

**BRBA**

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 vaccinaties een grote rol. Ter ondersteuning van het beleid en de uitvoering van dit nieuwe, omvangrijke vaccinatieprogramma en de mogelijke bijsturing daarvan is 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. Het 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:

- Veilige invoer van vaccinaties in de database van het RIVM.
- Security by design, privacy by default.
- Openheid, vertrouwen en transparantie in software ontwikkeling met open source technieken.
- Gebouwd volgens de actuele beveiligingsstandaard van de industrie en overheid, volgens BIO en het RIVM Handboek Informatiebeveiliging.
- Ontwikkeling 'in huis' bij het programma Realisatie Digitale Ondersteuning van het Ministerie van VWS.
- Beschikbaar voor alle situaties waarin geen geautomatiseerde melding van vaccinaties aan het RIVM voorhanden is.



Rijksoverheid

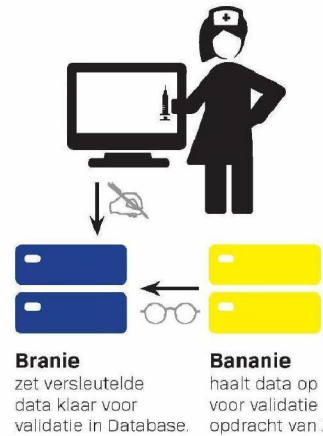
BRBA
**Registratie van vaccinaties
met *state-of-the-art* security**

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

Ontwerpschema



Invoer vaccinatie via webbrowser

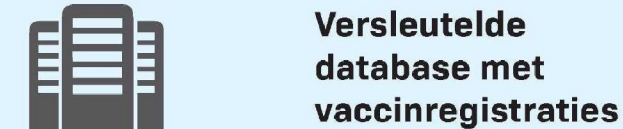


Bananie
haalt data op voor validatie in opdracht van Zeiko.

Hiero
haalt data uit externe systemen HIS en GGD CoronIT.

Zeiko

- valideert data.
- notificatie aan medewerker via Bananie aan Branie.
- plaatst gevalideerde data in Database.



Gegevenskoppelingen met BRP en vaccindata.

Opvragen data via webbrowser of veilige verbinding



Keiko
leest de database voor automatische of handmatige dataverzoeken.

```
10101100011001101
10101101010001101
10101111011001101
101011010100111
10111000100111
```



Ontwerp en functie

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

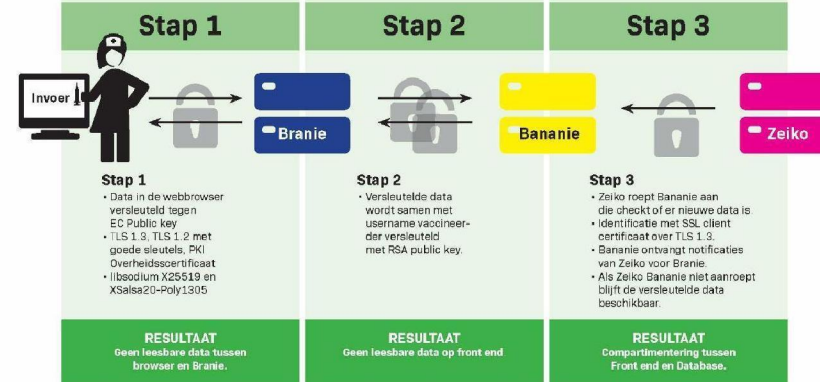
Directe invoer op de vaccinatielocatie:

De vaccinaties worden per stuk of als batch in een CSV-bestand ingevoerd in de webbrowser, die communiceert met het front-end. 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.

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

Versleuteling invoer registratie



Uitgangspunten

Keyrollover: controle sleutel op front end

Compartimentering: initiële contact alleen vanuit secure world



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

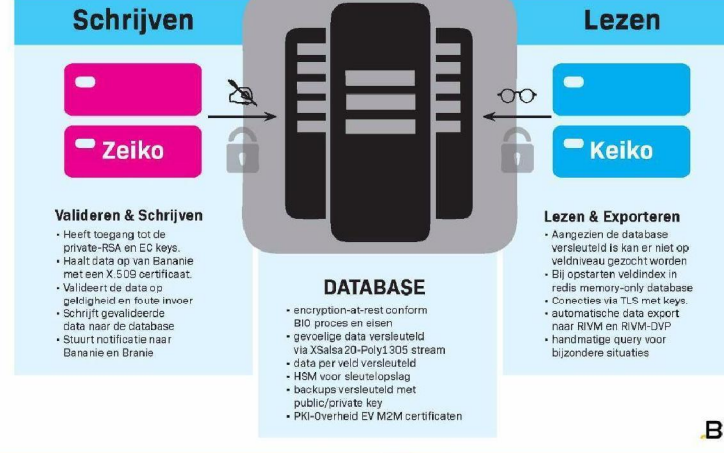
Database:

