To: (10)(2e), (10)(2e), (10)(2e) (10)(2e) @minvws.nl]; (10)(2e), (10)(2e), ((10)(2e))[(10)(2e) @minvws.nl]
From: (10)(2e), (10)(2e), (10)(2e) ((10)(2e))
Sent: Wed 5/27/2020 7:51:12 AM
Subject: FW: To UZI or not to UZI
Received: Wed 5/27/2020 7:51:13 AM

Hier de mailwisseling over UZI. Mail 2 van 2 .

Van: (10)(2e), . ((10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 27 mei 2020 09:38
Aan: (10)(2e), (10)(2e) . (10)(2e) ((10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: FW: To UZI or not to UZI

FYI

Met vriendelijke groet,

(10)(2e)

Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Parnassusplein 5 | 2511 VX | Den Haag (8ste etage)
Postbus 20350 | 2500 EJ | Den Haag

(10)(2e)

Tel: +31 (10)(2e) | e-mail: (10)(2e) @minvws.nl

Van: (10)(2e) ((10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: woensdag 27 mei 2020 09:23
Aan: (10)(2e), . ((10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: To UZI or not to UZI

Dank.

Even iets over punt 1: Het is van belang om een onderscheid te maken tussen het ontwerp van de app (waarin de GGD rondom het testen van mensen een rol speelt in relatie tot het publiceren van keys van positief geteste personen) en het gebruik van een middel (UZI-stelsel). Het gebruik van UZI-stelsel an sich is juist bedoeld als beschermingsmiddel! We hebben een zekere vorm van toegang nodig tot gevoelige informatie, en we gebruiken het UZI-stelsel. Dit staat kort toegelicht in het PvE (§4.2): "Om misbruik te voorkomen kan het melden van een positief testresultaat alleen plaatsvinden na autorisatie van een aangewezen instantie."

Ik stuur je mail ook even door aan mijn contact bij CIBG die hier eerder bij betrokken was.

Groeten,
(10)(2e)

---

(10)(2e): (10)(2e), . ((10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: dinsdag 26 mei 2020 23:34
Aan: (10)(2e) ((10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: FW: To UZI or not to UZI

Hi (10)(2e)

Ik bedacht me net dat het me ontschoten was om jou in de onderstaande mailconversatie mee te nemen. Excuus voor het ongemak.

Ik zal je in vervolg in deze mailconversatie meenemen.

Groet,

(10)(2e)

Verzonden met BlackBerry Work(www.blackberry.com)

Van: "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>
Verzonden: 26 mei 2020 19:44
Naar: "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>; "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>; "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>; "(10)(2e)" <(10)(2e)@minvws.nl>; "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>; "(10)(2e)" <(10)(2e)@minvws.nl>
Cc: "(10)(2e) (10)(2e)" <(10)(2e)@minvws.nl>
Onderwerp: RE: To UZI or not to UZI

Beste allen,

(10)(2e) en ik hebben de onderstaande vraag besproken en wij komen tot de volgende overwegingen.

(I) Impact op andere processen
Het voorstel over het gebruik van UZI in de app leidt tot andere privacyvraagstukken. Er wordt immers toegang gegeven tot de gegevens van de app-gebruiker. Bovendien kan dit voorstel het proces met de AP mogelijk lastiger maken. De AP geeft immers advies over de PIA en de inrichting van de app en dit voorstel is een nieuwe significante overweging waar ze rekening mee moet houden. Als gevolg hiervan kan het proces vertraagd worden.

