Rijksoverheid

BRBA registraties

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

Veilige registraties

Het project BRBA registraties, Beveiligde Registratie Bijzondere Assets, is opgestart met als doel een veilig en werkbaar systeem voor de registratie van de vaccinaties die worden gegeven in de campagne tegen COVID19. Voor de effectiviteit van de COVID-19 vaccinatiecampagne is het cruciaal dat bekend is wie, welk vaccin (inclusief batch of charge nummer), wanneer gekregen heeft. BRBA registraties biedt een oplossing voor registratie, van de vaccineerder tot en met de database bij het RIVM.

De aanleiding: toen in het nieuws kwam dat de ICT roet in het eten zou kunnen gooien bij de voortgang van de vaccinatiecampagne heeft de groep die ook aan de Coronamelder en GGD Contact app werkte de handen ineengeslagen om in korte tijd een flexibel en veilig systeem op te zetten. We zijn betrokken bij de bestrijding van COVID19 en willen met onze kennis en kunde bijdragen aan een veilige en werkbare oplossing voor de registratie van vaccinaties.

Vanuit deze wat onconventionele start is aan een state-of-the-art systeem gewerkt en is er in samenwerking met VWS Programma Realisatie Digitale Ondersteuning en het RIVM opgeschaald. Het systeem voldoet aan de eisen die programmeurs aan hun eigen materiaal stellen, is geschikt voor leken om te gebruiken en kan de toetsing op relevante regelgeving ruimschoots doorstaan.

Uitgangspunten:

- biedt een veilig en werkbaar systeem voor de registratie van de vaccinaties die worden gegeven in de campagne tegen COVID19.
- heeft security by design & privacy by default als uitgangspunten: maximale compartimentering en encryptie met moderne techniek.
- is gebouwd naar de actuele beveiligings-standaard van de industrie en overheid, volgt BIO 2019 en het RIVM Handboek Informatiebeveiliging.
- is opgezet door VWS, Programma Realisatie Digitale Ondersteuning, RIVM en de mensen betrokken bij Coronamelder en de GGD Contact app.
- wordt ingezet voor situaties waar geen digitale registratie voorhanden is en als 'Plan C' mocht dat nodig zijn.

