ГИД

Аутентификация API

Подходы и практики

Блажина Ирина

Москва, 2025

Спикер

Ирина Блажина

Архитектор информационной безопасности
ООО «Оператор Газпром ИД»

- Более 10 лет опыта работы в IT
- Архитектор корпоративного и системного уровня, проектировка безопасных решений
- Специализация на архитектуре для ИБ на базе решений FW, Proxy, NGFW, IDM, IAM, API-Gateway, IDS/IPS и др.
- Автор статей в публичных каналах

О чем будем говорить?

1. Определения
2. Ключевые подходы к аутентификации
3. Распределение на практике
4. Что-то посложнее…
5. Лучшие практики
6. Бонус

О чем будем говорить?

1
Определения

2
Ключевые подходы к аутентификации

3
Распределение на практике

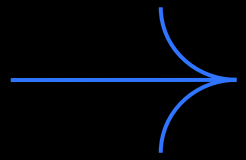
4
Что-то посложнее…

5
Лучшие практики

6
Бонус

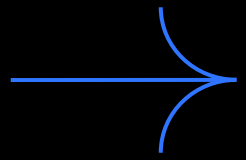
Определения

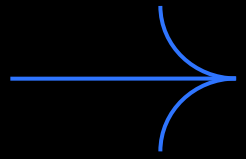
«Секрет»



Информация, используемая для проверки подлинности (напр., пароль, системный секрет)

Определения

«Секрет»  Информация, используемая для проверки подлинности (напр., пароль, системный секрет)

Аутентификация  Процедура проверки подлинности по «секрету»

Определения

«Секрет»	Информация, используемая для проверки подлинности (напр., пароль, системный секрет)
Аутентификация	Процедура проверки подлинности по «секрету»
Токен	Разновидность секрета, выдаваемая после процедуры аутентификации для доступа

Что важнее?

01

«Секрет»

02

Токен

О чем будем говорить?

