Web applicatie Security

Inhoud

Wat is een API?

API staat voor ***Application Programming Interface***. Een interface is een koppeling tussen verschillende softwarepakketten, gericht op het uitwisselen van gegevens. Uitwisselen betekent: gegevens aanmaken, gegevens uitlezen, gegevens updaten of gegevens verwijderen. De API definieert de functionaliteit van deze programma's, waardoor de buitenwereld de programma's kan gebruiken zonder veel details te kennen van de programma's.

Wat is een webservice?

Een webservice faciliteert net als een API verkeer tussen pakketten, waar een API meer als een echte koppeling kan worden gezien. Het is dus ook een manier om gegevens uit te wisselen tussen verschillende softwarepakketten (zie API). Het verschil is dat 'het envelopje met gegevens' bij een webservice vaak meer gegevens bevat dan bij het envelopje van een API. Het streven om zo efficiënt mogelijk om te gaan met de gegevens die worden uitgewisseld. Het wordt vooral gedreven door de ontwikkeling van apps die op mobiele apparaten (telefoons, tablets) draaien.

Wat is webservice authentication?

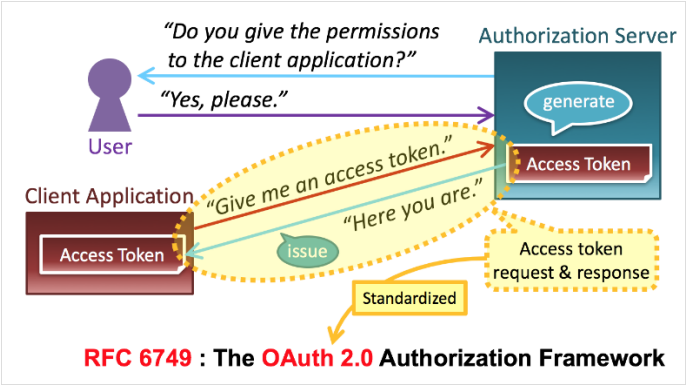
Om van een webservice gebruik te kunnen maken is een identificerende sleutel (API-key) nodig. Een "webservice key" is eigenlijk een wachtwoord (die je voor een koppelgebruiker op oneindige houdbaarheid instelt).

Wat is OAuth?

OAuth (***Open Authorization***) is een open standaard voor **autorisatie**. Gebruikers kunnen hiermee een programma of website toegang geven tot hun (privé)gegevens zoals die zijn opgeslagen op een ander systeem, zonder hun gebruikersnaam en wachtwoord uit handen te geven.

OAuth 2.0 maakt gebruik van tokens. Elk token geeft slechts toegang tot specifieke gegevens van één website voor een bepaalde duur. Zo kan ingesteld worden dat een bepaald programma slechts een jaar toegang heeft tot de gegevens. Na deze periode kan opnieuw toegang worden gevraagd.

Met OAuth kunnen wij derden veilig toegang geven tot het gebruik van bijvoorbeeld onze web API. Dit gebeurt niet via inloggen maar via een access stoken die de derde partij (beperkt) toegang geeft tot onze applicatie. Dit token bevat allerlei informatie over de aanvrager en kan dus ook rechten en claims bevatten. Het betreft dus een beperkte toegang.



schematische weergave over hoe OAuth 2.0 werkt. Bron: ***artikel***

Wat is OpenID Connect (OIDC)?

OpenID Connect is een laag bovenop OAuth 2.0 die voor **authenticatie** zorgt**. OpenID Connect gaat er voor zorgen dat een client de** identity **van een gebruiker kan** verifiëren **door naast een access token ook een identity token terug te geven. Met een client wordt een applicatie bedoeld die toegang probeert te krijgen tot een beschermde resource in naam van een gebruiker. In de Identity token is profielinformatie aanwezig van de gebruiker.**

Wat is OpenID

(Niet te verwarren met OpenID Connect)

OpenID **is een gedecentraliseerd authenticatie systeem voor het internet. Het doel van het** OpenID**-initiatief is gebruikers in staat te stellen op websites met één ID in te loggen in plaats van meerdere unieke accounts aan te maken. Voor het gebruik van** OpenID **moet een gebruiker zich eerst registreren op een website die** OpenID **ondersteunt.** Bij het bezoeken van andere sites die OpenID ondersteunen, kan de gebruiker inloggen met een **URL**