Rijksoverheid

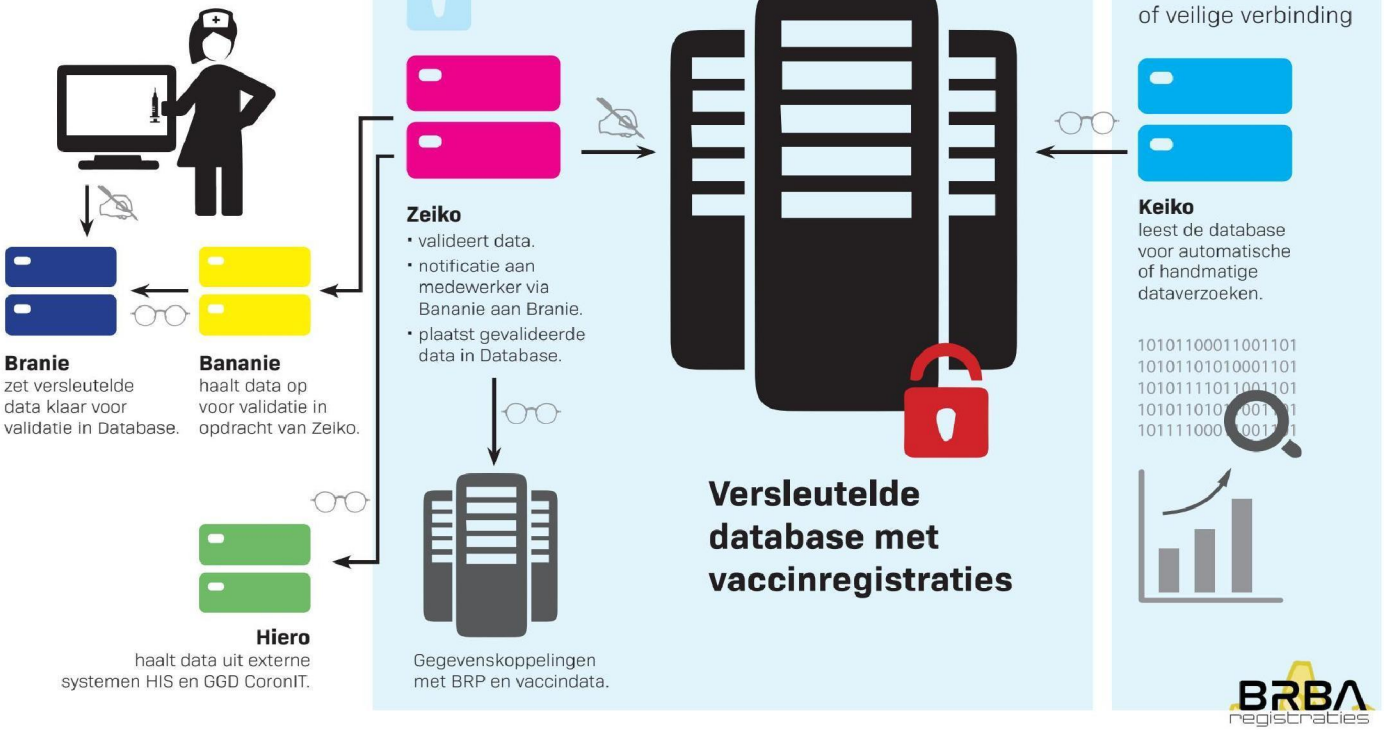
BRBA registraties

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

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

Ontwerpschema

Rijksoverheid



Ontwerp en functie

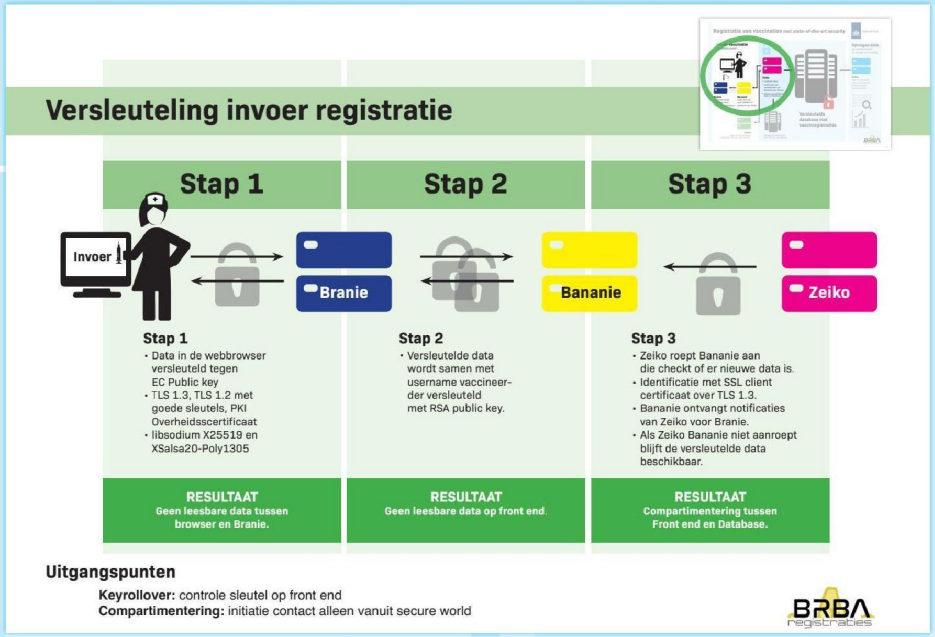
Vaccinaties worden geregistreerd via de webbrowser of via datasystemen zoals GGD CoronIT.

Directe invoer op de vaccinatielocatie:

De data wordt ingevoerd in de webbrowser, die praat 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 komt versleuteld binnen en wordt door Branie verder versleuteld samen met metadata zoals de accountgegevens van de invoerder. Vervolgens wordt 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 is en neemt deze af voor validatie. De gebruiker krijgt een notificatie van het resultaat van de validatie, die wordt verzonden via Bananie



en Branie. De gebruiker kan via een versleutelde notificatie de eigen vaccinaties terugzien.

Overname van data uit een derde systeem:

Hiero maakt een veilige verbinding met de dataleverancier en haalt de data op. Na controle wordt deze versleuteld en

klaargezet voor validatie door Zeiko. Het is een automatisch systeem met een volledige audit trail voor de dataleverancier.

Indien de data niet gevalideerd kan worden blijft deze versleuteld op Hiero beschikbaar tot het probleem kan worden herleid.

Vervolg ontwerp en functie

Validatie:
De door Bananie en Hiero aangereikte data wordt door Zeiko uitgepakt en gevalideerd tegen de beschikbare gegevenskoppelingen (BRP, vaccindata). Als de validatie van de data succesvol is wordt deze versleuteld opgeslagen in de database. Zeiko heeft alleen schrijf-rechten op de database en kan alleen informatie toevoegen maar niet uitlezen. Er is sprake van volledige compartimen-tering, tot het uiterste doorgevoerd.

Database:
De database is versleuteld, 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 bij het dataformaat van CIMS en levert de informatie die nodig is voor de logistieke en beleidsmatige vragen van het RIVM.

