PROJECT BRBA Registraties – Beveiligde Registratie Bijzondere Assets:
REGISTRATIE VAN VACCINATIE MET STATE-OF-THE-ART SECURITY

Documentatie
Versie: 21-0.02
Datum: 02-01-2021
Status: Vertrouwelijk – TLP/Amber

Versies

21-0.02	02-01-2021	Minor edits
21-0.01	01-01-2021	Nieuwe netwerktekeningen, nieuwe grondslag
0.8	31-12-2020	Minor edits
0.7	30-12-2020	Update na opschalen project
0.6	27-12-2020	Conclusie beveiligingsanalyse toegevoegd
0.5	27-12-2020	Pre final commented
		vorige versies…

Inhoudsopgave

1. Aanleiding en uitgangspunten

Het project BRBA registraties 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.

Het systeem is voorzien voor die zorgverleners die niet op een digitaal systeem zijn aangesloten en als flexibele intermediair tussen de locatie van vaccinatie en het RIVM in het geval dit nodig is ('Plan B').

Aanleiding

Toen in het nieuws kwam dat er risico's waren bij de voortgang van de vaccinatiecampagne vanwege de noodzaak tot registratie 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.

Het team is betrokken bij de bestrijding van COVID19 en wil met 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

BRBA registraties is gebouwd naar de actuele standaard van de industrie en overheid. Net als bij de Coronamelder en GGD Contact app vormen privacy & security by default de kern. Dat leidt tot de volgende uitgangspunten:

- **Werkbaar** is een systeem dat eenvoudig te gebruiken is, geschikt voor mensen die niet in de IT werken en waar met enige snelheid gegevens kunnen worden ingevoerd en verwerkt. Het systeem moet niet de bottleneck worden bij de opschaling van de vaccinaties.

- **Veilig** is een systeem dat geschikt is voor de omgang met medische gegevens en met persoonsgegevens, volgens de laatste stand van de techniek en randvoorwaarden vanuit de overheid (zoals de BIO 2019). BRBA registraties biedt een veilige gecompartimenteerde workflow met separation-of-concerns van vaccineerder tot en met de database, door in iedere stap te zorgen voor veilige overdracht en opslag van data.

- **Flexibel** is een systeem dat eenvoudig kan worden aangepast aan de dynamische praktijk. Door de eenvoudige opzet biedt BRBA registraties robuuste architectuur en

communicatie-infrastructuur en een stevige database voor de opslag van de gegevens, die eenvoudig aanpasbaar is aan de ontwikkelingen rondom de vaccinatie.

- **Inzichtelijk** is het systeem met goede monitoring en metrics, afhankelijk van wat nodig is. Er wordt een eenvoudig dashboard ontwikkeld dat met name de prestaties en status van het systeem zelf weergeeft, zodat goed te zien is of alles werkt.

- **Gebruiksvriendelijk**, maar alleen voor die mensen die er wat te zoeken hebben. Keiko zet de data klaar in een formaat dat past bij CIMS van het RIVM, zodat samenwerking in de keten op een goede en geautoriseerde manier kan plaatsvinden.

- **Interoperabel** is een systeem dat kan communiceren met de belangrijkste dataleveranciers en het RIVM.

- **Beheer** is eenvoudig, want het systeem moet tijdens de gehele looptijd van de vaccinatiecampagne functioneren. Het ontwikkelteam zorgt dat het systeem functioneert en draagt na verloop van tijd het beheer over aan de lijnorganisatie.

Team

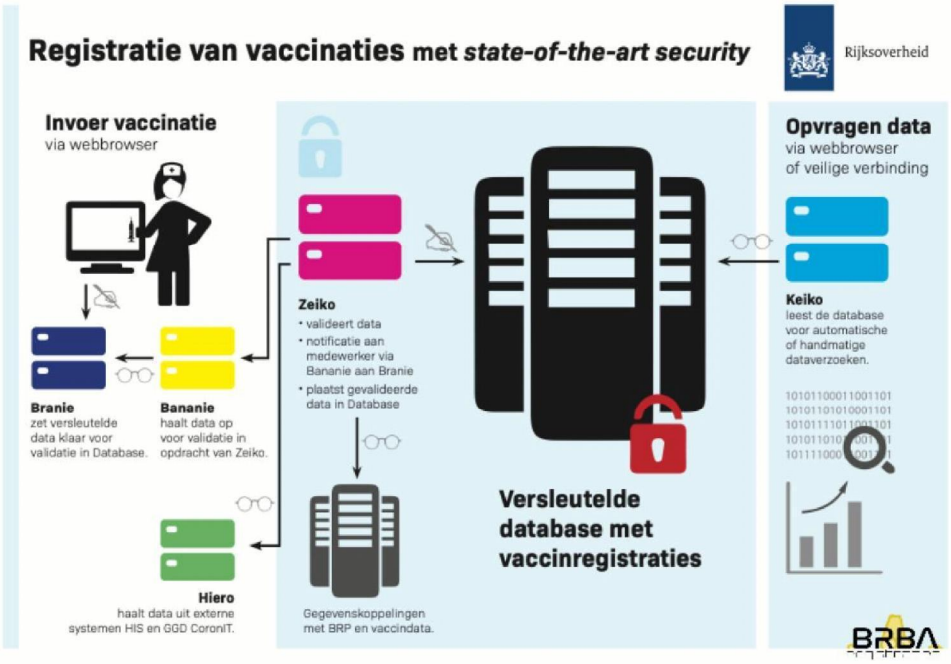
Het team dat aan BRBA registraties werkt valt onder projectleiding vanuit VWS en bestaat uit de volgende personen:

5.1.2e	Projectleiding, CSPO
5.1.2e	Projectleider uitrol
5.1.2e	lead ontwikkelaar
5.1.2e	cryptoarchitect
5.1.2e	requirements & documentatie
5.1.2e	softwareontwikkelaar
5.1.2e	softwareontwikkelaar
5.1.2e	CTO
5.1.2e	softwareontwikkelaar
5.1.2e	softwareontwikkelaar
5.1.2e	CI/CD
5.1.2e	databaseontwikkelaar en beheer
5.1.2e	databaseontwikkelaar en beheer
5.1.2e	uitrol
5.1.2e	DPIA
5.1.2e	onafhankelijk security tester

5.1.2e heeft als onafhankelijk security tester vanaf het begin bijgedragen.

