
Rijksoverheid
BRBA
registraties
Registratie van vaccinaties met state-of-the-art security
Veilige melding van vaccinaties
Bij de bestrijding van de pandemie ten gevolge van het coronavirus spelen de komende vaccinaties een grote rol. Ter ondersteuning van het beleid en de uitvoering van dit nieuwe, omvangrijke vaccinatieprogramma en de mogelijke bijsturing daarvan, wordt door het RIVM een centrale registratie opgezet. Wanneer zorgverleners mensen vaccineren, melden ze dit aan het RIVM. Niet iedere zorgaanbieder heeft (al) systemen waarmee dat kan.
BRBA, dat staat voor Beveiligde Registratie Bijzondere Assets, is ontwikkeld voor die situaties waarin wel gevaccineerd wordt, maar er geen aansluiting is op het centrale registratiesysteem. I let is een veilige invoermodule van het centrale registratiesysteem van het RIVM.
BRBA is met grote aandacht voor privacy en informatieveiligheid ontwikkeld door het team dat ook zorgde voor de CoronaMelder-app en de GGD Contact-app.

Uitgangspunten:

- Biedt een veilig en werkbaar systeem voor het doorgeven van de vaccinaties aan het RIVM.
- Heeft als uitgangspunten security by design & privacy by default.
- Zorgt voor compartimentering van software en organisatie.
- Is gebouwd op basis van de actuele beveiligingsstandaard van de industrie en overheid, volgt BIO 2019 en het RIVM Handboek Informatiebeveiliging.
- Is ontwikkeld door de medewerkers die betrokken zijn bij de CoronaMelder-app en de GGD Contact-app, in opdracht van het Programma Realisatie Digitale Ondersteuning van het ministerie van VWS en in samenwerking met het RIVM.
- Wordt ingezet in situaties waarin geen geautomatiseerde melding van vaccinatie aan het RIVM voorhanden is.