(II) juridisch duiden van dit vraagstuk
Het voorstel over het gebruik van UZI in de app vraagt om juridische duiding van dit onderwerp. Hiervoor hebben we nadere toelichting nodig. De behoefte aan meer informatie komt mede voort uit de omstandigheid dat tot nu toe niet is uitgaan van toegang tot de app door de zorgverlener dan wel laboratoriummedewerkers. De GGD beschikt over de gegevens die door o.m. aan de (huis)arts worden verstrekt in het kader van een verplichte melding wanneer een vermoeden dan wel een vaststelling van infectie met het COVID-19-virus bestaat. Deze meldplicht is opgenomen in de Wet publieke gezondheid. Op dat moment zal er een bron- en contactonderzoek plaatsvinden. Dit onderzoek zal geïnitieerd worden door middel van een versleutelde melding via de app. De gebruiker dient hiervoor de door de arts verstrekte code te gebruiken. Als wij het dus goed begrijpen, geeft de gebruiker dus zijn gegevens vrij aan de GGD in het kader van de meldplicht van de arts. Kortom, het uitgangspunt lijkt te zijn dat de gebruiker zelf zijn gegevens vrijgeeft. Het huidige voorstel lijkt af te wijken van dit uitgangspunt. Als gevolg hiervan is de voorvraag derhalve waarom en wie toegang tot UZI heeft. Waarom moeten de medewerkers van een laboratorium dan wel een zorgverlener, dus andere partijen dan de GGD, toegang hebben tot de app?

Een andere overweging is het gebruik van het SBV-z-register. Zorgaanbieders, indicatieorganen en zorgverzekeraars kunnen het BSN en het WID (paspoort, ID-kaart of rijbewijs) van een cliënt controleren en adresgegevens opvragen. In het kader van de app is een cliënt al geïdentificeerd omdat iemand voor het testen reeds in contact is met de arts en daar de BSN-check al gedaan is. Dit geldt in beginsel ook voor de GGD-arts. Dit betekent dat een BSN-check in het kader van de app niet nodig lijkt te zijn. Bovendien beoogt de app geen zorg op afstand.

Ons voorstel is om samen met (10)(2e) en andere collega's bespreken hoe dit op een andere manier kan worden opgelost. Vinden jullie dit een goed idee?

Met vriendelijke groet,

(10)(2e)

Ministerie van Volksgezondheid, Welzijn en Sport
Directie Informatiebeleid/CIO
Parnassusplein 5 | 2511 VX | Den Haag (10)(2e)
Postbus 20350 | 2500 EJ | Den Haag

(10)(2e)

Tel: +31 (10)(2e) | e-mail: (10)(2e)@minvws.nl

Van: (10)(2e) ([10)(2e)]) <(10)(2e)@minvws.nl>
Verzonden: dinsdag 26 mei 2020 14:33
Aan: (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>
CC: (10)(2e) <(10)(2e)@minvws.nl>
Onderwerp: RE: To UZI or not to UZI

Hoi,

Ik heb de afgelopen periode al een aantal keren contact gehad met (10)(2e) Dit ging over zowel techniek als domein. Om met de laatste te beginnen, een GGD valt binnen het huidige domein en kan zich registreren in het UZI-register (zie bijlage voor organisaties welke geregistreerd staan als GGD en het aantal producten).

Voor techniek gaat het met name over hoe je toegang inbouwt. Dit is geen "op de plank applicatie" die door het UZI-register wordt geleverd (alleen het middel wordt uitgegeven). Echter, er is wel kennis bij het CIBG hoe dit te bouwen (bij SBV-Z is er sprake van authenticatie). Voor vragen hierover zijn zij in contact gebracht met een architect van het CIBG.

Heb ook nog antwoord gegeven op de vragen in je mail.

Groet

(10)(2e)

Van: (10)(2e) <(10)(2e)@minvws.nl>
Verzonden: dinsdag 26 mei 2020 10:46
Aan: (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>
CC: (10)(2e) <(10)(2e)@minvws.nl>
Onderwerp: FW: To UZI or not to UZI

Collega's, DI & CIBG,

Zojuist sprak ik even met (10)(2e) een van de bouwers voor de app. Ik begreep dat er ook al contact was met CIBG, en hoorde daar ook de naam van (10)(2e) vallen. Gemakshalve mail ik (10)(2e) gelijk even mee.

