**To:** 5.1.2e )[ 5.1.2e @minvws.nl]; 5.1.2e )[ 5.1.2e @minvws.nl]
**From:** 5.1.2e )
**Sent:** Fri 1/15/2021 4:41:37 PM
**Subject:** RE: Unlock - analyse vanuit privacy
**Received:** Fri 1/15/2021 4:41:38 PM

Goed om deze vraag eerst voor te leggen aan WJZ.
5.1.2e is 5.1.2e 5.1.2e @minvws.nl

Groeten,

5.1.2e

**Van:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Verzonden:** vrijdag 15 januari 2021 16:22
**Aan:** 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e )
< 5.1.2e @minvws.nl>; 5.1.2e ) < 5.1.2e @minvws.nl>
**CC:** 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e < 5.1.2e >
**Onderwerp:** RE: Unlock - analyse vanuit privacy

Dag 5.1.2e

Dan zou daar ook een privacyjurist bij moeten lijkt me. Via de 5.1.2e lijkt me meest haalbaar.

Met vriendelijke groet,

5.1.2e
5.1.2e

**Ministerie van Volksgezondheid, Welzijn en Sport**

Postbus 20350 | 2500 EJ | Den Haag
5.1.2e 5.1.2e | 5.1.2e @minvws.nl | 070 5.1.2e

T 070- 5.1.2e
5.1.2e @minvws.nl

**Van:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Verzonden:** vrijdag 15 januari 2021 16:10
**Aan:** 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e )
< 5.1.2e @minvws.nl>; 5.1.2e ) < 5.1.2e @minvws.nl>
**Onderwerp:** RE: Unlock - analyse vanuit privacy

Ha 5.1.2e

5.1.2e en ik hebben net weer met het consortium (waaronder Unlock) gesproken.
Zij willen graag maandag as (op een door jullie aangegeven moment) nog even een half uurtje met jullie spreken, omdat zij denken dat hun blockchain app geen problemen oplevert met AVG.
5.1.2e n ik zouden het fijn vinden als jullie dit willen faciliteren, zodat we dinsdag (de brainstorm die nog gepland gaat worden) geen heel technische discussie hoeven hebben.
Kunnen jullie mij een half uurtje doorgeven, zodat we iets kunnen laten plannen? Unlock past zich aan jullie agenda's aan.
Veel dank, 5.1.2e

**Van:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Verzonden:** vrijdag 15 januari 2021 11:49
**Aan:** 5.1 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e )

< 5.1.2e @minvws.nl>; 5.1.2e ) < 5.1.2e @minvws.nl>
**Onderwerp:** RE: Unlock - analyse vanuit privacy

Dag 5.1.2e

Een poging van mij:

- **Blockchain en AVG: moeilijk verenigbaar**

Blockchain technologie is (tenzij met heel veel technische maatregelen) nauwelijks in overeenstemming te brengen met de AVG. Zie o.a. https://www.considerati.com/nl/kennisbank/is-de-blockchain-verenigbaar-met-de-avg.html. In dit geval lijken die maatregelen (verre van) aanwezig.

- **Implementatie: teveel verwerking van persoonsgegevens**

De gekozen implementatie leidt er daarnaast toe dat veel partijen veel persoonsgegevens (wie ik ben en hoe ik getest ben) kennen en verwerken. Iedereen die de check doet weet veel van mij. Dat is erg onwenselijk. Het bewijzen van een test kan met verwerking van veel minder gegevens en zonder dat er registraties ontstaan die weer (voor geld) verhandelbaar zijn.

Ten aanzien van vaccinaties speelt iets soortgelijks (in EU verband) waarbij de lidstaten willen komen tot zo min mogelijk verwerking van persoonsgegevens.