Rijksoverheid

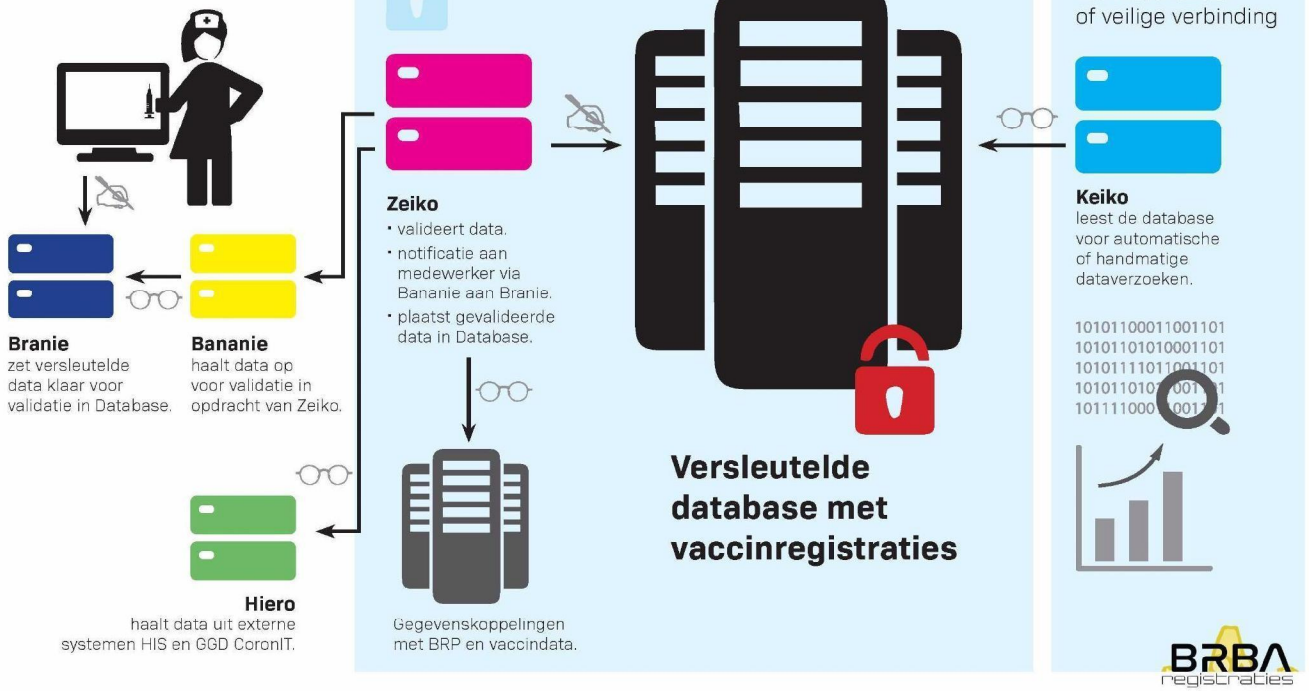
BRBA registraties

Registratie van vaccinaties met *state-of-the-art security*

Registratie van vaccinaties met *state-of-the-art security*

Ontwerpschema

Rijksoverheid



Ontwerp en functie

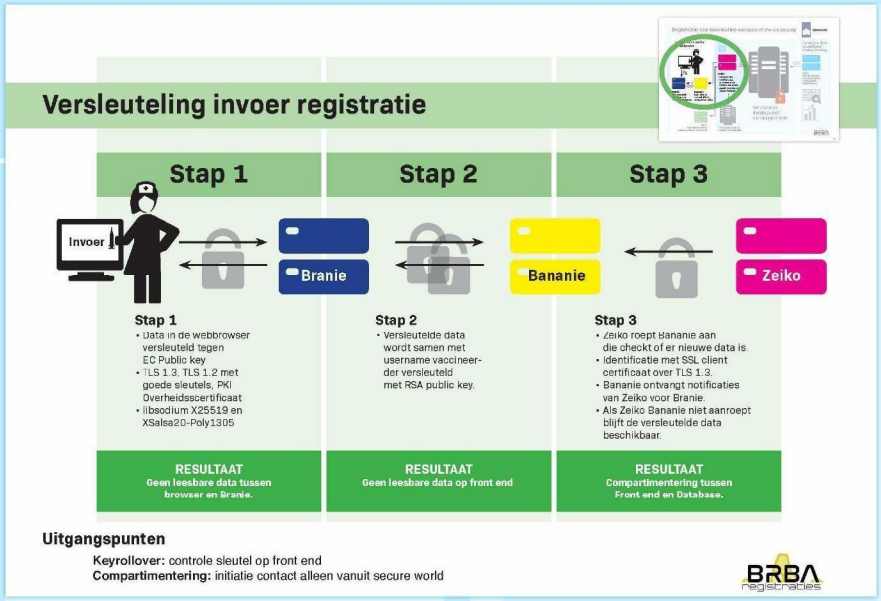
Vaccinaties worden geregistreerd via de webbrowser of via datasystemen zoals GGD CoronIT.

Directe invoer op de vaccinatielocatie:

De data worden ingevoerd in de web-browser, die communiceert met het frontend. De webbrowser maakt verbinding met Branie voor het inloggen van de gebruiker en het invoeren van de data. Webtoegang met een moderne browser werkt in vrijwel alle gevallen en is breed beschikbaar.

De data komen versleuteld binnen en worden door Branie verder versleuteld, in combinatie met metadata zoals de accountgegevens van de invoerder. Vervolgens worden de data klaargezet voor verdere behandeling. Het is een versleuteld 'one way'-systeem met asymmetrische encryptie, waardoor zelfs de beheerder niet bij de informatie kan.

Bananie wordt aangestuurd door de validator van het systeem, genaamd Zeiko. Zeiko vraagt aan Bananie of er nieuwe data beschikbaar zijn en neemt ze af voor



validatie. De gebruiker krijgt een melding van het resultaat van de validatie, die wordt verzonden via Bananie en Branie.

Overname van data uit een derde systeem:

Hiero maakt een veilige verbinding met de dataleverancier en haalt de data op. Na

controle worden de data versleuteld en klaargezet voor validatie door Zeiko. Het is een automatisch systeem met een volledige audit trail voor de dataleverancier. Als de data niet gevalideerd kunnen worden, blijven ze versleuteld op Hiero beschikbaar tot het probleem kan worden gevonden en opgelost.

Vervolg ontwerp en functie

Validatie:

De door Bananie en Hiero aangereikte data worden door Zeiko uitgepakt en gevalideerd aan de hand van de beschikbare gegevenskoppelingen (BRP, vaccindata). Als de validatie van de data geslaagd is, worden ze versleuteld opgeslagen in de database. Zeiko heeft alleen schrijfrechten voor de database en kan alleen informatie toevoegen, maar niet uitlezen. Er is sprake van volledige compartimentering, die tot het uiterste is doorgevoerd.

Database:

De database is versleuteld en volledig sandboxed. Zelfs de beheerder van de database heeft er geen toegang toe, omdat de sleutel tot de database zich op een andere plek bevindt. Zo is er op het basisniveau in het systeem een 'vier ogen'-methode ingevoerd.

Uitlezen en data-exports:

Keiko heeft toegang tot de database en kan automatische rapportages en handmatige informatieverzoeken verzorgen. Keiko sluit aan op het dataformaat van het RIVM en levert de informatie die nodig is voor de logistieke en beleidsmatige vragen van het RIVM.