Als ik het goed begrijp:

1. Moeten we een uitspraak doen of UZI passen ingezet kunnen worden ten dienste van de app, bij GGD medewerkers. Ik neem aan deels een juridische vraag: gaat het om mensen die aanspraak kunnen maken op een pas? Is daar juridische grond voor? In mijn optiek kunnen UZI middelen gebruikt worden ter ontsluiting van de app. Het is wel de vraag of het wenselijk is (stevigere verankering van het middel)
2. Verder ook een financiele vraag: kunnen we als VWS die kosten op ons nemen, of mag dat niet? Of willen we dat niet?
3. Hiermee zouden we antwoord moeten geven op de vraag: kunnen de UZI passen en certifacten voor dit programma ingezet worden?
4. Zoja, dan is er allerlei documentatie nodig, kan die zomaar opgeleverd worden? We leveren niet zomaar documentatie op.
5. Zie ik nog iets over het hoofd?

Groet!
(10)(2e)

Van: (10)(2e) <(10)(2e)@minvws.nl>
Verzonden: dinsdag 26 mei 2020 09:30
Aan: (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@webweaving.org>; (10)(2e) <(10)(2e)@minbzk.nl>; (10)(2e) <(10)(2e)@minvws.nl>
CC: (10)(2e) <(10)(2e)@egeniq.com>; (10)(2e) (10)(2e) <(10)(2e)@belastingdienst.nl>
Onderwerp: RE: To UZI or not to UZI

Wat nu nodig is is de analyse of bedoeld zorgproces en bedoelde zorgverleners in aanmerking komen voor een uzi pas en wat daar organisatorisch en technisch voor nodig is. Iets voor (10)(2e) dus

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e) (10)(2e) ((10)(2e)) <(10)(2e)@minvws.nl>
Datum: dinsdag 26 mei 2020 9:06 AM
Aan: (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e) (10)(2e) <(10)(2e)@webweaving.org>, (10)(2e) , (10)(2e) <(10)(2e) @minbzk.nl>, (10)(2e) , (10)(2e) , (10)(2e) ((10)(2e)) < (10)(2e) @minvws.nl>
Kopie: (10)(2e) (10)(2e) <(10)(2e)@egeniq.com>, (10)(2e) (10)(2e) < (10)(2e) @belastingdienst.nl>
Onderwerp: RE: To UZI or not to UZI

Hi,

(10)(2e) kan meekijken, als de vragen technischer worden, kunnen we iemand van CIBG vragen.
Ik hoor wel wat nodig is.

Groet!
(10)(2e)

Van: (10)(2e)) < (10)(2e) @minvws.nl>
Verzonden: dinsdag 26 mei 2020 09:04
Aan: (10)(2e) (10)(2e) (10)(2e) <(10)(2e)@webweaving.org>; (10)(2e) , (10)(2e) < (10)(2e) @minbzk.nl>; (10)(2e) , (10)(2e) , ((10)(2e)) <(10)(2e)@minvws.nl>
CC: (10)(2e) (10)(2e) <(10)(2e)@egeniq.com>; (10)(2e) (10)(2e) < (10)(2e) @belastingdienst.nl>
Onderwerp: RE: To UZI or not to UZI

Laat ik nu verantwoordelijk zijn voor de uzi infra :-). Graag even overleg vandaag.

(10)(2e) wie bij jou kan mee advies geven
(10)(2e) UZI kan by design ingezet door zorgverleners die nieuwe patiënten inschrijven om een Bsn Check te doen. Alle andere gebruik is afgeleid gebruik daarvan. Uitgifte stelt eisen aan zowel de organisatie als de persoon. Is gecheckt dat aan die eisen wordt voldaan door de medewerkers die over een pas zouden gaan beschikken?

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e) (10)(2e) (10)(2e) <(10)(2e)@webweaving.org>
Datum: dinsdag 26 mei 2020 8:47 AM
Aan: (10)(2e)) < (10)(2e) @minvws.nl>, (10)(2e) , (10)(2e) < (10)(2e) @minbzk.nl>
Kopie: (10)(2e) (10)(2e) <(10)(2e)@egeniq.com>, (10)(2e) (10)(2e) < (10)(2e) @belastingdienst.nl>
Onderwerp: To UZI or not to UZI

(10)(2e)

Om even terug te komen op je UZI vraag vs. de wens voor ook een username/password/2fa login voor laboratoria/staff.

