API koppelvlak eisen

Voor de uitwisseling van gegevens stelt de leverancier bij voorkeur een REST API of anders een SOAP API beschikbaar met de volgende kenmerken:

API URL:

1. De API heeft een vaste URL welke is opgenomen in het DNS van de leverancier. Naast een productie URL is er ook altijd minimaal een Acceptatie of Staging versie beschikbaar, welke op een ander (sub)domein staat. Deze is nooit aangesloten op de live dataset en heeft een ander IP adres.

   Productie: *https://api.voorbeeldplatform.nl* of *https://voorbeeldplatform/api*
   Acceptatie: *https://**acc**.api.voorbeeldplatform.nl* of *https://**acc**.voorbeeldplatform.nl/api*

2. Het major versienummer van de API vormt bij voorkeur onderdeel van de URL, waarbij een 'breaking change' in het schema van de API altijd een wijziging van het major versienummer tot gevolg heeft.

   *https://api.voorbeeldplatform.nl/**v1**/ of https://voorbeeldplatform/api/**v1**/*

3. Parameters worden toegevoegd als querystringparameters, niet als bookmarks

   *https://api.voorbeeldplatform.nl**?parameter1=waarde&paremeter2=waarde2***

Beveiliging

1. De API moet voorzien zijn van authenticatie als deze informatie bevat die niet openbaar is. Gebruik hierbij bij voorkeur OAUth 2.0 bearer token of JWT, maar geen basic authenticatie. Als gebruik wordt gemaakt van een API key, plaats deze dan in de authortization header en niet in de querystring.
2. De API is uitsluitend bereikbaar via SSL (HTTPS) op poort 443. De leverancier maakt hierbij gebruik van een SSL certificaat (minimaal TLS versie 1.2) welke geregistreerd is bij een officiële Certificate Authority. Self signed certificaten zijn niet toegestaan.
3. IP locking is alleen toegestaan tussen services, dus nooit naar een client en nooit als vervanger van authenticatie of SSL
4. Er is logging van aangeroepen API's welke op productie op loglevel 'ERR' staat. Deze logging bevat het origin IP en de aangeroepen service, maar geen gevoelige (persoons)gegevens. Alleen in debug modus mag de gehele call worden gelogd. Debug modus wordt alleen bij zeer hoge exceptie, en na expliciete goedkeuring van Opdrachtgever tijdelijk gebruikt op de productie omgeving, nadat gebleken is dat dit op de test en/of acceptatie omgeving niet bruikbare informatie op heeft geleverd om een acuut en zeer ernstige verstoring op te kunnen lossen.

Inhoudelijk

1. De REST API gebruikt JSON als standaardformaat voor een respons
2. Indien een object niet beschikbaar is maar verplicht terug te geven is volgens het domein, heeft het de waarde null.
3. Indien een lijst van objecten niet beschikbaar is en verplicht terug te geven is volgens het domein, wordt een lege lijst verwacht in JSON notatie '[]'
4. De datum- en tijdsnotatie volgen het ISO8601-formaat inclusief de tijdszone -indicatie
5. Gebruik bij voorkeur camelCase voor attributtnamen.
6. Maak gebruik van de standaard HTTP Statuscodes.
7. Standaarderrors zijn het gevolg van technische, systeem- of softwareproblemen. Deze worden weergegeven met de overeenkomstige HTTP errorcode
8. Validatie-errors zijn het gevolg van een businessevaluatie van de payload meegegeven in voorafgaande API-interactie. Naast de http errorcode bevat de response payload daarom een duidelijke aanwijzing welke validatie waarom heeft gefaald.

Documentatie

De actuele documentatie van de API is beschikbaar op basis van de swagger/open-api definition (voor Rest API's) of het XML schema (voor SOAP API's)