1
Определения

2
Ключевые подходы к аутентификации

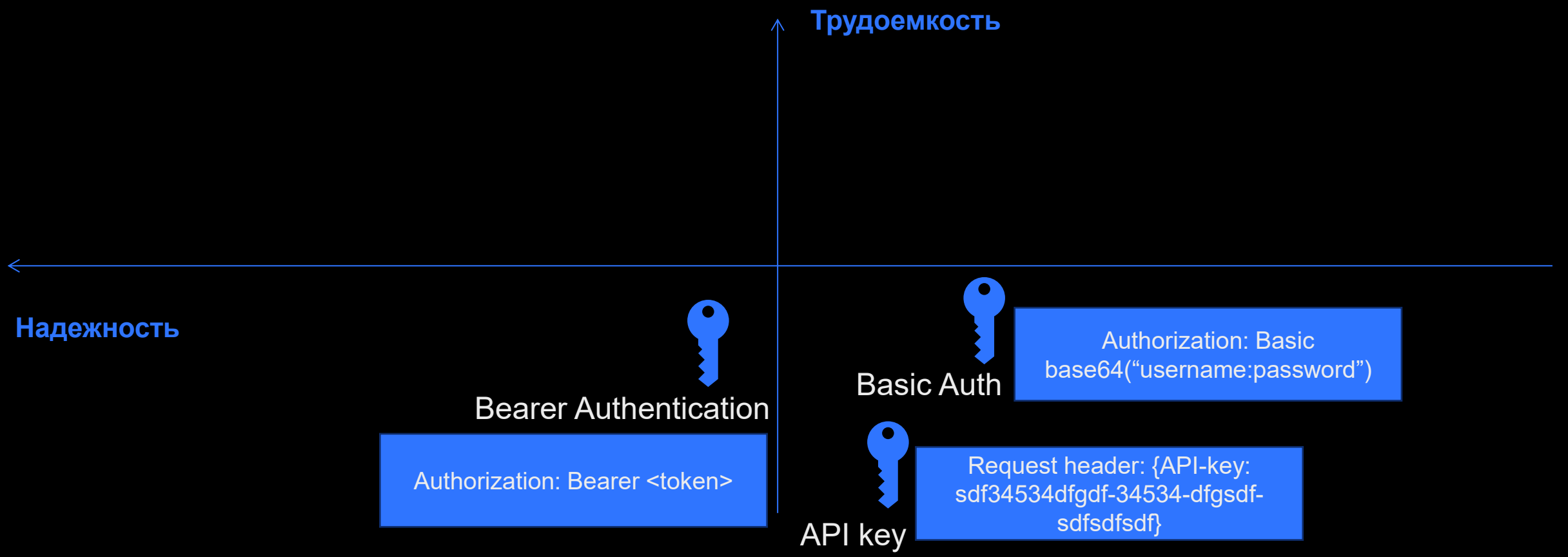
3
Распределение на практике

4
Что-то посложнее…

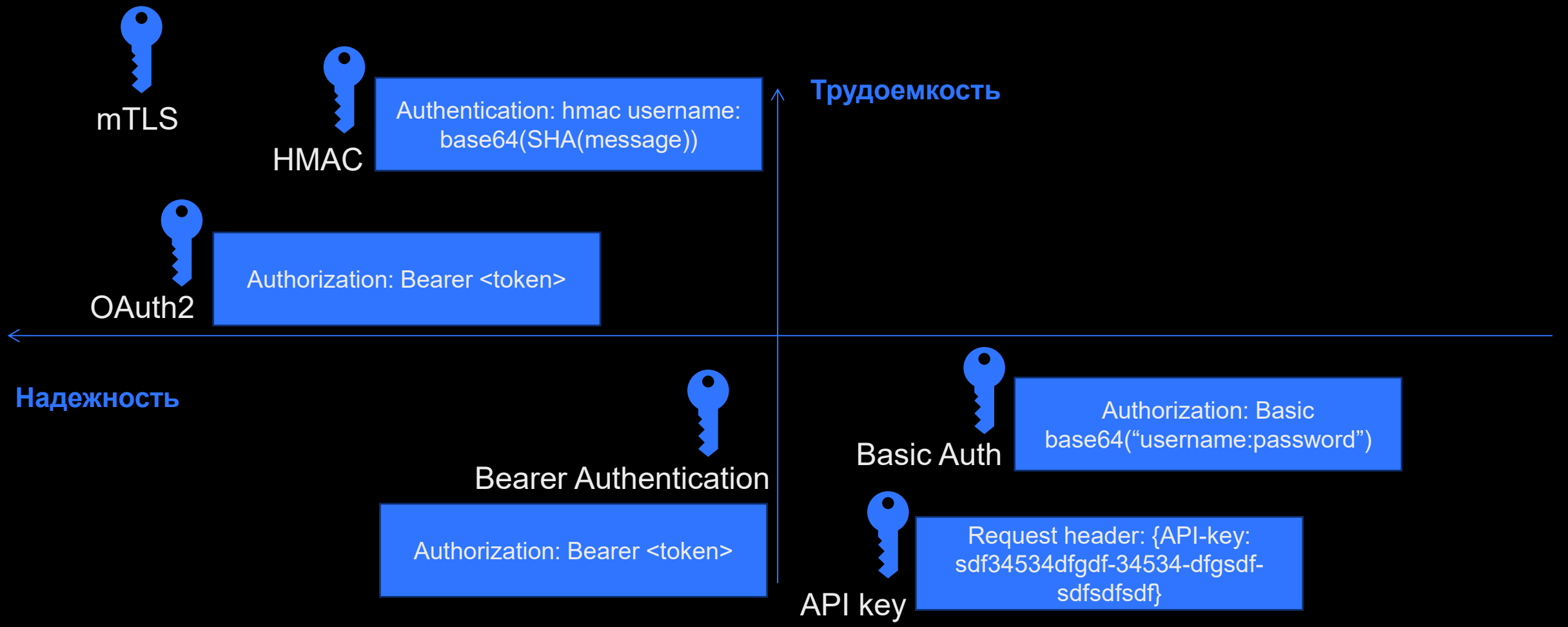
5
Лучшие практики

6
Бонус

Подходы к аутентификации API



Подходы к аутентификации API



О чем будем говорить?