2. Uitwerking op hoofdlijnen

BRBA registraties is opgezet met security als uitgangspunt. In onderstaande afbeelding is het ontwerp schetsmatig uitgewerkt, waardoor snel een overzicht verkregen wordt van de werking van het systeem.



De data wordt ingevoerd in de webbrowser, die praat met het frontend. Dit bestaat uit twee componenten, Branie en Bananie. 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. De door Bananie aangereikte data wordt uitgepakt en gevalideerd tegen de beschikbare gegevenskoppelingen (BRP, vaccindata). De gebruiker krijgt een notificatie van het resultaat van de validatie, die wordt verzonden via Bananie en Branie.

Als de validatie van de data succesvol is wordt deze versleuteld opgeslagen in de database. Zeiko heeft alleen schrijfrechten op de database en kan alleen informatie toevoegen maar niet uitlezen. Er is sprake van volledige compartimentering, tot het uiterste doorgevoerd.

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.

Keiko heeft toegang tot de database en kan automatische rapportages en handmatige informatieverzoeken verzorgen. Na autorisatie is Keiko raadpleegbaar voor vragen als 'hoeveel mensen hebben de eerste prik gehad', 'hoeveel vaccins zijn geregistreerd vanuit Batch YXZ' etc. Dankzij de automatische koppeling met het RIVM komt de data in het CIMS systeem, maar het is ook mogelijk om directe queries te specificeren.

Hiero is een mogelijkheid voor een aparte data ingang naar Zeiko met validatie voor externe gegevensbronnen, die wordt gerealiseerd en ingezet indien dit noodzakelijk is. Er zijn contacten gelegd om de data uit GGD CoronIT ook benaderbaar te maken, zodat de verbinding klaarligt mocht deze ingezet moeten worden.

3. Gebruikerservaring: hoe werkt het registreren?

De gebruikerservaring staat los van de communicatie-infrastructuur en de opslag van de data en is flexibel: wensen kunnen redelijk eenvoudig worden gerealiseerd. Deze uitleg geeft een beeld te geven van de stappen die doorlopen worden om de data vanaf de locatie waar gevaccineerd wordt naar het RIVM te krijgen.

Figuur 1 - Account en inlogprocedure

Gebruikers

In de uitvoerende organisatie zijn er twee typen gebruikers:

- *Gebruiker type registrant*

Dit is de beoogde eindgebruikers groep. Zij voeren registratie van de vaccinatie in. De invoer is conform richtlijnen van RIVM en VWS. De registrator en de vaccineerder zijn gescheiden

zodat de invoer ook - onder medische verantwoordelijkheid - door een administratieve kracht gedaan kan worden.

- *Gebruiker type administrator / locatie verantwoordelijke*

Dit gebruiker type kan *alleen* nieuwe accounts aanmaken voor de registrant/vaccineerder. Het aanmaken is gekoppeld aan de bevoegdheid om te vaccineren, de procedure is opgenomen in 'Encryptie: opzet en uitwerking' in dit document.

Accounts en inloggen

Iedereen die vaccineert is hiervoor bevoegd volgens de RVP-richtlijn Deskundigheid. Binnen de uitvoerende organisatie wordt een verantwoordelijke aangesteld die de accounts voor de vaccinerenden aanmaakt en bewaakt, gekoppeld aan de controle op de bevoegdheid. De procedure hiervoor is uitgewerkt in 'Encryptie: opzet en uitwerking' in dit document.

De registrator logt in op de account, bevestigt de inlog via de 2-factor authenticatie. Na het inloggen kan direct begonnen worden met registratie van gevaccineerde personen. Na 2 uur van inactiviteit wordt de registrator vanzelf uitgelogd.

User management is een essentieel onderdeel van de beveiliging van het systeem, wordt gekoppeld aan de bevoegdheid om de 'voorbehouden handeling' van het prikken uit te voeren en vereist 2-factor authenticatie.

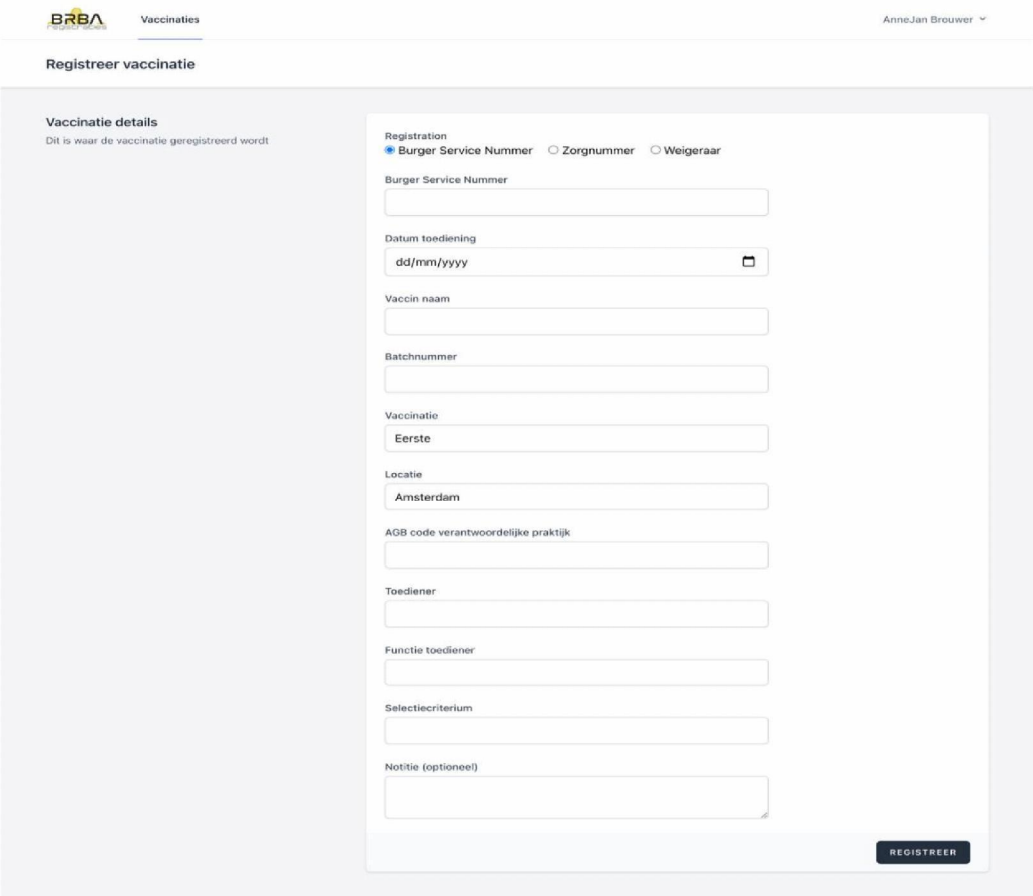
Naast goede documentatie is de helpdesk beschikbaar om te helpen met het instellen van de accounts en de 2-factor authenticatie. De documentatie is vanaf 4 januari beschikbaar.