Ik denk dat, indien dit /puur/ gaat op de prijs per UZI pas medewerker-niet-op-naam, er beslist geen positieve business case te maken is.

Een paar 100 gratis kaarten weggeven is vele malen goedkoper, heel veel sneller & levert een beter/betrouwbaarder/secuurder systeem op.

Dit komt omdat je gaat van een buitengewoon goede situatie (de 'gold standard' ontworpen voor medisch) die pentest/governance/compliance/gdpr/etc vrijwel triviaal maakt, met nauwelijks code, geen integratie en geen user database - naar een normal enterprise systeem gaat. Met account management, code, integratie, databases en alles wat er om heen zit inclusief een helpdesk inregelen.

Het inzetten/diep integreren van grote bestaande BD systemen & processen verandert hier niet veel aan (wat je bespaart aan code verlies je aan

governance, integratie en processen bijstellen). Het blijft echt een stevig stuk werk.

De kennis en kunde voor beide opties is overigens goed te vinden.

Meer gedetaileerd overzicht hieronder.

(10)(2e)

UZI approach - arch: 0 dagen, code: enkele dag(en) werk; governance/compliance: dagen

- gold standard
- Minimale exposed attack surface; pentest vrijwel triviaal & als er al wat gevonden wordt - compenserende maatregelen al in place.
  - Pentesters kunnen normale tooling niet gebruiken - dus geen junior 'onzin' findings. Moet door seniors gedaan.
  - Zeer zware rate limiting / opties limiting / zware koppeling pashouder - door calculatie op pas - heel vroeg na TCP connectie en voor TLS sessie.
- Geen noodzaak tot username, passwords, accounts, etc.
- Uiterst simpel te implementeren (inmiddels al gebeurt)
- Geen account management, geen beheerder/admin met override rechten
- Bestaand helpdesk/support/etc infrastructuur bij CIBG / Logius.
  Gewend aan medische omgevingen.
- Brute forcing & hele reeks security issues 'onmogelijk' & gezien als 'best in class' in de industrie.
- Portaal bestaat uit 1 of 2 triviale web-forms achter een standaard IIS server met SSL die een waarde in een DB duwen.
- UI/UX eigenlijk niet relevant.
- Geen zaken als MVC/Ajax nodig, geheel stateless, no cookies. geen extra javascript
- Omnipotent, stateless - dus geen failover complexiteit of andere zaken die niet lastig zijn.

NON-UZI approach - arch/planning: dagen; code: meer richting weken; governance/compliance: weken

- Normale exposed attach surface & alle normale bulk problemen.
- Additionele interfaces voor user account management, password reset, etc.
  - extra exposed attack surface voor serious pentesting
- Additional management interfaces voor users
  - extra exposed attack surface voor serious pentesting
- Integratie punten met 2FA van derden; indien Microsoft of SMS - exposed. Indien belastingdienst - rekening mee houden dat werknemers andere rechten hebben dan een MKB-er en burger t.a.v. zaken als auth-app op privé telefoon.
- Helpdesk regelen voor password / account management (ook als bestaande belasting dienst systemen gebruikt worden).
- Pentest is een serious issue; vrijwel zeker additioneel advies & compensatie maatregelen nodig. En grote surface.
- Portaal zal een 3-4 wat complexere pagina's zijn; met 3-5 pagina's voor account beheer.
- UI/UX relevant. Dat betekend zaken als javascript & rijkere frameworks - extra grote attack surface.
- Echt backend met zaken als sessie beheer, state, cookies, & failover tussen redundant systemen.
- AVG / GDPR aspect.

- Men kan het code werk vervangen door organisatorisch/compliance werk & doorlooptijd door relatief diep te integreren met bestaande belastingdienst systemen & processen.
- Bestaande/geplande mankracht onvoldoende - type resources afhankelijk van eigen code / BD integratie.

Buisiness case - non-uzi is duurder dan paar 100 uzi-passen door Min VWS gratis te laten weggeven.