1
Определения

2
Ключевые подходы к аутентификации

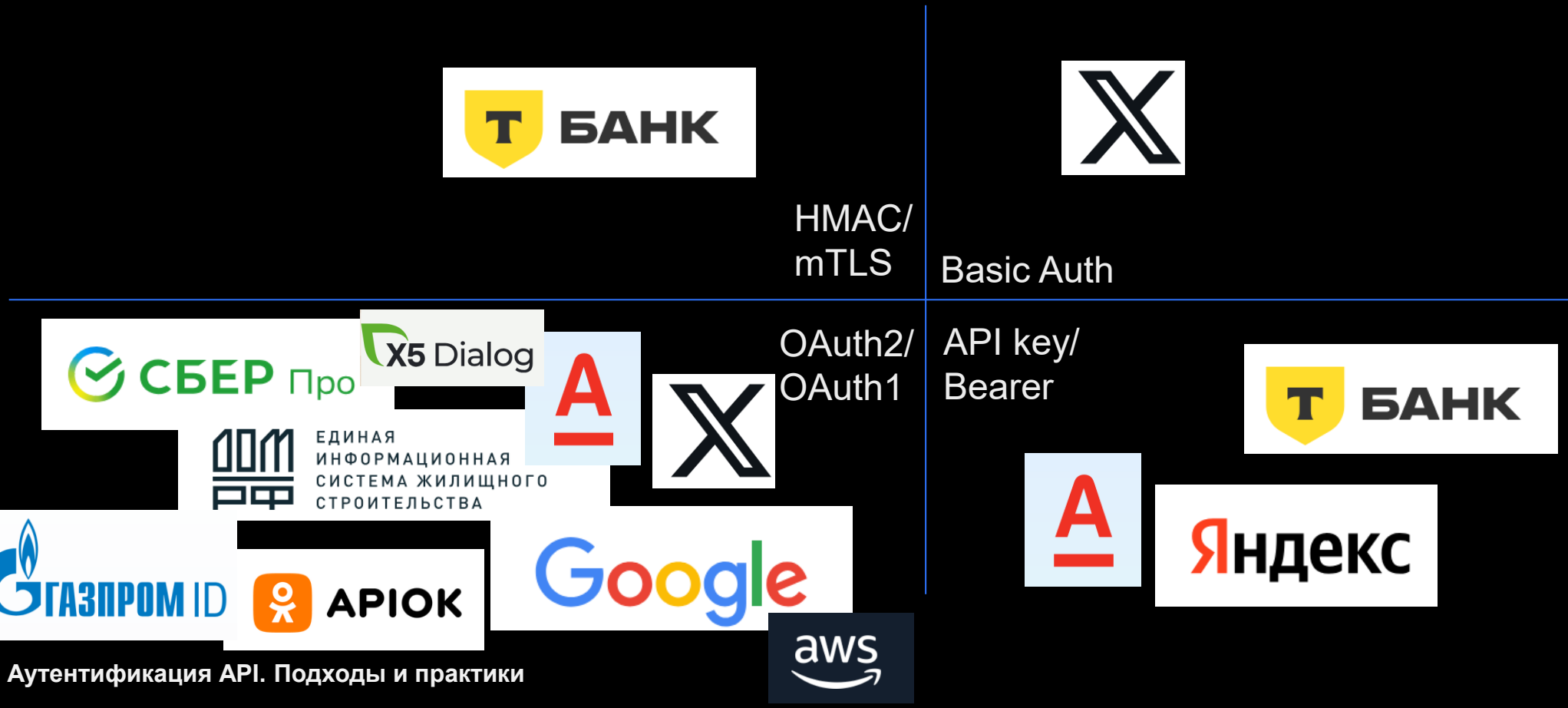
3
Распределение на практике

4
Что-то посложнее…

5
Лучшие практики

6
Бонус

Подходы на практике



О чем будем говорить?