Groet

5.1.2e

**Van:** 5.1 5.1.2e ) < 5.1.2e @minvws.nl>
**Verzonden:** donderdag 14 januari 2021 22:33
**Aan:** 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e .
( 5.1.2e ) < 5.1.2e @minvws.nl>
**CC:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Onderwerp:** RE: Unlock - analyse vanuit privacy

Dag 5.1.2e
Dank. Ik begrijp ongeveer wat hier staat ;-)
Mijn vraag zou nog zijn: zijn al deze tekortkomingen inherent aan hun technologie, of zou je hen bij het verstrekken van een heldere opdracht met harde randvoorwaarden alsnog in het keurslijf van AVG en andere wet- en regelgeving kunnen persen?
Mvg
5.1.2e

5.1.2e
5.1.2e
5.1.2e @minvws.nl
+31 6 5.1.2e

**Van:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Verzonden:** donderdag 14 januari 2021 22:08
**Aan:** 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1 5.1.2e ) < 5.1.2e @minvws.nl>; 5.1.2e .
( 5.1.2e ) < 5.1.2e @minvws.nl>
**CC:** 5.1.2e ) < 5.1.2e @minvws.nl>
**Onderwerp:** Unlock - analyse vanuit privacy

Dag 5.1.2e

Nav je telefoontje, hierbij een korte weergave van onze analyse van het Unlock concept en waarom wij van mening zijn dat het niet geschikt is voor het doel van testbewijs. Basis voor de analyse zijn de documenten die we gekregen hebben en de gesprekken tussen onze experts en de developers van Unlock half december om meer informatie te achterhalen over de technische architectuur. De informatie die door uNLock is aangeleverd bestaat uit een aantal flowcharts waarin aangeduid wordt hoe informatie tussen verschillende partijen wordt uitgewisseld. Verdere technische specificatie in geschreven vorm ontbreekt, en de aangeleverde flowcharts bevatten onderdelen (o.a. de Trusted Service Provider) die nog niet bestaan of alleen geschikt zijn om gebruikt worden in de financiële toepassing van deze technologie bij de Rabobank, en geen betrekking hebben op uNLock.

Een aantal bevindingen:

- Het Unlock concept is gebaseerd op blockchain. Blockchain is –simpel gesteld- een decentrale gedistribueerde boekhouding van transacties, waarbij eenieder kan controleren of een transactie heeft plaatsgevonden. Dat is bijzonder prettig in de context van bijvoorbeeld financiële transacties waarbij je niet één centrale partij wilt of kunt vertrouwen. Kenmerk van een blockchain is dat alle transacties eeuwig vastgelegd worden en voor iedereen inzichtelijk zijn. Een testresultaat heeft geen waarde / functie meer na 72 uur; een eeuwige vastlegging is dus niet nodig en niet gewenst.
- De toepassingen van houder, controleur en uitgever waar Unlock gebruik van maakt zijn primair ontworpen voor zaken als hypotheken, tikkies en payments.
- Er zit een fundamenteel/diep in het ontwerp gewortelde traceerbaarheid van wie & wat ('smart contracts' in blockchain), waarin elk test-resultaat een uniek traceerbaar nummer heeft die centraal wordt bijgehouden.
- In het concept wordt de gebruiker gevraagd om zijn persoonlijke ID gegevens op te slaat in de 'wallet' door zijn rijbewijs / paspoort te scannen, en de testuitslag gekoppeld aan zijn identiteit te delen bij de toegangscontrole van een evenement.
- **Door deze eigenschappen is er geen doelbinding, is het niet proportioneel en voldoet het niet aan de eis van data minimalisatie.**
- Belangrijke zaken (zoals de verificatie van verifier identiteit) ontbreken nog.
- Het is niet ontworpen voor het threat model rond vaccinatie/testen - waarbij zowel de burger (de naar zijn pop concern wil) als de controleur (de portier van het concert) niet a priori volledig te vertrouwen zijn.
- Interactie tussen houder en controleur gaat exclusief van de wallet over het internet naar een server, waarbij de communicatie eindigt bij de server. Geen peer-to-peer interactie tussen houder en controleur (of end-to-end beschermd verkeer.)
- Scenario waarin de maker van de software alle terminating infrastructuur draait waar de identifiers langskomen is waarschijnlijk.
- De apps zijn geen native apps – maar grotendeels web-apps, met andere veronderstellingen qua veiligheid.

Mede namens 5.1.2e

5.1.2e
5.1.2e
Ministerie van VWS
06 5.1.2e