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 basisoniveau in het systeem een 'vier ogen'-methode ingevoerd.

Uitlezen en data-exports:

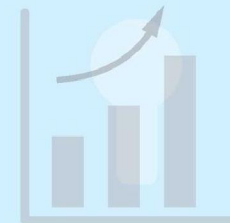
Keiko heeft toegang tot de database en kan automatische rapportages en handmatige informatieverzoeken verzorgen. Keiko sluit aan op het dataformaat van het RIVM en levert de informatie die nodig is voor de logistieke en beleidsmatige vragen van het RIVM.

Compartimentering & versleuteling database



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 locatieverantwoordelijke 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

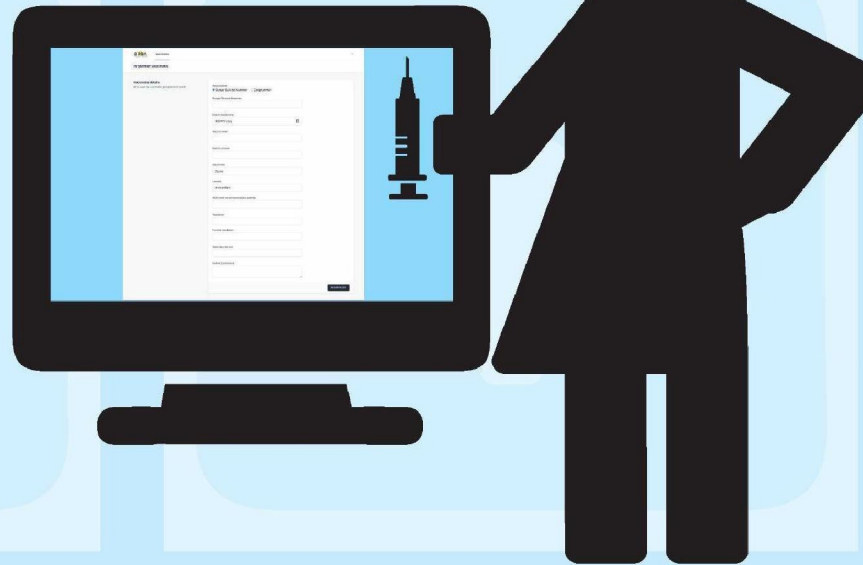
- Online invoeren
- Validatie controleren
- Papieren registratie

BRBA werkt 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.

BRBA is direct toegankelijk met een persoonlijke UZI pas of na aanvraag van een account. De instelling vraagt accounts aan voor de verantwoordelijken in de organisatie en na controle worden deze personen toegelaten tot het systeem. De accountgegevens worden persoonlijk uitgereikt en bij het inloggen wordt tweestapsverificatie gebruikt.

Naast de praktische documentatie is ook een deskundige helpdesk beschikbaar, via telefoon en e-mail.

De handleidingen voor BRBA.nl zijn beschikbaar via <https://docs.brba.eu/handleidingen/>



Hoofdlijnen van het securityconcept

Het securityconcept van BRBA 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

Toepassing BRBA.nl in de vaccinatiecampagne

BRBA.nl wordt ingezet als flexibele invoerapplicatie in de meest uiteenlopende situaties.

Dankzij de betrokkenheid van het ontwikkelteam en het 'in house' concept van softwareontwikkeling bij programma Realisatie Digitale Ondersteuning van het Ministerie van VWS speelt BRBA.nl in op de ontwikkeling van de campagne.

De ziekenhuizen gebruikten BRBA.nl direct vanaf de start van de campagne op 6 januari 2021, voor de invoer van de prikken die bij de medewerkers zijn gezet.

In de volgende stappen van de campagne wordt BRBA.nl ingezet daar waar geen bestaande koppeling met het RIVM voor handen is.