1. Определения
2. Ключевые подходы к аутентификации
3. Распределение на практике
4. Что-то посложнее…
5. Лучшие практики
6. Бонус

Расширения OAuth2 для API

RFC 6750, RFC 7519, RFC 7662, RFC 7636, OAuth2.0 Security best current practices, RFC 6819, RFC 7591, RFC 8628, RFC 9068, DPoP/MTLS и альтернативы будущего: OAuth 2.1 и GNAP

01

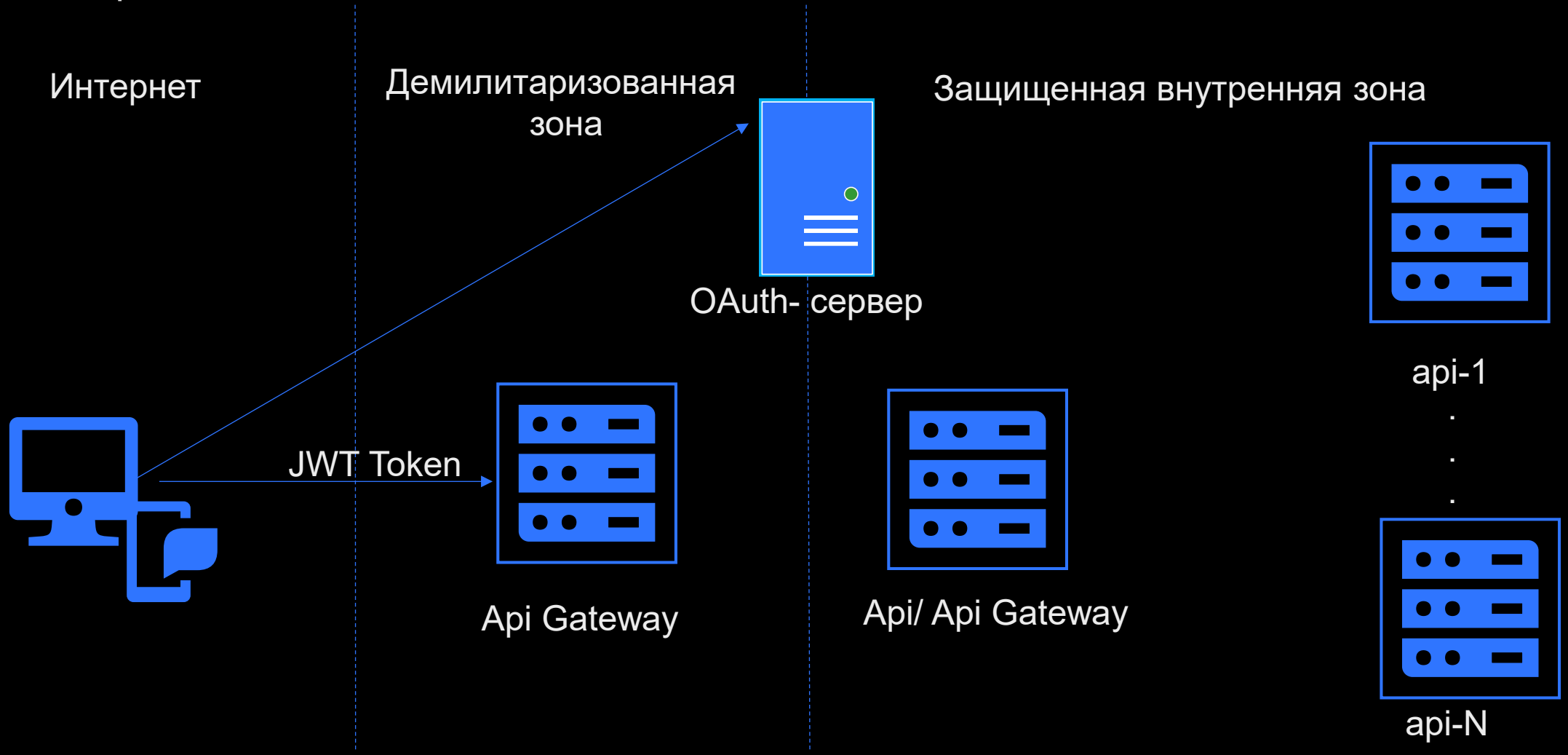
Token Exchange

02

FAPI 2.0

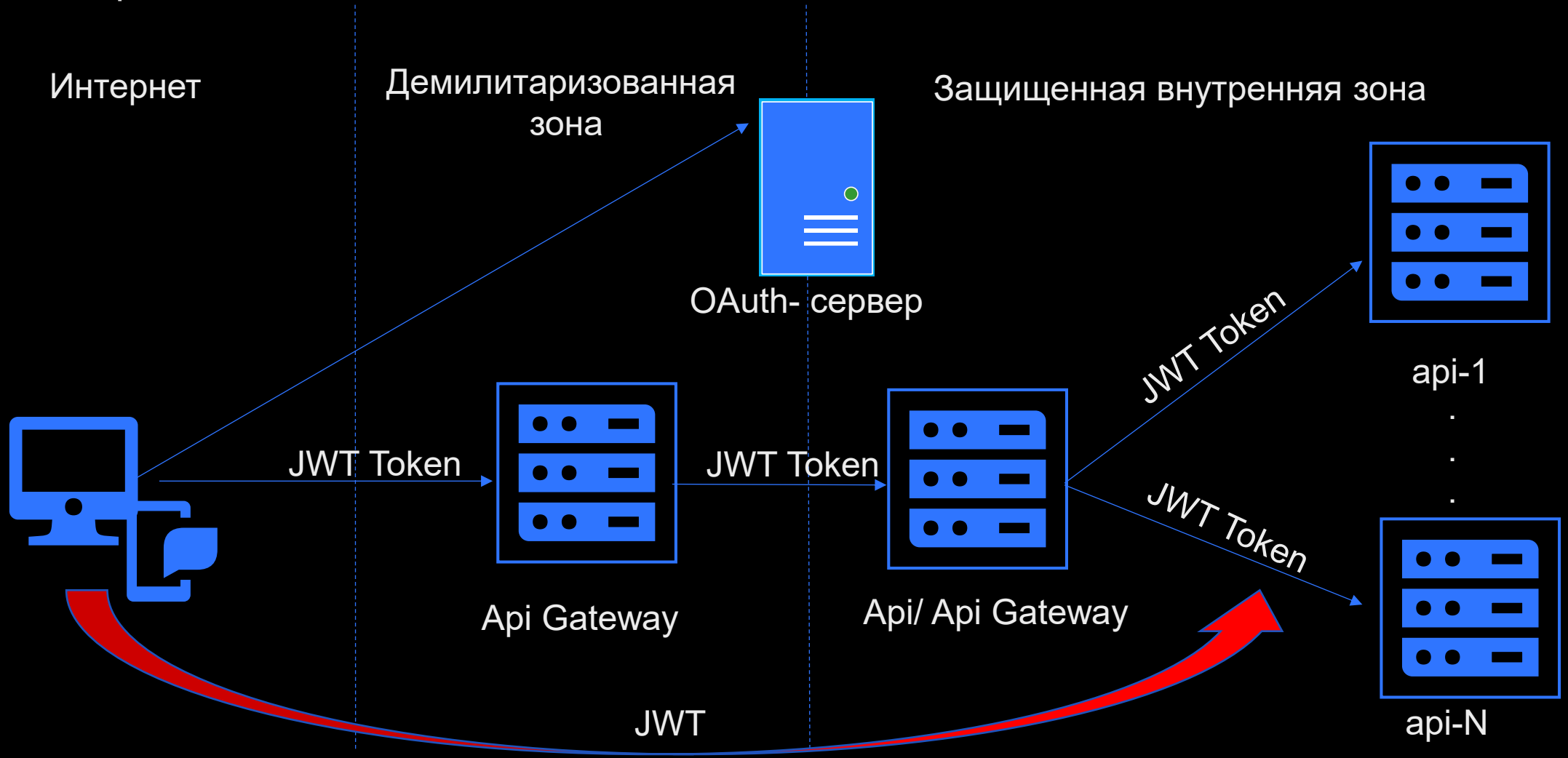
Token Exchange

Делегирование



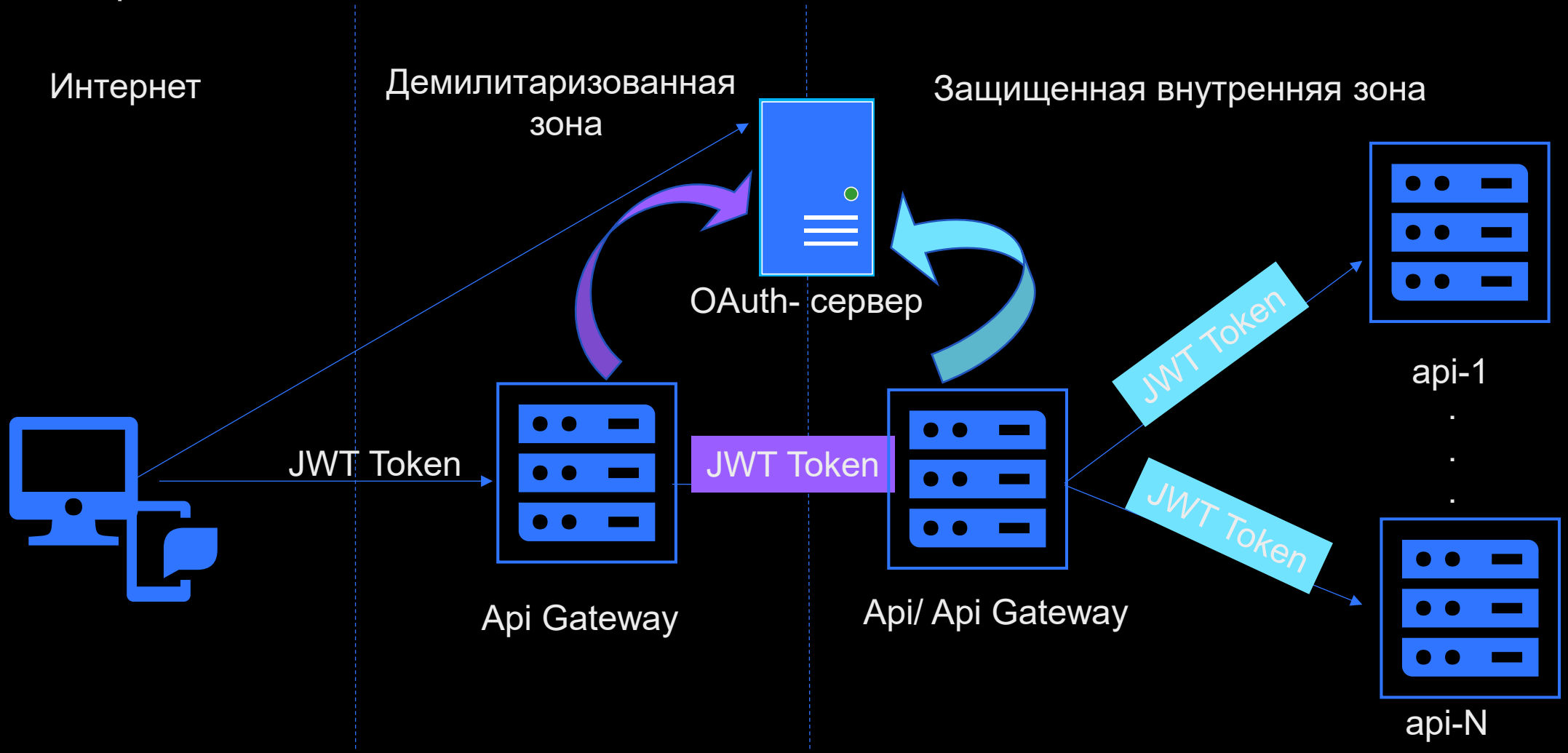
Token Exchange

