерацией кода авторизации и передачей ответа на запрос аутентификации с цифровой подписью сервера авторизации в формате ID токена
- PKCE (Proof Key for Code Exchange): ключ подтверждения передачи кода авторизации

Алгоритмы ГОСТ в OpenID Connect

- Цифровая подпись по алгоритму ГОСТ Р 34.10-2012
- КА по алгоритму HMAC_GOST3411_2012_256 (Р 50.1.113-2016)
- Диверсификация ключа по алгоритму KDF_GOSTR3411_2012_256 (Р 50.1.113-2016) на основе хэш-функции ГОСТ Р 34.11-2012
- Согласование ключа VKO_GOSTR3410_2012_256 (Р 50.1.113-2016) с длиной 256 бит на основе хэш-функции ГОСТ Р 34.11-2012
- Шифрования данных шифрами «Кузнечик» и «Магма» в режиме MGM (Р 1323565.1.026-2019)

Ключи OpenID Connect

- Ключи TLS сервера авторизации и клиента
- client_secret – симметричный ключ клиента
- Ключи ЭЦП сервера авторизации и клиента
- Ключи вычисления ключей шифрования сервера авторизации и клиента

OpenID Connect в ЕСИА+ЕБС

- ЕСИА, как сервер авторизации, аутентифицирует пользователя в процессе OpenID Connect по логин/паролю
- ЕСИА, как сервер ресурсов, хранит ПДн пользователя и предоставляет эти данные клиенту
- ЕБС, как сервер авторизации, аутентифицирует пользователя в процессе OpenID Connect по биометрическим данным
- ЕБС, как сервер ресурсов, хранит биометрические данные пользователя и предоставляет клиенту результат верификации

infotecs

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363

Спасибо за внимание!

Грунтович Михаил Михайлович

Руководитель обособленного подразделения

e-mail: Mikhail.Gruntovich@infotecs.ru

Подписывайтесь на наши соцсети

vk.com/infotecs_news

t.me/infotecs_news

rutube.ru/channel/24686363