Memo

Aan
Bob van der Staak, Erik de Rooij, Geri Wolters, Remco Gerlich
(cc Flip Dirksen)

Datum	**Kenmerk**	**Aantal pagina's**
7 augustus 2018	11202186-000-DSC-0025	2

Van	**Doorkiesnummer**	**E-mail**
Stef Hummel	+31(0)6 1019 8112	Stef.Hummel@deltares.nl

Onderwerp
Verslag web conference Digitale Delta Authenticatie aanpak

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

Bespreking document "*OpenID Connect explained-bobvdstaak*"

Zoals besproken tijdens het vorige overleg (8 juni, zie verslag 11202186-000-DSC-0019-DD-Authenticatie-20180608-def) heeft Bob een document opgesteld waarin beschreven wordt hoe binnen de Digitale Delta gebruikers-authenticatie plaatsvindt. Dit gebeurt op basis van OAuth2 en OpenID Connect. Tijdens de vergadering wordt het document doorgenomen. Het voorliggend verslag bevat de daarbij naar voren gekomen opmerkingen over en aanvullingen op het document.

Erik

Er staat dat *Implicit Flow* niet ondersteund wordt. Waarom is dat?
Blijkt een misinterpretatie te zijn; Bob dacht dat de wens ooit geuit was om dit niet supporten.
Conclusie: *Implicit Flow* hoeft niet te worden uitgesloten.

Remco

Was in eerste instantie wat verward door het voorkomen van het woord *authorisatie*, terwijl het document over *authenticatie* gaat. Later werd duidelijk dat over het bij *authorisatie* gaat over profiel dat de Authentication Provider meegeeft. Dit zou wat duidelijker kunnen worden weergegeven. En zo zijn er wat meer dingen die voor iemand die het voor het eerst wat helderder beschreven kunnen worden, b.v. ook in sommige gevallen bij de verwijzing in de tekst naar een figuur.
Remco heeft hier aantekeningen van gemaakt. Hij stuurt die naar Stef, die vervolgens –zijnde ook een zo goed als verse lezer - een edit-slag doet.

Inhoudelijke vraag. Wel onderdeel vormt de unieke identificatie?

- iss + sub?
- e-mail adres?

In principe is iemand's e-mail uniek, dus dat moeten we gebruiken. Wel kan het gebeuren dat iemand zich bij twee issuers (Authentication Providers) aanmeldt met hetzelfde e-mail-adres, maar op zich is dat niet erg. Wel is het van belang dat de DD Authentication Providers garanderen dat:

- bij=nnen zijn systeem het e-mail-adres van een zich aanmeldende gebruiker uniek is
- het e-mail adres gevalideerd is

We gaan deze eisen aan het document toevoegen.

Het e-mail-adres is dus wat de gebruiker van de DD uniek maakt. De vraag is vervolgens of iemand die via twee verschillende Authentication Providers binnenkomt dan ook verschillende dingen mag. Zou in principe moeten kunnen, en zou misschien zelfs handig kunnen zijn. Wordt t.z.t bij authorisatie (als we dat centraal gaan regelen) nader besproken.

Geri

Geen aanvullingen op het eerder besprokene.

Stef

Vindt dat er geen bestaande user-ids en wachtwoorden in het document mogen staat. We zouden de test-setup weg kunnen laten, maar die is juist zeer informatief. Besloten wordt hem erin te laten, maar hem te anonimiseren. Stef zal deze slag doen.

Acties / Planning

Remco:
- Aantekening m.b.t. verbetering van de leesbaarheid naar Stef

Stef:
- inhoudelijke aanpassing n.a.v. meeting
- tekstuele slag na opmerkingen van Remco.
- test-setup anonymiseringsslag, waar nodig met support van de anderen
- uiterlijk 1 september nieuwe versie
- datumprikker voor de week erop om over die versie te praten