Делегирование



Token Exchange

Делегирование



FAPI 2.0

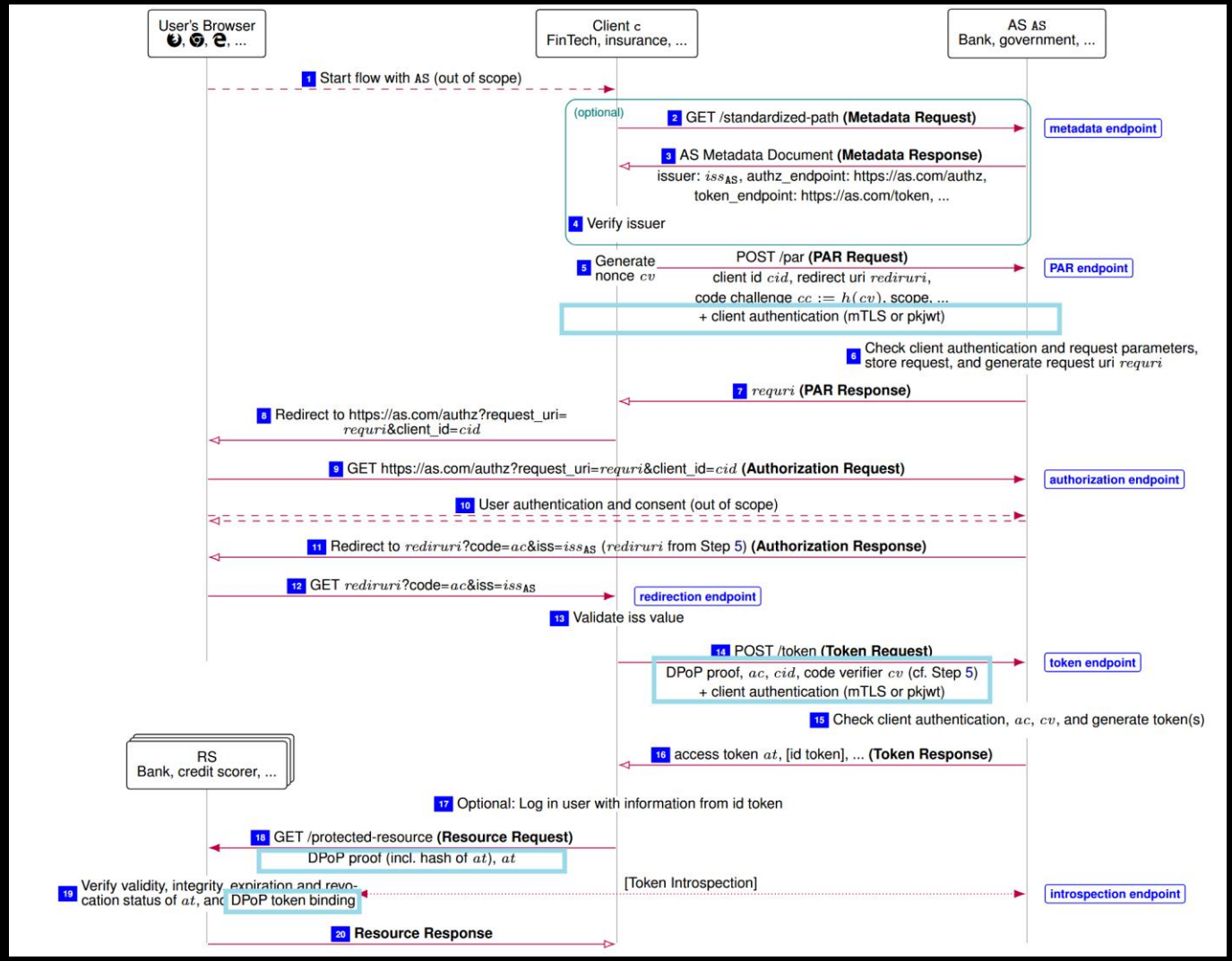
В здравоохранении, финансовой индустрии, электронном правительстве и т.д.