Registratie

Na het inloggen komt de registrator in het registratiescherm. Hier kunnen de gegevens van de gevaccineerde worden geregistreerd. Voor zover data via een gegevenskoppeling kan worden opgevraagd wordt dat – verderop in het systeem – gedaan. Alle informatie die niet hoeft te worden ingevuld is voor de doorloopsnelheid van het vaccineren meegenomen.

Het systeem volgt bij de registratie de hiervoor geldende richtlijnen (RIVM, CIMS). Het onderstaande screenshot is gebaseerd op de 'proof of concept' in de testomgeving. In een volgende stap van de ontwikkeling worden de juiste normen geïmplementeerd. Het systeem is gebouwd om hier flexibel mee om te gaan.
Indien een cliënt geen BSN heeft kan in het systeem een aparte pagina worden opgeroepen waar de NAW-gegevens en eventuele andere identifiers zoals een zorgnummer of paspoortnummer van een ander land kunnen worden opgenomen. Er wordt gewerkt aan validatie op basis van BSN zoals in de zorg gebruikelijk is.

Pragmatisme is essentieel bij deze diverse groep zonder BSN, die gaat van diplomaten naar vluchtelingen en daklozen. Belangrijk is dat als het nodig is de mensen die een bepaalde batch vaccins gekregen hebben traceerbaar zijn, voor zover ze toestemming hebben gegeven om deze informatie te delen.



Validatie

De ingevoerde data wordt via het systeem gecontroleerd. Dit gebeurt in de ‘secure world’ door Harrie-5 zeiko. Hier wordt de data getoetst via de gegevenskoppelingen met relevantie gegevensbronnen en het resultaat wordt met een notificatie teruggekoppeld naar het registratiescherm.

De gevalideerde dataset wordt toegevoegd aan de database. Indien er problemen zijn worden deze in een notificatie toegelicht. In het screenshot is een notificatie na een gevalideerde registratie te zien.

Een niet gevalideerde invoer moet worden gecorrigeerd. De registrator krijgt een uitgebreide foutmelding die aangeeft welke velden niet gevalideerd konden worden. Mocht

de validatie niet direct kunnen plaatsvinden dan blijven de gegevens behouden en worden ze later afgehandeld.

Papieren wereld

De papieren registratie blijft bestaan. In de bijlage bij deze documentatie is een concept voor een formulier opgenomen waarop altijd de belangrijkste gegevens van de vaccinatie genoteerd worden. Er is een korte en een lange registratie, de bovenste en de onderste helft van het formulier. Indien het systeem om wat voor reden dan ook niet toegankelijk is (geen internet, werkstation kapot etc.) en de vaccinaties doorgaan kan op het formulier de volledige informatie van de cliënt worden genoteerd zodat dit achteraf alsnog in te voeren is.

4. Gebruikerservaring: Toegang door RIVM

Via een webbrowser kan contact gemaakt worden met Keiko die de interface biedt voor geautoriseerde gebruikers om toegang tot de data te krijgen.

Geautomatiseerde data wordt afgeleverd op de servers van het RIVM via een sftp verbinding met keys, geencrypt tegen een x509 certificaat. Dit gaat in eerste instantie om meta-data, aantallen gevaccineerden etc. die gebruikt kunnen worden om de vaccinatiecampagne te monitoren. De data sluit aan bij CIMS zodat het voor het RIVM optimaal in de bestaande systemen past.

Handmatige database query's kunnen ook worden gedaan. Bijvoorbeeld een overzicht van welke personen het vaccin uit een bepaalde batch hebben gekregen. Dit soort handmatige verzoeken hebben een extra goedkeuring nodig van de verantwoordelijke binnen het RIVM.

Alle personen binnen het RIVM die handmatige verzoeken kunnen doen krijgen een individueel account zodat gedane verzoeken traceerbaar zijn. De verzoeken worden door de verantwoordelijke binnen het RIVM aangemaakt en op naam van de betreffende medewerker uitgevoerd conform het proces beschreven in het RIVM Handboek Informatiebeveiliging. Accounts worden – net als bij de invoer – met 2-factor authenticatie beveiligd. Processen worden ingericht volgens BIO 2019.

5. Status

Status en tijdlijn

De proof of concept staat, de organisatie is opgeschaald, de afhankelijkheden zijn in beeld en worden opgelost.

- Het ontwikkelpad de komende dagen:
  - Door ontwikkelen proof of concept, parallel pentesten om te zien of alles klopt
  - Opstarten infrastructuur
  - Koppeling met externe gegevensbronnen ten behoeve van de validatie

- Uitwerken documentatie en overleg met relevante partijen (onder andere dit document).

- Het project werkt met de volgende planning:

  - *4 januari:* Het systeem draait zo goed als volledig, kan op grotere schaal getest worden, de helpdesk en de uitvoerende organisaties kunnen getraind worden op usermanagement en het gebruik van het registratiesysteem.

  - *8 januari*: Start van de vaccinatiecampagne.

Afhankelijkheden

Een project als BRBA registraties is inherent afhankelijk van de partijen waarmee wordt gecommuniceerd. Daarbij is sprake van schuivende panelen met betrekking tot de invulling en opdracht die voor het project geldt. Dat sluit aan bij de doelstelling van BRBA registraties als Plan B.

