

# Аутентификация, Авторизация, Аудит

## Общие положения

Основной задачи системы AAA/IAM является управление базой учетных записей пользователей, выдача разрешений и аудит доступа к ресурсам связанных с IAM подсистем.

Основные механизмы аутентификации базируются на принципах протокола Kerberos v5 с расширениями (Claims), применительно к системам веб аутентификации (jwt), включая возможности делегирования, пересылки токена, двусторонней аутентификации, запроса расширений авторизации по сервисному имени принципала (SPN).

Использование механизмов, завязанных на принципала, с использованием технологии электронных подписей совместимых со стандартом JWT позволяют проводить следующие способы аутентификации пользователя:

- Аутентификация по логину-паролю (ключевая пара)
- Сквозная аутентификация по сертификатам электронной подписи
- Аутентификация по одноразовому ключу (SMS, OTP)
- Аутентификация по оффлановому токenu (QR-код) без доступа к IAM
- Аутентификация по сохраненному токenu (Progressive Web Application, HTML5 Offline Application)
- Прокси-аутентификация со стороннего сервиса (OAuth2/SAML 2.0)

Общий формат записи токена аутентификации:

```
{
  "principal": "User Principal Name",
  "uid": "GUID",
  "displayName": "User Published Name",
  "groups": [...],
  "claims": [...],
  "principalSignature": "jwt digest/RSA|ECDSA 2048bit",
  "signature": "jwt digest/RSA|ECDSA 2048bit"
}
```

Поля *Groups*, *Claims* и *PrincipalSignature* могут отсутствовать. В качестве обязательного идентификатора пользователя выступают поля *Principal* и *UID*

## Архитектура

Архитектура сервиса IAM предполагает наличие модульного механизма работы с поддержкой горизонтального масштабирования. Сервис IAM состоит из нескольких независимых максштабируемых сервисов:

- **AAA** — Сервис аутентификации, авторизации и аудита. Отвечает за выдачу токенов, производных токенов (для каждого SPN) и запись событий доступа.
- **Profile** — Сервис управления профилем пользователя, хранит сведения о профиле пользователя, позволяет хранить ряд дополнительных данных, таких как связанные документы, изображения, дополнительные реквизиты и т.п.
- **Permission** — Сервис управления доступом. Управляет видами групп доступа для каждого сервиса и ролями доступными пользователю.

□

## Общая схема работы OAuth2 сервиса:

Сервер поддерживает как обязательные (базовые) механизмы OAuth2, так и расширенные (опциональные) механизмы аутентификации и делегирования токена. В качестве расширений механизмов аутентификации вводятся дополнительные сущности - *UserPrincipalName*, *OrganizationPrincipalName* и *ServicePrincipalName*, где UPN и OPN относятся к категории субъекта аутентификации, а SPN - к категории конечной точки аутентификации. OAuth2 токен (Bearer) формируется по стандарту JWT и может использоваться в оффлайн операциях в течение всего срока (времени жизни) такого токена.

При прохождении процедуры аутентификации в системе цифрового паспорта пользователь получает базовый цифровой ключ доступа в виде JWT токена, кодированного в Base64 для передачи по техническим каналам связи или в открытом виде для формирования оффлайн QR кода. Допускается использовать формирование QR кода на основе Base64 кодированного JWT токена, для поддержки данного требования рекомендуется использовать следующий алгоритм:

1. Попытка расшифровать JSON
2. Если расшифровать JSON не удастся (ошибка в 1 символе) - производится декодирование Base64 в строку
3. Осуществляется повторная попытка декодирования JSON
4. Проверяется корректность подписи JWT
5. Проверяется срок действия JWT

После того как базовый токен аутентификации получен, он может использоваться для доступа к различным сервисам, с минимальным уровнем гарантированных привилегий. В случае если сервис поддерживает механизмы работы оффлайн, он может содержать реплику групп безопасности сервиса для аутентификации пользователя. Для получения полного доступа к ресурсам после процедуры аутентификации производится:

1. Выбор роли пользователя в системе - присвоение UID или OID и расширенных атрибутов (расширенный JWT токен) - утверждений
2. Расширенная аутентификация в сервисе - получение SPN для запрашиваемого ресурса
3. Получение специального токена для запрашиваемого ресурса по его SPN

Общий набор полей всех JWT токенов является одинаковым, но для каждого типа токенов характерны выделенные специальные поля. Состав и форматы полей JWT токенов описаны ниже.

Набор функций сервиса зависит от совпадения набора требований и утверждений сервиса и JWT токена для доступа к тому или иному функционалу приложения. Любой полученный токен имеет свой срок действия, может быть обновлен в пределах окна обновления и содержит валидную (проверяемую) цифровую подпись системы цифрового паспорта АО НК. Любой токен может быть использован оффлайн для аутентификации пользователя, например для каждого сервиса может быть сгенерирован отдельный временный оффлайн токен доступа в виде QR кода. Стандартный период действия токена составляет 2 часа, базового токена - 8 часов. При необходимости может быть запрошен токен расширенного срока действия, но не более 168 часов (7 дней) с момента получения такого токена.

При делегировании токена нижестоящей системе, промежуточный узел может как передать токен в режиме "как есть" (прокси-токен) или получить на его основании новый SPN токен для конечного сервиса. В этом случае для получения нового SPN сервис обращается к системе цифрового паспорта за делегированием токена передавая:

- Токен пользователя (SPN JWT)
- Адрес конечного сервиса

Срок действия делегированного токена сервиса не должен превышать срок использования оригинального токена пользователя.

Возможность продления истекшего JWT токена не допускается, из такого токена могут быть получены основные реквизиты для запроса подтверждения (аутентификации) со стороны пользователя с целью выпуска нового JWT токена с теми же условиями (Владелец, Организация, Сервис).

---

🔄Версия #1

★Баталин Иван создал 2 апреля 2024 02:58:13

✍Баталин Иван обновил 2 апреля 2024 03:10:34