FAPI 2.0 Security Profile (Final)
FAPI 2.0 Attacker Model (Final)
FAPI 2.0 Message Signing (Draft)

FAPI 2.0

RFC 8705 - Mutual TLS Client Authentication and Certificate-Bound Access Tokens

RFC 9449 - DPoP: Demonstrating Proof-of-Possession at the Application Layer



О чем будем говорить?

1
Определения

2
Ключевые подходы к аутентификации

3
Распределение на практике

4
Что-то посложнее…

5
Лучшие практики

6
Бонус

Лучшие практики

- ✓ Внедрение управления API (API Management)
- ✓ Внедрение API Gateway как единой реперной точки
- ✓ Обеспечение управления версиями и документацией
- ✓ Предоставление метрик и видимости трафика
- ✓ Обеспечение масштабируемой безопасности API
- ✓ Учет изменений в стандартах

О чем будем говорить?

1
Определения

2
Ключевые подходы к аутентификации

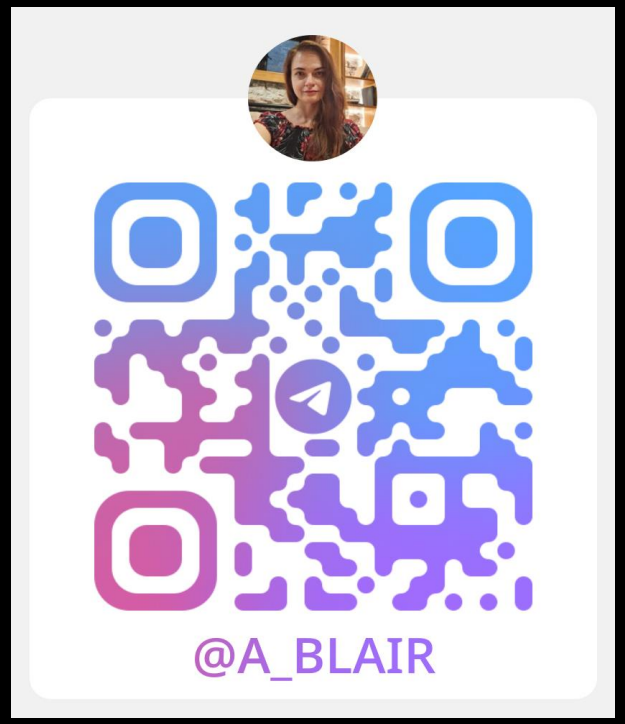
3
Распределение на практике

4
Что-то посложнее…

5
Лучшие практики

6
Бонус

Бонус



Ирина Блажина

Архитектор ИБ

@A_Blair

Чек-лист функционального тестирования защищенности API

Минутка рекламы

ГИД

О нас

Мы — молодая компания ГИД,
работаем над созданием нескольких продуктов
для внутреннего и внешнего рынков

ГИД – корпоративная экосистема, формирующая
цифровое пространство Группы Газпром

Газпром ID – универсальный идентификатор, позволяющий
авторизовываться в различных сервисах и площадках

Победитель Конкурса «Лучшие цифровые решения
для нефтегазовой отрасли 2023» в номинации «Лучшее
решение для обеспечения информационной безопасности»

ГИД

Спасибо за внимание!