Memo

Aan
Bob van der Staat, Erik de Rooij, Geri Wolters, Jeroen Graave, Werner Kramer.
cc: overige DD-Werkgroepleden

Datum	**Kenmerk**	**Aantal pagina's**
5 november 2019	11203680-DSC-25-v0.9	2
Van	**Doorkiesnummer**	**E-mail**
Stef Hummel	+31(0)6 1019 8112	Stef.Hummel@deltares.nl

Onderwerp
Bespreekverslag CORS-headers in de DD-API, sessie 31 oktober, web conference

---

Aanwezig:
- zie '**Aan**' en '**Van**'

Voorstelrondje

Vanwege twee nieuwe gezichten, of beter gezegd: stemmen, (Jeroen en Werner) stelt een ieder zich kort voor.

Discussie over CORS-headers

Er volgt een uitgebreide discussie over o.a.:
- Wanneer CORS-headers nodig zijn
  (Zulks ook in relatie tot het al of niet geauthentiseerd een request doen)
- Welke types CORS-headers en -mechanismen er zijn
- Of het ondersteunen van CORS-headers tot beveiligingsrisico's leidt
- … et cetera …

Conclusie

Uit de discussie komt onderstaande door alle partijen onderschreven conclusie naar voren:

Een DD-node moet, zolang het bevragen van DD-nodes nog niet onder OpenID-Connect identificatie gebeurt, de volgende CORS-verzoeken ondersteunen:
- Simple requests
- Preflight requests met Access-Control-Allow-Origin header, waarbij in de DD-node een lijst aanwezig is met url's van waaruit browsers data moeten opvragen.

Afgesproken wordt dat Bob kort beschrijft wat de opties bij het gebruik van CORS zijn en waarom bovenstaande opties op dit moment de meest logische zijn.
Dat heeft hij meteen na de vergadering gedaan; zie volgende pagina.

Afwegingen CORS

Cross-Origin Resource Sharing (CORS) is een mechanisme dat gebruikt wordt in moderne browsers om te bepalen of een webapplicatie (vanuit de front-end) een verzoek mag uitvoeren naar een specifieke end point. Deze verzoeken worden altijd uitgevoerd indien het gaat om een verzoek dat buiten het eigen domein valt. Bijvoorbeeld:

domein-a.com doet verzoek naar domein -b.

Er zijn twee soorten CORS verzoeken die plaats kunnen vinden.

Simple Request:
Deze wordt uitgevoerd mits er aan bepaalde voorwaarden wordt voldaan, zoals dat het alleen gaat om andere de GET HEAD POST methods, en om bepaalde content-Types: (voor volledig overzicht zie https://developer.mozilla.org/nl/docs/Web/HTTP/CORS)

Preflight Request:
Indien niet aan deze voorwaarden wordt voldaan zal er een **Preflight request** worden uitgevoerd. Dit is een verzoek dat de browser van te voren stuurt naar de server om na te gaan of het verzoek in kwestie “legaal” is bij de server. Hiervoor moet de Server in kwestie de OPTIONS-header ondersteunen omdat dit altijd wordt meegegeven als de HTTP method in een preflight verzoek.

Er zijn verschillende headers die geset kunnen worden voor CORS:
Access-Control-Allow-Origin: Geeft aan welke url’s bij de aangeven server (via de browser) mogen komen. Vroeger kon hier een wildcard worden gespecificeerd om aan te geven dat elke url goed gekeurd was. In Firefox en Chrome is het nu niet meer toegestaan om een wildcard (*) te gebruiken indien er spraken is van Authenticatie. Dus indien er verzoeken gedaan worden via de front-end moet deze of:

- Dynamisch worden toegevoegd aan de allow-origin header, of
- Van tevoren moet er een lijst samen worden gesteld waarin staat welke urls toegestaan zijn via de browser, of
- de verzoeken moeten altijd via een backend worden gestuurd.

Access-Control-Allow-Methods: Hierin specificeren welke HTTP methods allowed zijn: (GET, POST, OPTIONS in iedergeval)
Access-control-Allow-Headers: Aangeven welke custom headers worden toegestaan.

Voor de Digitale Delta zou bij de start een lijst bijgehouden moeten worden welke url’s (naast het eigen domein) bij de knopen en Identity Providers mogen komen om verzoeken bij deze servers te mogen uitvoeren. Deze lijst moet dan in ieder geval door de knopen en IDP worden gebruikt om verzoeken via de front-end te accepteren.

Als slotpunt nog even de side note dat CORS dus een implementatie is voor browsers. Het biedt geen garantie voor enige veiligheid, omdat indien verzoeken worden gedaan via een backend, deze verzoeken niet via de browser worden gedaan en dus worden omzeild.