De onafhankelijkheid van BRBA registraties maakt dat we zo snel kunnen groeien en dat er straks een operationeel systeem staat dat kan communiceren met andere partijen. Dit is een gevolg van ontwerpkeuzes: een modulaire opbouw en een heldere keuze om datgene te doen waar het project voor is: registreren, veilig opslaan en doorgeven aan de partij die de gegevens rechtmatig gebruikt.

De belangrijkste afhankelijkheden zien er als volgt uit:

Infra en hosting

De infrastructuur voor BRBA registraties wordt opgebouwd en ondergebracht bij een gekwalificeerde hoster die in staat is om op deze korte deadlines in te spelen. Dit is gelukt en we zijn op korte termijn 'live' in een staging omgeving die een 100% kopie is van de uiteindelijke productieomgeving.

Externe organisaties, validatie en data overdracht

Een aantal verbindingen weten we nu al en zijn work-in-progress. Door de dynamiek van de situatie kan dit overzicht veranderen. De inzet is datgene mogelijk maken wat voor een goede registratie nodig is.

1. Het certificaat voor de validatie van BSN nummers; de procedure voor de aanvraag is in beeld en we hebben een uitzondering kunnen bedingen waardoor we gebruik kunnen maken van de uiterst praktische 'zorgtoegang' SVB-Z met UZI servercertificaat. Hiervoor moeten we het RIVM mee hebben, dit loopt. Als dit klapt is er nog plan b en plan c. De Rijksdienst voor Identiteitsgegevens heeft RIVM een 'all clear' gegeven voor deze toepassing, dat is een scenario en koppeling via een gemeente kan ook maar is niet zo fraai.

2. Koppeling met het RIVM kan via hun CIMS ingang. Onze oplossing om hier met audit trail op aan te sluiten is dat ze een x509 certificaat aanmaken waartegen we de data versleutelen. Dit is work in progress via 5.1.2e van het shared service centre.

3. GGD GHOR heeft een dataplatform waar we mee kunnen koppelen. Dit zal met een VPN verbinding gebeuren, de uiteindelijke datakoppeling liefst met een API. Gesprekken met 5.1.2e lopen.

6. Infrastructuur

Hosting en infrastructuur

Het uitgangspunt is dat de IT-infrastructuur niet de beperkende factor moet zijn voor de snelheid van het vaccineren. De infrastructuur waar BRBA registraties op draait is een kopie van de infrastructuur voor de GGD Contact app met enkele wijzigingen. Deze is getest, schaalbaar voor grotere aantallen en heeft zich bewezen. De hoster is voldoet aan de eisen die gesteld worden voor deze toepassing.

Voorzieningen op de werkplek

Ter plaatse geldt dat er voor elke registrant een apparaat met een webbrowser beschikbaar moet zijn en een eigen telefoon voor de 2-factor authenticatie. De internetverbinding hoeft niet buitengewoon te zijn: het is een lichte website en er wordt relatief weinig data verzonden. De accounts kunnen worden verstrekt op een normale kantoorwerkplek met een printer.

7. Helpdesk

De helpdesk voor Coronamelder en GGD Contact wordt opgeschaald voor BRBA registraties. Er is een 088-nummer beschikbaar en de helpdesk is capabel om de meerderheid van de vragen te beantwoorden.

BRBA registraties levert informatie aan over UI, documentatie van het systeem en helpt de helpdesk met de belangrijkste issues die we verwachten:

- Accounts aanmaken, beheren
- 2-factor authenticatie instellen
- Vaccinaties invoeren
- Data validatie door het systeem en hoe ermee om te gaan
- Problemen met heel erg oude browsers

Zo schat de helpdesk zichzelf in: “Basis vragen zijn goed te beantwoorden, wordt het heel ingewikkeld dan graag hulp. Graag een team sessie met de mensen die het gaan doen om het systeem uit te leggen, lekker praktisch.”

Tenzij er grote verschuivingen in de functie van BRBA registraties komen kan de helpdesk rustig aan 'groeien' en merken we stapje bij beetje welke vragen er zijn.

8. Training en e-Learning

De NSPOH (Netherlands School of Public & Occupational Health) maakt tussen 1 en 4 januari op basis van de UI en projectdocumentatie de trainingen en e-Learning voor het gebruik van het systeem. Hiermee kunnen zowel de helpdesk als registranten en administratoren het systeem gebruiken.

Het systeem is eenvoudig om te gebruiken maar met name het usermanagement en de goede omgang met data en de validatie vragen om deze ondersteuning.

9. Securityconcept op hoofdlijnen

Mitigerende maatregelen

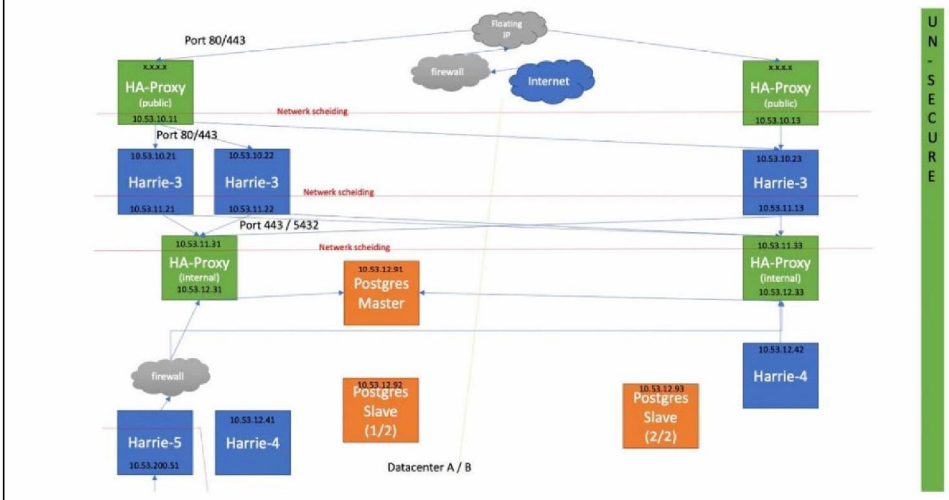
De mitigerende maatregelen worden in dit document verder uitgewerkt, maar zijn puntsgewijs als volgt te omschrijven:

