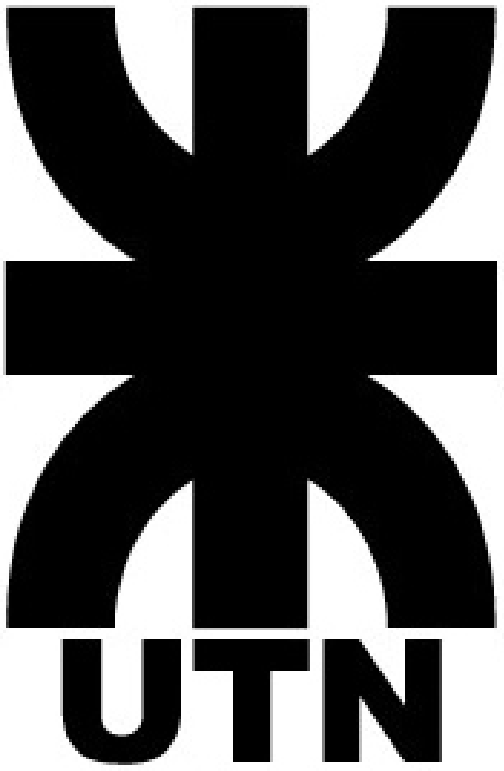
Actividad Semana 6

Token de Aplicación

UTN FRC - Integración de Aplicaciones en Entorno Web - 5K4



Cátedra: 5K4
Profesores:

- María Soledad Romero
- Rubén Aníbal Romero

Estudiante:

- 85828 Gutierrez, Santiago

Fecha: 22/09/2024

Índice

cURL para obtención del access token

```
curl --location 'token_url' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=my_client_id' \
--data-urlencode 'client_secret=my_client_secret' \
--data-urlencode 'grant_type=client_credentials'
```

Access token

Obtenido mediante el cURL


```
{
   "access_token": "access_token",
   "expires_in": 300,
   "refresh_expires_in": 0,
   "token_type": "Bearer",
   "not-before-policy": 0,
   "scope": "email profile"
}
```

Token desencriptado

Cabecera


```
{
 "alg": "RS256",
 "typ": "JWT",
 "kid": "key_id"
}
```


Payload


```
{
  "exp": 1726786528,
  "iat": 1726786228,
  "jti": "jti",
  "iss": "token_issuer",
  "aud": "account",
  "sub": "token_sub",
  "typ": "Bearer",
  "azp": "client_id",
  "acr": "1",
  "realm_access": {
    "roles": [
      “example_roles”
    ]
  },
  "resource_access": {
    "client_id": {
      "roles": [
        "example_roles"
      ]
    },
    "account": {
      "roles": [
        "example_roles"
      ]
    }
  },
  "scope": "email profile",
  "clientHost": "host_id",
  "email_verified": false,
  "clientId": "client_id",
```

```
  "preferred_username": "service-account-client_id",
  "clientAddress": "client_ip"
}
```

Firma digital

```
RSASHA256( base64UrlEncode(header) + "." +
        base64UrlEncode(payload),
        {
          "e": "AQAB",
          "kty": "RSA",
          "n":
        “4Aac0FqhJjDpumGvf69OPbbQMaXl4aRxT8dunkzK0H_nLWYVZ7Xe4
        uzarKatXVUcJpYLZO9_1boCiCtcR2aYnYKz9AHbu6_mX-vluCJEit85p
        KFPchCbnQM_w-PfVKn8jOeUT2wuxBM7sv5tGZ08KdB9C4aKkePH2
        Xy2EQvbpPafbrqInX-MnWo95lQ4uCLQgZgm80zf0p8YNXjx9v_9svNY
        DBrKh7L7H_TJgr6hzqRMnfXQzNuYZaQlfZoUNQD5Iz2qOT1sY5M8rJf
        Eg60RtyndwNSTBRwh48_xa55rhkJ-kG1hRlq5HevAMwe3gAdzW5Yk
        UAwOTcMd1TS-uAoWcw"
        }
)
```

Explicación de los claims del token

JSON Web Tokens (JWT) es un estándar abierto que se utiliza para compartir información de manera segura entre dos partes. Al estar firmada digitalmente, se garantiza la integridad y autenticidad de esta información.

Está compuesto por tres partes separadas por puntos:

- Cabecera
- Payload
- Firma

Debido a esto, la estructura general de un JWT es **xxxx.yyyy.zzzz**.

Claims de la cabecera

- alg: algoritmo de firma que se utiliza para firmar el token. En este caso se utiliza RS256. Este es RSA con SHA-256 (algoritmo asimétrico con claves pública y privada)
- typ: tipo de token.
- kid: id de llave. En entornos donde se utilizan varias llaves o llaves distintas, ayuda a identificar qué llave utilizar.

Claims del payload

Se dividen en claims registradas, públicas y privadas. Por un lado, las registradas son claims predefinidas que no son obligatorias pero se recomiendan, ya que proveen claims interoperables útiles. Por otro lado, las claims públicas pueden ser definidas a voluntad, pero para prevenir colisiones deberían estar definidas en el IANA JSON Web Token Registry o cómo una URI que contenga un espacio de nombre resistente a colisiones. Por último, las claims privadas son claims personalizadas para compartir información entre las partes que acuerdan utilizarlos.

- exp: Fecha de expiración
    - Valor: 1726786528
- iat: Fecha de emisión
    - Valor: 1726786228
- jti: Identificador único del token
    - Valor: token_id
- iss: Emisor del token
    - Valor: url-emisor-token
- aud: Audiencia a la que está dirigido el token
    - Valor: account
- sub: Sujeto del token
    - Valor: token_sub
- typ: Tipo del token
    - Valor: Bearer
- azp: Parte autorizada
    - Valor: client_id
- acr: Contexto de autenticación
    - Valor: 1
- realm_access: Acceso al ámbito
    - Roles
        - roles
- resource_access: Acceso a recursos
    - client_id
        - Roles
            - example_roles
    - account
        - Roles
            - example_roles
- scope: Alcance de permisos
    - Valor: email profile
- clientHost: Dirección IP del cliente
    - Valor: client_ip

- email_verified: Verificación de correo electrónico
    - Valor: false
- clientId: Identificador del cliente
    - Valor: client_id
- preferred_username: Nombre de usuario preferido
    - Valor: service-account-client_id
- clientAddress: Dirección IP del cliente
    - Valor: example_ip

Firma digital

Indica el proceso de firma del token. RSASHA256 indica el algoritmo de firma utilizado. Luego, indica que se concatena con un punto de por medio el contenido de la cabecera y el payload en Base64Url. Por último, se agrega el resultado de la firma de esta concatenación (“cabecera.payload”), utilizando la clave privada del emisor.

Bibliografía

JWT.io. (s.f.). *Introduction to JSON Web Tokens*. https://jwt.io/introduction

Johnson, W. (2022, mayo 4). *RS256 vs HS256: What's The Difference?* Auth0. https://auth0.com/blog/rs256-vs-hs256-whats-the-difference/