To: 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e [5.1.2e @ 5.1.2e ; 5.1.2e .
(5.1.2e)[5.1.2e @minvws.nl]
Cc: 5.1.2e)[5.1.2e @minvws.nl]
From: 5.1.2e)
Sent: Tue 1/19/2021 11:10:10 AM
Subject: RE: Contact volgende week en meer documentatie
Received: Tue 1/19/2021 11:10:12 AM

Dank! Paar vragen in de tekst

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: dinsdag 19 januari 2021 12:05
Aan: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e <5.1.2e @ 5.1.2e >; 5.1.2e)
< 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: RE: Contact volgende week en meer documentatie

Ha 5.1.2e

Er zijn een paar punten die me opvallen:

1. Het initiatief is zeer lovenswaardig. Dat er een gedachte is om op basis van testbewijzen of vaccinatiebewijzen zaken weer mogelijk te maken. Op Europees niveau zien we deze gedachte vaak terugkomen alsmede in de luchtvaart. De vraag is alleen:
    1. Aan wie is het om een dergelijk bewijs uit te geven. Juist omdat het een invloed heeft op burgers ligt deze vraag waarschijnlijk bij de overheid. Zij hebben immers een taak op basis van de Wet publieke gezondheid en andere wetgeving. Hier is meer over te zeggen
    2. Het is belangrijk dit via het eHealth netwerk te doen. Daar zijn momenteel andere bewegingen zichtbaar.
    3. Het is twijfelachtig of er voor deze verwerking er wel een juridische basis is. Dat blijkt uit de documentatie waar de vraag wordt gesteld of consent van de gebruiker nodig is om gegevens door te geven. Er zijn nogal wat partijen die of toestemming of een verwerkersovereenkomst moeten hebben. Er lijkt sprake van een definitieprobleem.

    Welke partijen bijvoorbeeld?

2. Er is geen DPIA in de stukken aangetroffen. Daarom is niet veel zinnigs te zeggen over de risico's voor betrokkenen, de rechtmatigheid van de verwerking en het toepasselijke wettelijke kader.
3. Er zijn veel verschillende componenten. Het is cruciaal om op al die punten privacy en security goed te regelen. Lukt dit op een punt niet? Dan is over het geheel de privacy gecompromitteerd en loopt de security risico's. Kleinere componenten hebben absoluut voordelen, maar het geheel van de zaken moet kloppen. Dat zie ik op dit moment niet terug in het plan.
4. Er wordt geleund op een blockchain. Er zijn een paar vragen:
    1. maar het is niet duidelijk wat de blockchain exact biedt. Dat is wel noodzakelijk om doelbinding, tijdelijkheid van de verwerking te waarborgen en de rechtmatig in het geheel te beoordelen
    2. De naam "Verifiable Data Registry" maakt niet duidelijk wat wordt geverifieerd, door wie en wat de grondslag daarvan is.
    3. Het wordt niet duidelijk, waarom hier de blockchain hier een wenselijke oplossing is. De logica is juist voor bredere inzet dat er een noodzaak is voor een zeroknowledge oplossing, meer dan het bewijzen transactionele integriteit.
    4. In het Verifiable Data Registry lijkt alleen pointers naar persoonsgegevens te zitten, die niet direct voor het proces noodzakelijk zijn. De logica is dan om cryptografie zo in te zetten dat een paar digitale handtekeningen dit kunnen vervangen. Dan zet je cryptografie effectief is en bespaart de noodzaak blockchain en cloud.
5. Er wordt erg geleund op de cloud en het continu in verbinding staan met de blockchain. Dat betekent dat her en der sporen ontstaan. Dat geeft twee uitdagingen:
    1. Het continu schrijven naar systemen en verbindingen opzetten betekent een vraagstuk rond logboeken (en de persoonsgegevens die daar uitvloeien).
    2. Het moeten verbinden met een cloud geeft een afhankelijkheid van altijd online waar dit niet strikt noodzakelijk is. Je kunt ook anders cryptografisch borgen dat er recht is op testbewijzen. In een QR-code kun je aardig wat data kwijt.
6. De oplossing is technisch complex. Niet manipuleerbare technieken zouden niet technisch complex dienen te zijn, hooguit wiskundig correct.
7. In het systeem zitten de nodige handmatige processen verwerkt. Vooral aan de kant van de overheid speelt dat. Dit leidt tot een aantal risico's:

Heb je voorbeelden?

