De beperkte, beheerste en gecontroleerde inzet van GKVI

De bedoeling van GKVI

GKVI is bedoeld om personen te faciliteren voor wie het niet mogelijk is om via de hoofdroute van "CoronaCheck" (die ziet op direct vanuit bronsystemen genereren van bewijzen en dus als het gaat om de GGD'en gekoppeld is met CoronIT) een coronatoegangsbewijs te genereren voor nationaal, dan wel internationaal gebruik. VWS heeft de GGD'en verzocht om in die gevallen gebruik te maken van de uitzonderingsroute "het GKVI-Portaal". Hoofdlijn van de inzet van GKVI is:

(1) Het lukt de persoon niet om via de hoofdroutes zelf een bewijsmiddel te genereren en
(2) Het probleem kan niet via een structurele technische oplossing worden opgelost richting de hoofdroute.

Er is een maatschappelijk belang om GKVI zo spoedig mogelijk uit te rollen. Het is namelijk voor veel uitzonderingsgroepen (bv. buitenlandse vaccinaties, geen BSN, geen woonplaats NL en wel hier gevaccineerd ect) een oplossing voor het verkrijgen van coronabewijzen. Al deze mensen moeten zo snel mogelijk geholpen worden, zeker met het oog op de mogelijke invoering van een 2G beleid. Daarnaast is op Europees niveau bepaald dat iedereen, die getest, gevaccineerd of hersteld is, een wettelijke recht toekomt om een DCC (Digital Covid Certificate) te ontvangen.

Frauderisico GKVI

Door de eerdere ervaringen met HKVI, die hebben geleid tot tienduizenden fraudegevallen, is in gezamenlijkheid besloten om over te stappen naar GKVI. Hierdoor konden de benodigde technische functionaliteiten (o.a. logging en monitoring) in het portaal worden geïmplementeerd om het frauderisico zoveel mogelijk te mitigeren. Echter blijft ook GKVI risicovol als het gaat om fraude, aangezien er sprake is van een handmatige invoer van gegevens bij het gebruik van het portaal. Dit heeft tot gevolg dat een ieder met toegang tot GKVI portaal ten onrechte een bewijs kan uitgeven, wanneer de desbetreffende persoon ter kwader trouw is. Parralel aan de uitrol van GKVI, dient dit risico dient via twee hoofdsporen zoveel mogelijk gemitigeerd te worden:

(1) Zoveel mogelijk uitzonderingsgroepen bedienen via een directe koppeling met CoronIT
(2) Een beheerste en gecontroleerde inzet van het GKVI portaal

1. Zoveel mogelijk uitzonderingsgroepen bedienen via een directe koppeling met CoronIT

Er zijn verschillende groepen waarvan de gegevens wel bekend zijn in CoronIT, maar geen gebruik kunnen maken van de hoofdroute CoronaCheck. Dit zijn onder andere:

- Personen die niet beschikken over een Burgerservicenummer (BSN)
- Personen die geen toegang tot DigiD hebben en geen woonplaats hebben in Nederland
- Personen die een eerste vaccinatie elders hebben verkregen, maar de tweede (dan wel derde) via de GGD
- Personen die in ons land woonachtig zijn, maar die gevaccineerd zijn in een ander land dan Nederland. *De GGD buitenlanddesk registreert namelijk de ontvangen gegevens in CoronIT*

We kunnen er gezamenlijk voor zorgen dat deze groepen bediend worden via een directe koppeling met CoronIT. Daardoor ontstaat geen handmatige invoer bij het vertalen van de gegevens in CoronIT naar een Coronabewijs.

Om dit mogelijk te maken, is het volgende nodig:

- Een "Coronabewijs knop" toevoegen in CoronIT
- Die zorgt ervoor dat de benodigde gegevens van het medische dossier worden samengevat
- De samenvatting van gegevens worden verstuurd naar de signer van CoronaCheck
- VWS stuurt het ondertekende Coronabewijs terug naar CoronIT

We stellen voor om de volgende afspraak te maken:

Het mogelijk maken van een directe koppeling met CoronIT binnen een tijdsbestek van 6 weken. GGD GHOR Nederland en VWS realiseren dit samen. Wanneer blijkt dat er extra technische hulp nodig is om bovengenoemde activiteiten te ontwikkelen, dan vragen we jullie om de aangeboden hulp van VWS te accepteren

2. Een beheerste en gecontroleerde inzet van het GKVI portaal

Er zullen altijd uitzonderingsgroepen bestaan, waarbij het gebruik van het GKVI portaal noodzakelijk is. Dit zijn onder andere:

- Personen waarvan de gegevens niet in CoronIT bekend zijn of niet kunnen worden opgeslagen.