Keiko levert de volgende informatie vanuit BRBA-registraties:

- Het aantal vaccinaties per doelgroep, leeftijd, woonplaats, regio en geslacht
- Het aantal vaccinaties per batch en locatie (voor de logistiek)
- Tracering van personen per vaccinbatch
- Gegevens worden toegevoegd aan de vaccinatieregistratiedatabase van het RIVM

Gebruikerservaring

Account aanmaken

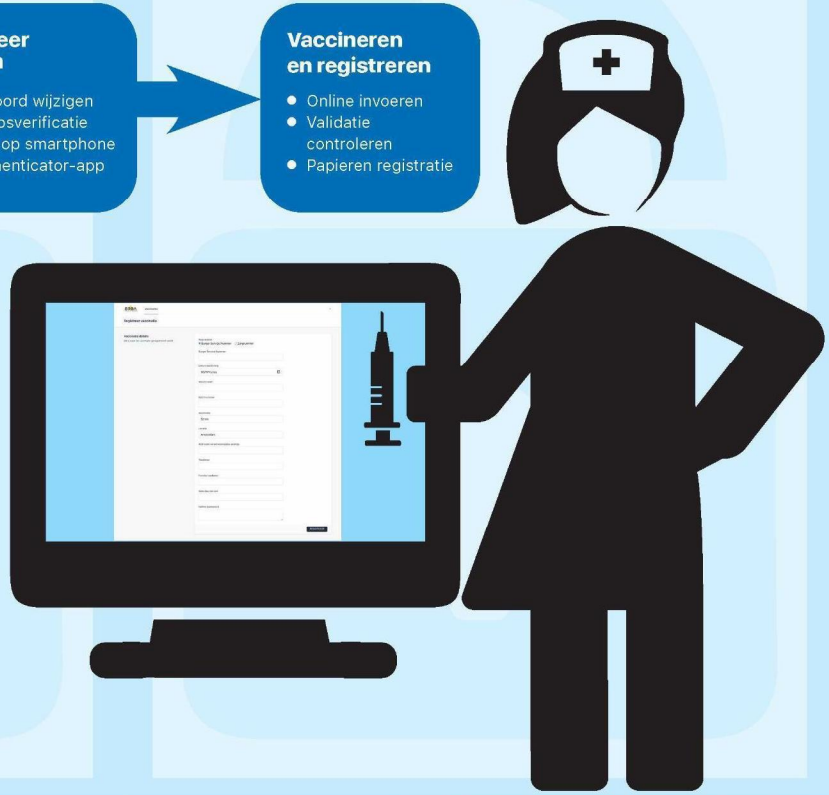
- Door locatieverant-woordelijke arts
- Bevoegdheid wordt gecontroleerd
- Wachtwoord, 2FA QR-code op papier

Eerste keer inloggen

- Wachtwoord wijzigen
- Tweestapsverificatie instellen op smartphone met Authenticator-app

Vaccineren en registreren

- Online invoeren
- Validatie controleren
- Papieren registratie



BRBA-registraties werken met een invulformulier in een recente browser, waardoor de invulomgeving voor iedereen herkenbaar is. Iedereen die vaccins prikt is hiervoor bevoegd, maar het invullen zal vaak door een ondersteuner gedaan worden. Dit is zo eenvoudig mogelijk gemaakt.

De locatieverantwoordelijke arts (degene die medisch verantwoordelijk is voor de registratie van de vaccins) is verantwoordelijk voor de accounts van de medewerkers die de vaccins invoeren. Inloggen gaat met tweestapsverificatie. Naast goede documentatie is de helpdesk beschikbaar om te helpen met het instellen van de accounts en de tweestapsverificatie.

De documentatie is vanaf 4 januari beschikbaar.

Hoofdlijnen van het securityconcept

Het securityconcept van BRBA-registraties is aangepast aan het soort data dat aangeleverd wordt.

- Security & privacy by design
- Sterke functiescheiding en compartimentering met 'one way'-verkeer
- Openbare sleutel/asymmetrische encryptie op meerdere lagen
- Hardware Security Module (HSM) voor sleutelbeveiliging
- SOC/SIEM, waardoor aanvallen snel worden opgemerkt en er snel gehandeld wordt
- Threat Hunting, waarbij pro-actief wordt gezocht naar aanvallen
- Hosting die geschikt is voor medische gegevens
- Gebruik van moderne ontwikkelmethodes en herhaalde evaluatie van code
- Het uitgangspunt is geen dataverlies, zowel in de software als door beheermaatregelen
- Off-site back-ups, nood- en herstelplan

Conclusie beveiligingsanalyse

5.1.2e **van Secundity heeft het team begeleid als security tester en positieve conclusies getrokken over de tot nu toe gezette stappen:**

"Het ontwikkelteam achter het COVID-19 vaccinatieregistratieportaal heeft in korte tijd een indrukwekkende prestatie geleverd. Als dit op dezelfde voet en met meer capaciteit en ondersteuning wordt doorgezet [...], dan is het ambitieus, maar wel haalbaar om via het ontwikkelde portaal veilig vaccinatieregistraties mogelijk te maken op 8 januari 2021."

Naar aanleiding van de conclusies van 5.1.2e 5.1.2e **is het team uitgebreid en op schema om op 6 januari 2020 de eerste vaccinaties te registreren.**