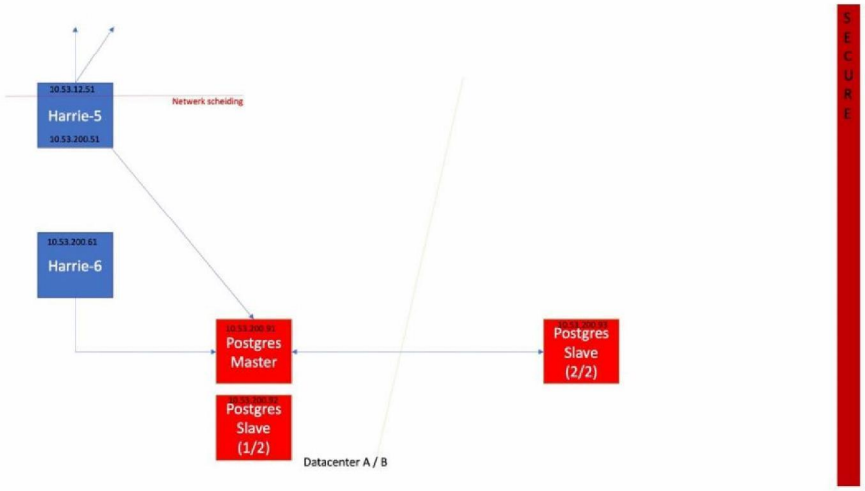
- Security & privacy by design.
- Sterke functiescheiding. Alleen invoer via de frontend, 'one way'. Er kan niet worden gemuteerd of worden teruggelezen.
- Public key / asymmetrische encryptie op meerdere lagen, waarbij de private keys niet aanwezig zijn.
- Hardware Security Module (HSM) om sleutels aanvullende te beveiligen[1].
- Continue bewaking op beheerniveau van de systemen. Hierdoor worden aanvallen snel en efficient ontdekt.
- SOC/SIEM, waardoor aanvallen snel worden opgemerkt en gehandeld wordt.
- Threat Hunting, er wordt pro-actief gezocht naar aanvallen.
- De hostende partij levert beheersdiensten en beschikt over certificeringen waaruit kwaliteitsmanagement en een niveau van beveiliging blijkt. Concreet betekent dat er sprake is van goede beheersprocessen. De auditor die deze certificering heeft afgegeven doet regelmatig werkzaamheden voor ZBO's en voor het Rijk (in het bijzonder het Ministerie van Volksgezondheid, Welzijn en Sport). Dit zijn ISO 27001, ISO 20000, ISO 9001 en ISO 14001 alsmede NEN 7510 (voor de zorg), ISAE3402 type II, SOC2 en DigiD TPM.
- Gebruik van moderne ontwikkelmethodes. Herhaalde codereview.
- Iedere component heeft andere beheersrollen, waardoor de mogelijkheden van misbruik enorm worden beperkt.
- Uitgangspunt is geen dataverlies, zowel in de software als door beheermaatregelen.
- Backups off-site, contingency en recovery plan.

[1] Waar mogelijk en noodzakelijk. Zo zal bijvoorbeeld de publieke (niet geheime) sleutel in de browser niet zo beschermd worden.

Technisch ontwerp

Het technisch ontwerp wat als basis dient voor de bouw van het systeem wordt steeds verder uitgewerkt. De basis is opgenomen in de eerste illustratie, de uitwerking van een deel van het systeem in de tweede.





In de basis wordt er:

- In de secure world een keypair aangemaakt voor EC encryptie.
- Een keypair aangemaakt voor RSA encryptie.
- Een secret voor gebruik binnen harrie-3 branie en harrie-4 bananie ten bate van database encryptie.
- Een secret voor gebruik binnen harrie-5 zeiko en harrie-6 keiko ten bate van database encryptie.

- *Insecure world (Front-end)*

- **Harrie-3 branie**
  Alle data die door de webbrowser verzonden wordt is encrypted tegen een EC public key[2]. Op de frontend (harrie-3 branie) PHP wordt deze data samen met extra data (username) ingepakt met de RSA public key. Hiermee is de data op de frontend niet meer leesbaar aanwezig en heeft de frontend nooit de inhoudelijke data met bijzondere persoonsgegevens in leesbare vorm ontvangen.

  Op de webserver voor harrie-3 branie is alleen TLS 1.2 met goede versleuteling en TLS 1.3 toegestaan. Hier wordt een PKI Overheidscertificaat gebruikt.

- **Harrie-4 bananie**
  Er is een apart proces (harrie-4 bananie) dat de data ophaalt vanuit de database waar harrie-3 branie deze encrypted en dubbel encrypted gegevens heeft opgeslagen. Deze API kan alleen vanaf harrie-5 zeiko worden aangeroepen, identificatie gaat met SSL client certificaat over TLS 1.3. Ook kan harrie-4 bananie notificaties ontvangen en deze klaarzetten voor gebruik en tonen door harrie-3 branie. Als harrie-5 harrie-4 niet aanroept blijft de data beschikbaar, tot deze gevalideerd of afgewezen is.

- *Secure world (Back-end)*

- **Harrie-5 zeiko**
  In de secure world draait harrie-5 zeiko. Deze haalt de gegevens op vanaf harrie-4 bananie met een X.509 client certificaat en verwerkt deze. Deze service heeft dus toegang tot de private RSA en private-EC key. Hier wordt de data gevalideerd op geldigheid en foutieve invoer. Bij problemen wordt er een notificatie terug gestuurd via harrie-4 bananie naar de vaccineerder die op/in harrie-3 branie werkt.

- **Harrie-6 keiko**
  Harry 6 keiko heeft toegang tot de database en kan daar verwerking (statistieken en andere vragen) op uitvoeren. Aangezien alle data in de database versleuteld is, is het niet mogelijk om in de database op velden te zoeken. Daarom zal bij het opstarten een index van velden worden opgebouwd en deze zal worden opgeslagen in een

[2] Industry best pratice 2Factor Authentication, standards compliant (RFC4226/6238) en industry best practice Password-Based Key Derivation Function voor de wachtworden 'salted/hashed.

redis memory-only database. De connecties met de datatabase zullen via TLS verlopen; met digitale certificaten aan beide zijden.