Dit wordt dan ook het bedoelde gebruik van GKVI genoemd. Dit gebruik dient beheerst en gecontroleerd te worden ingezet. Er zijn inmiddels verschillende technische functionaliteiten ingebouwd die ervoor gaan zorgen dat GKVI portaal op een beheerste en gecontroleerde gebruikt kan worden. Echter zijn er nog steeds verschillende risico's gesignaleerd, waarbij we per risico de volgende maatregel voorstellen:

1. **Risico:** Het GKVI portaal inzetten voor de technische knelpunten die tot gevolg hebben dat gegevens uit CoronIT niet doorkomen in de CCA database in plaats van de hoofdroute in te richten
   Maatregel: Oplossen van technische problemen pakken GGD GHOR Nederland en VWS samen op, zodat het probleem binnen een tijdsbestek van maximaal 4 weken opgelost kan worden

2. **Risico:** VWS heeft momenteel geen inzicht in de rapportage en monitoring van het gebruik, inclusief mogelijke verdachte patronen
   Maatregel: Taak inrichten bij de GGD SOC die elke dag aan hoofdgebruiker én aan VWS terug wordt gemeld hoeveel bewijzen zijn uitgegeven per account, welke accounts geactiveerd en gedeactiveerd zijn etc. De hoofdgebruiker zicht op werkelijk gebruik, VWS krijgt zicht op afwijkend en verdacht gebruik.

3. **Risico:** VWS heeft geen inzicht in welke maatregelen zijn genomen om fraude te beheersbaar te maken
   Maatregel: Het organiseren van een risicobeheersingssessie met VWS (bijv. een FMEA-sessie), waarbij inzicht wordt gegeven hoe de mitigerende maatregelen worden opgevolgd

4. **Risico:** Er is momenteel geen rate limiter per dag/per uur ingesteld die ervoor kan zorgen dat mensen niet teveel bewijzen per uur en/of dag kunnen uitgeven
   Maatregel: Samenwerking met VWS en GGD om goede requirements te definiëren, zodat deze functionaliteit ingebouwd kan worden

5. Er zijn verschillende IAM (identity and access management) risico's gesignaleerd die voortvloeien uit de inrichting van de bestaande IAM processen en functionaliteiten, onder andere:

5.1 **Risico:** Het niet kunnen afsluiten van GKVI-gebruikers buiten werktijden
Maatregel: Technisch inregelen dat alleen toegang tot GKVI mogelijk is binnen werktijden

5.2 **Risico:** Er kan geen rolonderscheid gemaakt worden, waardoor er niet per gebruiker kan worden aangegeven welke type bewijzen ze mogen uitgeven
Maatregel: In het IAM proces mogelijk maken dat per rol ingesteld kan worden welke type bewijzen ze kunnen uitgeven en welke functionaliteiten geactiveerd zijn

5.3 **Risico:** Er kan geen rolonderscheid gemaakt worden, waardoor het is niet mogelijk om het 4-ogen beleid technisch af te dwingen,
Maatregel: 4-ogen beleid inrichten door in het IAM proces mogelijk te maken om een supervisor rol toe te kennen aan 1 of meerdere gebruikers

5.4 **Risico:** Er kan niet centraal ingesteld worden dat alle gebruikers verplicht 2FA dienen te gebruiken, aangezien de gebruiker op regionaal niveau inlogt via de Identity hub
Maatregel: Ervoor zorgen dat 2FA verplicht ingesteld staat in alle IAM processen op regionaal niveau.

5.5 **Risico:** Het toekennen van rollen gaat per GGD regio, waardoor geen centrale controle via GGD SOC kan plaatsvinden
Maatregel: Samenwerking inrichten om de centrale SOC te koppelen aan de beheerteams van de regio's

Conclusie ten aanzien van de beperkte, beheerste en gecontroleerde inzet van GKVI

Om er gezamenlijk voor te zorgen dat het GKVI portaal op een beperkte, beheerste en controleerde wijze wordt ingezet in alle GGD regio's, is ons uitgangspunt als volgt (in orde van prioriteit):

1. De uitrol van GKVI vindt plaats op voorwaarde dat alle gesignaleerde IAM risico's zijn gemitigeerd: 5.1 t/m 5.5, aangezien deze punten randvoorwaardelijk zijn voor gecontroleerd gebruikersbeheer.
2. Parralel aan de uitrol van GKVI: we zorgen er gezamenlijk voor dat de directe koppeling met CoronIT mogelijk wordt gemaakt; binnen een tijdsbestek van 6 weken .
3. Parralel aan de uitrol van GKVI: het organiseren van een risicobeheersingssessie met VWS (bijv. een FMEA-sessie), waarbij inzicht wordt gegeven hoe de mitigerende maatregelen worden opgevolgd. Hierbij gaan we er ook vanuit dat alle gesignaleerde risico's uit deze nota worden meegenomen.