To: 5.1.2e [5.1.2e@cwi.nl]
Cc: 5.1.2e 5.1.2e @minvws.nl]; 5.1.2e @umcutrecht.nl[5.1.2e @umcutrecht.nl]
From: 5.1.2e
Sent: Thur 9/17/2020 11:37:14 AM
Subject: 'Meldcode' voor coronamelder notificaties
Received: Thur 9/17/2020 11:37:30 AM
GACT-VF.pdf

Hoi 5.1.2e,
5.1.2e heeft me gevraagd om even contact met je te zoeken m.b.t. de 'meldcode' om na een notificatie een test aan te vragen met iets meer zekerheid dat de aanvrager een melding heeft gehad, zoals je ook aan 5.1.2e gestuurd had.

De DP-3T manier is een elegante, en zouden we in CoronaMelder kunnen toepassen. Een belangrijke kanttekening is echter dat het, zoals DP-3T aangeeft, geen waterdichte code is. Omdat onze app open source is en er geen 'secrets' in zitten is het lastig dit op zo'n manier te doen dat het niet heel makkelijk na te maken is. Iemand zou een site kunnen maken die geldige meldcodes produceert.

We hebben in mei overigens een voorstel naar Apple en Google gestuurd om het protocol uit te breiden met 'validated feedback', een cryptografisch wél waterdichte manier om te valideren dat je een notificatie hebt gehad, zonder de privacy aan te tasten. Dit voorstel heb ik in de bijlage bijgevoegd. 5.1.2h

Laten we voor nu even uitgaan van een meldcode zoals bij DP-3T. Waar we dan rekening mee moeten houden zijn een aantal dingen:

1) Het proces van aanmelden voor een test moet aangepast worden, die medewerkers moeten een site krijgen waar ze meldcodes kunnen valideren/opzoeken die ze te horen krijgen, en het moet ergens geregistreerd worden (anders heb je er voor de statistiek niets aan).

2) Onze product owners vermoeden dat een meldcode een erg lage drempel is, omdat als je een notificatie wil veinzen maar geen meldcode hebt, je ook gewoon kunt zeggen dat je klachten hebt, dus zij twijfelen of je er daadwerkelijk een drempel mee creeeert.

3) 5.1.2h
5.1.2h En daar zou dan aktie op moeten worden genomen (op welke juridische basis?) - dit is ook wat DP-3T in hun voorstel suggereert.

4) 5.1.2h
5.1.2h

Als we denken dat, ondanks deze kanttekeningen, dit een nuttige route is, dan kan ik hem bij het development team neerleggen en vragen of ze dit gaan inbouwen (op de DP-3T manier).

Hoe denken jullie over bovenstaande kanttekeningen?

(Overigens stelt DP-3T voor om de datum van notificatie mee te nemen in de berekening van de meldcode, ik zie daar niet zoveel meerwaarde in, qua security, want een fake meldcode generator kan dezelfde teks van het cdn downloaden en elke datum in de afgelopen 14 dagen gebruiken om een geldige meldcode te genereren - wellicht is het dan drempelverlagend als de user die datum niet ook hoeft op te geven).

Mvg,
5.1.2e

--
5.1.2e
5.1.2e
5.1.2e
5.1.2e@egeniq.com
www.egeniq.com

5.1.2e