- *Techniek*
  Industry best practice technologie, conform of beter dan de relevatie regelgeving en vingerende versie van het EU/ENISA: Algorithms- Key Sizes and Parameters Recommendations:

- **Database encryptie: libsodium met secretbox**
  XSalsa20 stream cipher Poly1305 MAC https://libsodium.gitbook.io/doc/secret-key_cryptography/secretbox

- **EC encryptie: libsodium sealed boxes**
  XSalsa20 stream cipher Poly1305 MAC https://libsodium.gitbook.io/doc/public-key_cryptography/sealed_boxes

- **RSA encryptie: Op dit moment GPG, moet worden S/MIME.**
  met s/MIME: RSA 4096 bits keylength, AES256

- **TLS verbinding**
  TLS 1.2/1.3
  EECDH+ECDSA+AESGCM:EECDH+aRSA+AESGCM:!SHA:!RC4:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!SRP:!DSS

- **Certificaat**
  Bij oplevering PKI-Overheid EV.

- **HSM**
  Het is procestechnisch mogelijk om de RSA encryptie in de HSM te laten plaatsvinden. Helaas lukt dit niet voor Q1 2021 met de libsodium keys indien er gekozen wordt voor een utimaco HSM. Het is mogelijk dat er overgeschakeld moet worden naar EC (curve25519) met AES.

10. Koppeling met externe gegevensbronnen

De koppeling met externe gegevensbronnen ten behoeve van de validatie door Harrie-5 zeiko wordt toegevoegd als bekend is welke mogelijkheden hiervoor zijn. Te denken valt aan BPR, vaccin data (welke batches).

De validatie tegen het BRP en de vaccindata is niet essentieel voor het project, maar wel een goede manier om de kwaliteit van de data te waarborgen. Voor de validatie tegen het BRP kan gebruik gemaakt worden van de gegevenskoppeling die via SBV-Z wordt aangeboden.

11. Encryptie: opzet en uitwerking

Het uitgangspunt is dat BRBA registraties inherent veilig moet zijn, voorzien van 'state-of-the-art' beveiliging. Dit is normaal voor software die omgaat met bijzondere persoonsgegevens, maar niet vanzelfsprekend. Het securityconcept sluit aan bij het ontwerpoverzicht dat in de tweede paragraaf uitwerking op hoofdlijnen wordt genoemd.

Definities

- *Authenticatie:* Bewijzen van identiteit
- *Insecure world:* Applicatiedeel dat vanaf "publiek" bereikbaar is
- *Secure world:* Applicatiedeel dat zeer beperkt bereikbaar is
- *Authenticator:* google authenticator of een vergelijkbare app

Uitgifte wachtwoorden en 2FA

- *2FA Techniek*

Het project volgt industry best practice 2FA standaard TOTP (RFC6238)
Hiermee kan door een gebruiker op een veilige manier geauthenticeerd worden.
Uit beperkingen die in authenticator zitten is het slechts mogelijk om SHA-1 met 6 cijfers als code uit te rollen. Aangezien codes slechts 30 seconden geldig zijn is dit meer dan voldoende om te voldoen aan de huidige standaarden die vereist zijn voor 2FA.

- *Aanmaken gebruiker*

Beheerders kunnen gebruikers aanmaken door het invullen van een emailadres en een volledige naam.
Hierna wordt het wachtwoord geprint zodat deze aan de gebruiker meegegeven kan worden.
Ook wordt er een QR-code getoont die de gebruiker dient te scannen met de authenticator. Nadat deze gescand is dient de huidige getoonde code in authenticator te worden ingevoerd. Is dit succesvol dan is de gebruiker aangemaakt en kan de gebruiker vanaf dan inloggen.

- *Lengte en tekenset wachtwoord*

Aangezien het wachtwoord met een duidelijk font geprint kan worden is het niet nodig om een andere beperking dan de standaard ascii tekenset (US-keyboard) aan te houden.
Voor de lengte van het wachtwoord is het noodzakelijk om dit niet te lang om in te typen te maken maar ook niet te kort dat het te makkelijk te raden zou zijn.
Het is daarom aangeraden om het wachtwoord tussen de 10 en 13 tekens te maken. De lengte van het wachtwoord varieeren geeft ook entropie en maakt het gokken van het wachtwoord door een aanvaller nog moeilijk.

- *Datatransport beveiliging*

Het datatransport dient versleuteld zijn met HTTPS TLS 1.3 en TLS 1.2 met de juiste ciphers en Perfect Fofward Secrecy (of soortgelijk – dus dat een key compromise op dag 10 niet leidt tot confidentialiteit verlies van dag 1-9). Op de test van Qualys SSL Lab zal een A+ gehaald dienen te worden. Hiernaast zal aan de eisen van de BIO voldaan moeten worden.
Uit privacy- en security-overwegingen volstaat het niet data slechts op transport-niveau te versleutelen. Op de de endpoint van de bovengenoemde TLS verbinding mag de data

niet leesbaar aanwezig zijn. Dit zorgt ervoor at er een gesplitste backend is en daardoor er defense-in-depth ontstaat.

Encryptie lagen

- *Client side*

Op de client wordt de data voor verzending versleuteld met libsodium X25519 en XSalsa20-Poly1305 Daarna wordt dit verzonden via een TLS1.3 (of 1.2 met goede ciphers) verbinding naar de webserver.

- *Frontend side*

Op de frontend (de ontvangende webserver) worden de aangekomen berichten niet ontsleuteld, maar slechts voorzien van meer metadata zoals welke gebruiker dit heeft aangeleverd en daarna ingepakt in op basis van een RSA public key en opgeslagen voor verdere verwerking binnen de secure world.

- *Database storage*

Data die wordt opgeslagen in de database wordt encrypted met XSalsa20 en Poly1305 MAC te authenticatie.

- *Disk encryption*

Disk encryptie zal plaatsvinden met een BIO conform proces en eisen.