1. Het maken van fouten (waardoor er privacyrisico's ontstaan).
2. Het overbelasten van een systeem, waarbij het juist goed denkbaar is volledig geautomatiseerd te werken.

8. Bij het communiceren is een 'cloud agent' nodig voor de communicatie in de Final Archicture. Het is niet duidelijk wat deze doet en waarvoor dat nodig is.
9. Bij het issuing (het uitgeven) staat niet beschrijven wat er gebeurt richting de blockchain.
10. Bij het verifying (het verifieren): het is niet duidelijk wat het precies doet bij de blockchain. Daarbij is het onduidelijk hoe de verificatie daadwerkelijk werkt en hoe risico's worden gemitigeerd.
11. Men wil alleen proof of negative opslaan. Dat roept de vraag op of dit losse systeem niet een proof of negative moet opslaan.
12. Er zijn wat privacy specifieke problemen:
    1. De testuitslag wordt gekoppeld aan je ID. Dat betekent dat overal waar een testuitslag nodig is er ook controle van je ID moet zijn. Dit betekent dat er risico's ontstaan als:
        1. Een verifier kan zien wie er negatief getest is of een vaccinatie.
        2. Er kan een rechtmatigheidsprobleem ontstaan met het verifieren van een ID.
        3. Er is een methodiek denkbaar die veel meer subsidiair is en voorkomt dat er kennis ontstaat bij partijen, die deze informatie verwerkt.
    2. Er worden pasfoto's, leeftijd en andere zaken verwerkt, die bedoelt zijn ter indentificatie. Voor pasfoto's maakt dat een bijzonder persoonsgegeven.
        1. Het is de vraag of het wenselijk is deze gegevens te verwerken op een database verdeelt over veel computers bij veel verschillende organisaties;
        2. Het is niet noodzakelijk om een bewijs van vaccinatie of negatieve test te leveren.
        3. Geen bewaker kijkt momenteel naar de pasfoto. Dit vergt een aanpassing van het proces bij de GGD'en.
        4. Controle is op basis van de foto.
        5. Het is de vraag of het scannen van een paspoort of id rechtmatig is en vooral subsidiair.
        6. De app ontvangt de pasfoto, waardoor deze gegevens nogmaals moeten worden verwerkt via de cloud en een blockchain. Dit roept veel vragen van proportionaliteit en subsidiariteit op.
13. Er is geen borging dat alleen de gebruiker zelf de wallet beheert.
    1. Niet duidelijk is waarom er persoonsgegevens moeten worden verwerkt.
    2. Het is onduidelijk hoe de security van deze wallet is geborgd.
    3. Onduidelijk is hoe wordt voorkomen dat een rogue app gebruik maakt van de opgeslagen gegevens.
14. De security komt uit de app en niet uit het protocol. Dat betekent dat het sneller fraudegevoelig is. Het is denkbaar dat een shady website met bijvoorbeeld HTML-5 hetzelfde bewijs kan geven. De logica is dat de verificatie uit het protocol komt.
15. De enige manier om authenticiteit te controleren door een centraal register is door de handtekening van het centrale register te controleren, dat hoeft niet perse via een decentraal protocol te gebeuren.
16. Transparantie. Zoveel mogelijk open source is uit. Mij is niet bekend waar de broncode is, waardoor niet te toetsen is of de app functioneert.
17. De papieren oplossing laat veel onduidelijk. Is duidelijk nog niet goed genoeg uitgedacht.

Volgens mij moet hier nog even goed over worden nagedacht.

Hartelijke groet,

5.1.2e

Van: 5.1.2e) < 5.1.2e @minvws.nl>
Verzonden: maandag 18 januari 2021 17:04
Aan: 5.1.2e < 5.1.2e @ 5.1.2e ; 5.1.2e) < 5.1.2e @minvws.nl>
CC: 5.1.2e) < 5.1.2e @minvws.nl>; 5.1.2e) < 5.1.2e @minvws.nl>
Onderwerp: FW: Contact volgende week en meer documentatie
Urgentie: Hoog

Ik stel voor eerst tegen onze lat leggen en dan antwoorden. Eens?

5.1.2e 5.1.2e

dubbel

Pagina's zijn verwijderd 1500099

3 - 4

dubbel