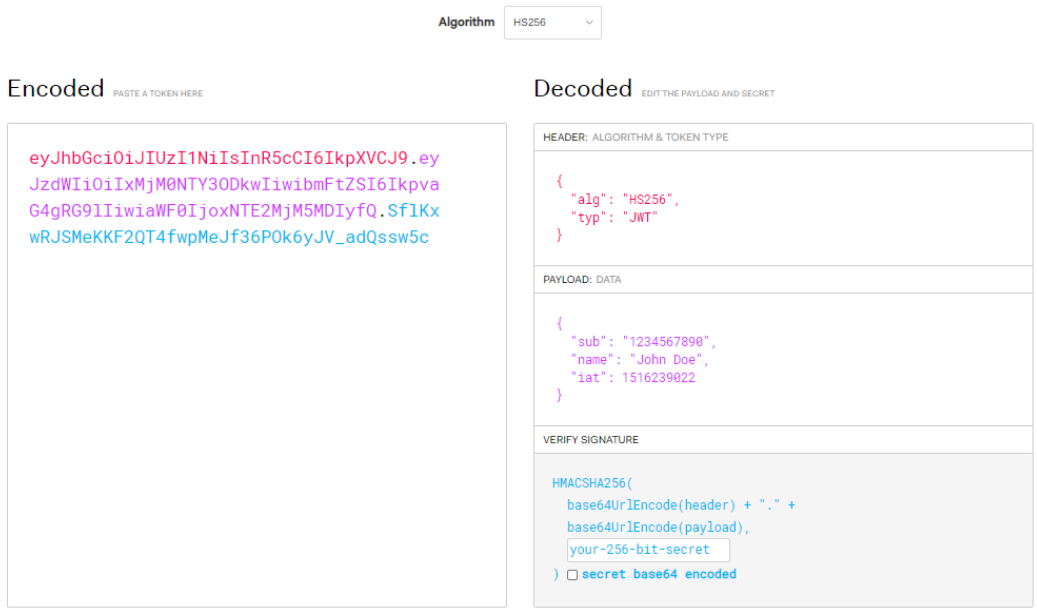
Wat is IdentityServer

IdentityServer is een **OpenID Connect** en **OAuth 2.0 framework**. OAuth is een **token based** standaard voor autorisatie. De OAuth token wordt een **access token** genoemd. Indien je in het bezit bent van een geldig access token kan je toegang krijgen tot een beschermde resource (API). De token gaat geen info bevatten over de user, het is enkel een 'sleutel' tot de API.

Het grote voordeel **om een autorisatieserver zoals IdentityServer te gebruiken, is dat de** authenticatie op één plaats zal gebeuren **en er dus** single sign-on **is. Verder kan IdentityServer gebruik maken van verschillende** identity providers**. Er kan ingelogd worden met users en paswoorden die we in een lokale database bijhouden, maar er kan standaard ook gebruik gemaakt worden van** Active Directory **en** social providers **zoals Google, Facebook en Twitter.**

Wat is een JWT Access Token?

Een access token wordt als een **JSON Web Token** (JWT) voorgesteld en wordt **base64 geëncodeerd**. Een token bevat ook altijd een handtekening van de autorisatieserver zodat een API kan controleren of het een geldige token is. Hiervoor heeft het de **public key** nodig van de autorisatieserver, die via een OpenID endpoint kan opgevraagd worden.
Via de website https://jwt.io/ kan je een **JWT** access token decoderen:



Een token bestaat uit volgende 3 delen:

- **Header**: info over de encryptie zodat men weet hoe de token te verifiëren.
- **Payload (claims)**:
    - Issuer
    - Audience: de resource server (API) waarvoor het token bedoeld is
    - Not before: geeft aan vanaf wanneer de token geldig is
    - Expiry: geeft aan hoe lang de token geldig is
    - Client id: id van de applicatie die de beschermde resource wil aanspreken
    - Scopes:
        - Identity Scopes: deze bepalen welke user informatie er kan opgevraagd worden met deze access token
        - Resource scopes: gebruikt om access te limiteren, bv. 'read' scope zou enkel reads toelaten op API
    - Custom data

Handtekening

Voorbeeld van een ID token:


```
{
"aud": "testapp",
"sub": "32679f2c76dc20a73a1b51e72d3cc85ccc90937a",
"nbf": 1559130785,
"iss": "https://oidcng.test2.surfconext.nl",
"exp": 1559155985,
"iat": 1559130785,
"nonce": "WfnzwjIW4Wd9EhMBkGRpbqDWSIwVcXgfY2uvC2wx7OA",
"jti": "0110a8d8-c96c-40b5-b674-a337a62275ea"
}
```


Het ID token bevat veel informatie:

- aud: *audience*, de applicatie waaraan het token is uitgedeeld.
- sub: s*ubject*, de zogenaamde *identifier* van de gebruiker; een unieke reeks cijfers en letters waarmee iedere gebruiker uniek wordt geïdentificeerd.
- nbf: *not before*, dit token is niet geldig voor deze datum.
- iss: *issuer*, de partij die het token heeft uitgegeven.
- exp: *expiry*, dit token is geldig tot uiterlijk dit tijdstip. Het formaat is een **Unix timestamp.**
- iat: *issued at*, het tijdstip waarop dit token is uitgegeven.
- nonce: een *nonce* is eenmalig wachtwoord, bedoeld om de ervoor te zorgen dat de twee verzoeken die de RP moet doen tijdens het login proces met elkaar te verbinden. De RP kan hiermee verifiëren dat het uitgegeven ID token behoort bij het oorspronkelijke loginverzoek.
- jti: een unieke identifier voor het token.

Claims

Claims bevatten extra informatie over een gebruiker. Een Claim kan elk soort gegeven zijn over een geauthenticeerde gebruiker. Bv de email-adres,naam, geslacht, rol (bv Admin),…

Referenties

https://darutk.medium.com/the-simplest-guide-to-oauth-2-0-8c71bd9a15bb

https://en.wikipedia.org/wiki/OpenID#OpenID_vs._pseudo-authentication_using_OAuth

https://en.wikipedia.org/wiki/OpenID_Connect

https://en.wikipedia.org/wiki/OAuth

https://jwt.io/