- *Keyrollover*

Ten bate van keyrollover wordt er op de frontend gecontroleerd of de sleutel waartegen de opgestuurde data is versleuteld. Indien er een nieuwe sleutel is wordt het bericht afgekeurd en zal dit opnieuw verzonden moeten worden. Op de webserver van de frontend is het laden van een nieuwe RSA sleutel een technisch eenvoudig proces. (configuratie). Ten bate van identificatie wordt voor elk bericht en elk dataveld opgeslagen met welke sleutelID's deze zijn versleuteld.

- *Serverside*

De opslag op de server vindt plaats in een SQL database en in een in-memory redis database.
Op de database en applicatie servers zal encryption-at-rest (harddisk versleuteling) worden toegepast met een encryptie en sleutelbeheer conform BIO.
In de redis memory database worden de shared-secrets opgeslagen zodat deze door de applicatie te raadplegen zijn.
In de SQL database zal op alle velden die privacy gevoelige informatie bevatten versleuting worden toegepast door de applicatie. De versleuteling is op basis van een XSalsa20-Poly1305 stream.
De sleutels voor de database encryptie zullen worden opgeslagen op de HSM.
Gezien de data per veld apart encrypted is opgeslagen kan er zonder problemen via de normale gangbare beheersprocessen een backup gemaakt worden. Deze back-ups zullen versleuteld dienen te worden met een public/private encryptiemethode waarvan de private sleutel niet op de servers aanwezig is.

De decryptiesleutel voor backups zal volgens een BIO conform proces gebruikt kunnen worden indien de backups teruggezet dienen te worden.

• *Eenrichtingsverkeer*
Er is slechts vanuit de secureworld de mogelijkheid tot het initieeren van communicatie, hiermee is het niet mogelijk om de achterliggende systemen te overladen met informatieverzoeken. Terugmeldingen worden ook vanuit de secureworld geinitieerd en daarmee is er slechts vanuit 1 richting verkeersinitiatie mogelijk. Het aanvalsvlak op de achterliggende systemen is hiermee enorm verkleind aangezien er geen actieve services worden aangeboden.

• *Notificaties*
Indien er foutmeldingen over de inhoud van de data (data = incorrect) aan de gebruiker verstuurd dienen te worden wordt dit vanuit de secure world geinitieerd en aan de private beschermde API van de webserver in de insecure world aangebonden.
De website (browser) van de gebruiker controleert regelmatig of er nieuwe berichten zijn, en indien deze er zijn en het niet storend is voor het invoerproces zal deze melding worden getoont.

• *Certificaten*
Voor de backend zal gebruik moeten worden gemaakt van PKI-Overheid EV-certificaten (PKI-overheid OV bestaat niet meer, de opties zijn dus DV versus EV. DV is niet voldoende) en de app zal controle van het certificaat doen op basis van de normale (Subject) controles, CA pinning, DNS CAA records en de DNS van de backend zal DNSsec gesigneerd dienen te zijn.

Gezien de recente G3 situatie verdient het hierbij aanbeveling om, waar mogelijk, gebruik te maken van de M2M certificaten van de PKI Overheid (die beter geisioleerd zijn van het World CAB forum en de wensen van google.com).
Clients dienen zich niet te identificeren met een certificaat. De toegevoegde waarde van een certificaat is nihil gezien de inhoud al versleuteld is (zie Versleutelen verstuurde data). Terwijl dit al gauw tot een zeer hoog niveau van traceerbaarheid zou leiden – met volledig verlies van de privacy. Het registreren/ondertekenen van een client certificaat zou ook geautomatiseerd dienen te gebeuren zonder extra controles ten opzichte van de andere processen. Het dient mogelijk te zijn om 'goedkoop' vast te stellen of een binnenkomend bericht echt genoeg is om resources te vragen (dus zonder al te veel database lookups – en liefst geheel zonder (ECDHE of HMAC check)). Zodat een DDoS goedkoop kan worden afgevangen.

De overwegingen hierbij zijn:

- PKI overheid EV heeft een hele lijst met eisen waaraan voldaan dient te worden.^^3^
- CA pinning zorgt ervoor dat slechts 1 CA toegestaan is voor dit gebruik
- DNS CAA zorgt er ook voor dat er slechts de gepubliceerde CA toegestaan is (en dit kan eventueel ook onderdeel uitmaken van een pin in de app).
- DNSsec is nodig om DNS geauthenticeerd is en valse data tegen te gaan

- *Ciphers*

Indien het device het ondersteunt zal er gebruik gemaakt dienen te worden van TLS 1.3 omdat deze vele voordelen heeft ten opzichte TLS 1.2 in niet meer ondersteunde onveilige communicatiemogelijkheden. Ook bij een niet perfecte configuratie is de kans op een mogelijke niet goede encryptie zeer sterk beperkt.
Toegestane TLS strings voor communicatie:
TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384

- *Opslag tijdelijke sleutels*

Op de backend zullen de sleutels die genereerd worden op basis van random verkregen uit de HSM alleen tijdelijk in memory mogen worden opgeslagen. Dit mag in een database maar na 3 weken zullen deze sleutels vernietigd dienen te worden. Indien er hierna nog gecommuniceerd dient te worden met de client zal er een re-keying proces plaats dienen te vinden.

12. Risicoanalyse en bedreigingen voor het functioneren

De risico's ten aanzien van BRBA registraties hebben betrekking op een paar domeinen:

- *Het functioneren van het systeem zelf*

Het functioneren van het systeem zelf heeft betrekking op de kwaliteit van de software en de bestendigheid van de infrastructuur. Dit betreft niet alleen de software van BRBA registraties maar ook de kwaliteit van de computers die door de gebruikers worden ingezet.

- *Kwaliteit van de data*

De kwaliteit van de data: kloppen de gegevens, werkt de validatie, is het bruikbaar voor het doel?

- *Het lekken van data vanuit het systeem*

Datalekken vanuit het vaccinatiesysteem hebben betrekking op de bijzondere persoonsgegevens en de gegevenskoppelingen die in het systeem gebruikt worden. Het gaat om de database als geheel en om gegevens van individuen, direct maar ook via de validatie en gegevenskoppelingen.

De bedreigingen voor BRBA registraties zijn onder andere:

- Kwaadwillenden die de database proberen te bemachtigen voor spionage of financieel gewin.
- Kwaadwillenden die contactgegevens van een individu in handen proberen te krijgen.

