To: 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e)
Sent: Sun 1/17/2021 6:59:59 PM
Subject: FW: Uitslagen verkrijgen zonder effort aan de GGD kant
Received: Sun 1/17/2021 7:00:00 PM

Kijk... we kunnen het ook zonder centrale database bij de GGD.... Mijn idee van volledig decentraal zou dus kunnen werken... maken we geen ingewikkeld afsprakenstelsel, maar wel aansluitspecs voor toegangstesten BV en evt anderen. Als we verbinding secure maken met certificaten etc. hebben we trust over de afzender.

Van: 5.1.2e <5.1.2e @webweaving.org>
Verzonden: zaterdag 16 januari 2021 11:36
Aan: 5.1.2e <5.1.2e 5.1.2e
CC: 5.1.2e) <5.1.2e @minvws.nl>; 5.1.2e <5.1.2e @gmail.com>
Onderwerp: Re: Uitslagen verkrijgen zonder effort aan de GGD kant

Mooi. Dus dit is geheel veilig te doen - en uitstekend verhaal waarom dit minstens zo goed is als bestaande oplossing - en in feite op 2-3 punten beter.

5.1.2e

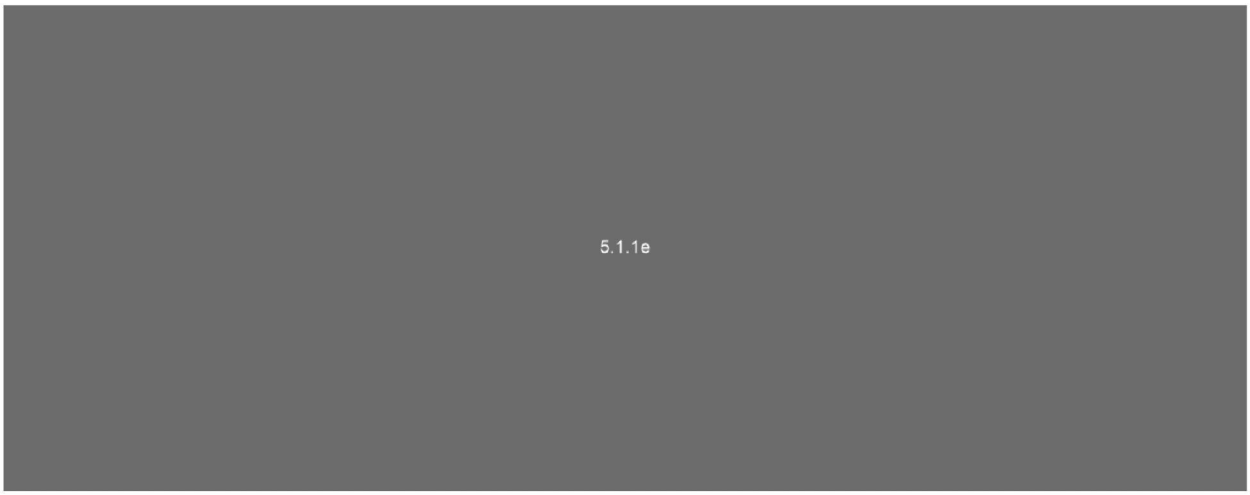
On 16 Jan 2021, at 11:23, 5.1.2e <5.1.2e 5.1.2e wrote:

Hoi,

Ik heb op verzoek van 5.1.2e even gekeken hoe eenvoudig het is om de bestaande coronatest website te gebruiken om uitslagen op te halen, zodat we een testbewijs zouden kunnen maken zonder dat dit de GGD of topicus veel effort kost.

TL;DR: het kan.

Het bleek zelfs super eenvoudig, er zit niet eens een referer/csrf check o.i.d. op, ik kon de api achter de site met minimale effort benaderen:



Dit is zowel mijn testuitslag uit juni (hmm, is er grond die zo lang te bewaren?) als die uit november. (Interessant: het afspraak id zit erbij dus mochten we ooit toch de afspraken route gaan volgen dan kunnen we de juiste uitslag bij de desbetreffende afspraak matchen.)

Het oauth bearer token kreeg ik direct na de digid authenticatie. Het bleef ca 5 minuten geldig, daarna kreeg ik met hetzelfde token een lege array als response. (Dit gedrag is er op de site ook, hij logt je welliswaar niet

uit, maar na 5 minuten toont hij 'We vinden geen testuitslag'). Het bsn zelf hoeft dus niet over de lijn, het oauth token is voldoende.

Ik heb gecheckt of het token device/ip gebonden is. Dat is NIET het geval. Ik kon eenvoudig eerst via digid inloggen, vervolgens het bearer token kopiëren naar een ander device met een ander ip (via 4g) en de api call werkt daar direct. (Laat het 5.1.2e maar niet horen). Dat wil zeggen dat we de call zowel rechtstreeks uit de app zouden kunnen doen, of proxyen via de coronatester backend als we willen.

Er zit een PKI-O certificaat op de API dus we kunnen ook SSL pinnen als we de call direct vanuit de app doen, zodat iemand niet met een man in the middle attack een negatieve uitslag kan genereren.

De vraag is nog even of er iets bijzonders gebeurt met het bearer token, of dat we hier rechtstreeks het bearer token kunnen gebruiken dat we van identity hub krijgen zodra we zelf een digid koppeling hebben. Ik vermoed dat er niets geavanceerds op zit. En zou dat toch het geval zijn, dan zal het in ieder geval beperkte effort aan de ggd kant zijn om deze API voor ons toegankelijk te maken.

Mvg,

5.1.2e