Keiko levert vanuit BRBA registraties minimaal de volgende informatie:

- aantal vaccinaties per doelgroep, per leeftijd, per woonplaats, per regio, per geslacht
- hoeveel mensen wel NAW / geen NAW geregistreerd in de database t.o.v. aantal vaccinaties
- aantal vaccinaties per batch en locatie (voor logistiek)
- tracering personen per vaccinbatch
- gegevens naar RIVM vaccinregistratiedatabase

Gebruikerservaring

Account aanmaken

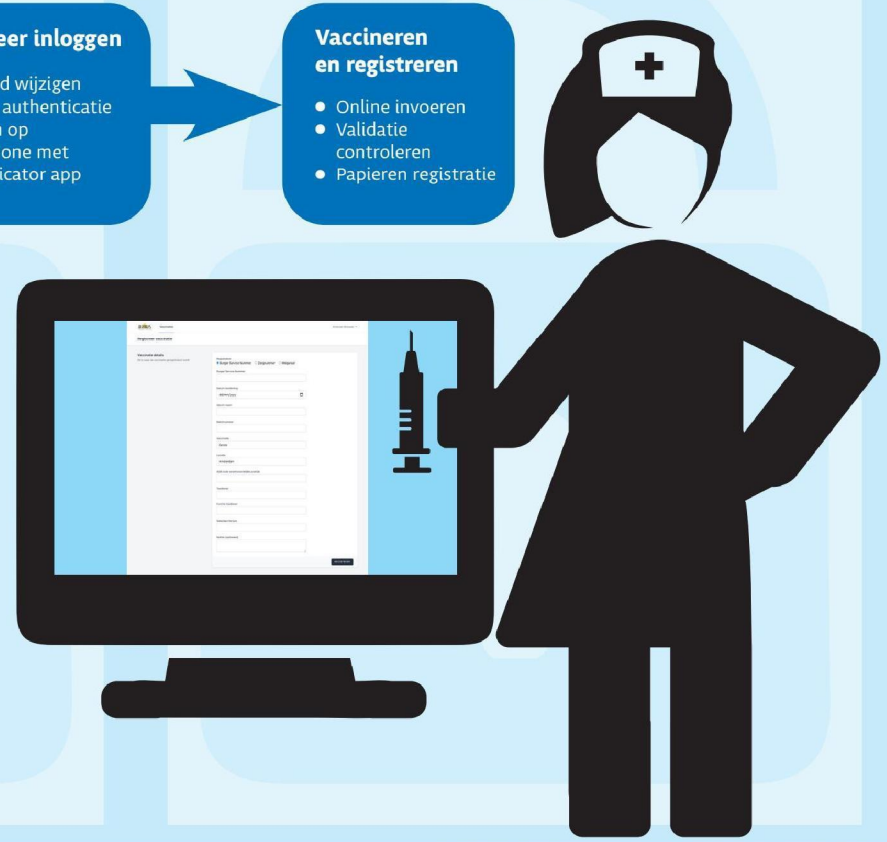
- Door locatie verantwoordelijke
- Bevoegdheid gecontroleerd
- Password, 2FA QR code op papier

Eerste keer inloggen

- Password wijzigen
- 2-factor authenticatie instellen op smartphone met Authenticator app

Vaccineren en registreren

- Online invoeren
- Validatie controleren
- Papieren registratie



BRBA registraties werkt met een invulformulier in een recente browser, waardoor het voor iedereen een herkenbare invulomgeving is. Iedereen die vaccins prikt is hiervoor bevoegd, maar het invullen zal vaak door een ondersteuner gedaan worden. Dit is zo eenvoudig mogelijk gemaakt. Met deze aantallen telt elke vereenvoudiging. Eenmaal ingelogd is ook de ingevoerde informatie terug te kijken.

De medische verantwoordelijke van een locatie is verantwoordelijk voor de accounts voor de mensen die de vaccins invoeren. Inloggen gaat met 2-factor authenticatie. Naast goede documentatie is de helpdesk beschikbaar om te helpen met het instellen van de accounts en de 2-factor authenticatie.

De documentatie is vanaf 4 januari beschikbaar.

Securityconcept op hoofdlijnen

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.
- Public key / asymmetrische encryptie op meerdere lagen.
- Hardware Security Module (HSM) voor sleutelbeveiliging.
- SOC/SIEM, waardoor aanvallen snel worden opgemerkt en gehandeld wordt.
- Threat Hunting, er wordt pro-actief gezocht naar aanvallen.
- Hosting geschikt voor medische gegevens.
- Gebruik van moderne ontwikkelmethodes. Herhaalde codereview.
- Uitgangspunt is geen dataverlies, zowel in de software als door beheermaatregelen.
- Backups off-site, contingency en recovery plan.

Conclusie beveiligingsanalyse

5.1.2e **van Secundity heeft het team begeleidt 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 indien nodig op 4 januari 2020 de eerste vaccinatie te registreren.**