- Activisten of vandalen die het vaccinatieproces proberen te verstoren door de werking van BRBA registraties te saboteren, bijvoorbeeld met een DDOS aanval.
- Kwaadwillenden voeren een ransomware aanval uit op de infrastructuur van BRBA registraties of proberen via spoofing of phising financieel gewin te behalen
- Beheerders of betrokkenen doen iets doms, onopzettelijk schadelijk handelen

De belangrijkste maatregelen bij deze risico's zijn:

- Ontwerp van het systeem met checks zodat aanvallen minder kans maken
- Volledig sandboxed versleutelde database; de sleutels staan op een ander systeem dus zelfs al kopieer je de hele database dan kun je er niks mee.
- Een breed scala van tests en onderzoeken uitvoeren om de kwaliteit en betrouwbaarheid van BRBA registraties vast te stellen.
- Een adequaat meldingsproces voor incidenten, kwetsbaarheden en signalen over concrete dreigingen, en richt adequate incidentrespons in.
- Communiceer open en duidelijk over het doel, het ontwerp, de werking en de beveiliging van de oplossing richting het publiek én interne betrokkenen (zoals beheerders).
- Zorg dat de betrokken partijen goed geïnformeerd zijn over BRBA registraties, zich bewust zijn van de risico's en hoe hier mee om te gaan.
- Inrichten van industry best practice DOS, DDOS bescherming, monitoring en de bijbehorende escalaties, piket diensten en aanverwante processen.

13. Security maatregelen

Om de belangrijkste risico's en bedreigingen voor BRBA registraties tegen te gaan wordt een samenspel van maatregelen ingezet. Deze maatregelen zijn vergelijkbaar met de GGD Contact app: de infrastructuur hiervan wordt opnieuw gebruikt.

Software maatregelen

- alles open source
- hiermee is het voor elke belanghebbende mogelijk om zelf de correcte werking van de software te (laten) controleren.
- code reviews vanaf moment 0 in de ontwikkeling
- De software wordt inhoudelijk beoordeeld door partijen die hierin gespecialiseerd zijn.
- pen tests vanaf moment 0 in de ontwikkeling
- De implementatie van de oplossing wordt door gespecialiseerde partijen gecontroleerd.
- Het gebruik van standaard opensource software voor encryptie en decryptie.

Hosting maatregelen

- hosting in gekwalificeerd data center
- hsm voor backing alle secret keys en random input voor key generatie

- De bovengenoemde sleutels aan de kant van de portaal worden beheerd onder controle een HSM installatie. Deze levert de waarborgen dat sleutelbeheer op een veilige manier plaatsvindt en de encryptiesleutels voorzien zijn van gewaarborgde randomness.
- injected secrets aan de server kant (geen secrets in code)
- De sleutels voor automatische communicatie, decryptie van de databasevelden en andere zaken staan niet bij de applicatie opgeslagen, maar in een apart proces wat deze bij het opstarten aanlevert aan het serverproces.
- Firewalls tussen de verschillende processen, tussen de verschillende machines. Op basis van hardware en software op meerdere lagen. Het fout configureren van 1 firewall mag niet leiden tot een kritieke situatie waarbij er toegang mogelijk zou zijn tot een proces waar men geen toegang tot zou mogen hebben.
- Er zullen van de verschillende componenten backups worden gemaakt. De uitvoerende componenten worden zo ingericht dat deze zijn gemaakt op basis van automatisch herbouwen. De database componenten zullen meerdere malen per dag worden gebackupt op een veilige wijze met encryptie.

Continu monitoring

- Threat-hunting. Het proactief en iteratief zoeken in netwerken om geavanceerde bedreigingen te detecteren die bestaande beveiligingsoplossingen (proberen) te omzeilen en deze dreigingen succesvol te isoleren. Dit wordt gedaan door middel van hypothesegericht onderzoek en onderzoek op basis van bekende aanvalsindicatoren
- Dreigingbeheer. Maatregelen voor dreigingsbeheer, zoals firewalls, inbraakdetectiesystemen (IDS), malware-sandbox en SIEM-systemen, welke doorgaans identificeren op basis van uitgevoerd onderzoek nadat er een waarschuwing is geweest voor een mogelijke bedreiging.

Passieve analyse mitigatie

- Same size payloads groot zodat er uit passief meegeluisterd verkeer niet af te leiden is of en wat voor type data er uitgewisseld wordt.
- Ghost responses zodat een hacker niet kan zien of ie met een key succes heeft
- Niet van echt te onderscheiden antwoorden voor niet echte gebruikers. Indien een niet-echte gebruiker verzoekt om informatie voor een bepaalde sleutel wordt er wel antwoord teruggegeven zodat het op passief netwerkniveau niet ontdekken is of dit correcte data is.

Actieve en passieve datasecurity

- Encryptie van gevoelige velden voordat ze de database in gaan
- Privacygevoelige velden en velden die tot herleidbaarheid van een persoon zouden kunnen leiden worden versleuteld opgeslagen.
- Sleutel rotatie op de encryptie van de gevoelige datasets zodat oude backups na verlopen van de key geldigheid niet meer te ontsleutelen zijn

- At rest encryptie van secrets, data en logging. Hiermee wordt voorkomen dat als er andere processen falen (backups, schijven, toewijzingen van datablokken) er geen toegang tot de data mogelijk is.
- Versleutelde backups. Backups worden versleuteld opgeslagen. Dit op een manier zodat de backups alleen terug te halen zijn door geautoriseerde personen en alleen op expliciete opdracht.

14. Beveiligingsanalyse

5.1.2e van Secundity heeft het team tijdens de eerste fase begeleidt als security tester en een eerste beveiligingsanalyse gedaan 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 (alle hens aan dek), dan is het ambitieus, maar wel haalbaar om via het ontwikkelde portaal veilig vaccinatieregistraties mogelijk te maken op 8 januari 2021."

Vanaf 29 december is 5.1.2e aan het team verbonden en doet een doorlopende beveiligingsanalyse.

15. Privacy maatregelen

Uit de bespreking van het systeem met het NCSC en het NBV kwamen een aantal privacy / AvG gerelateerde vragen naar voren. Privacy is allereerst gediend met een veilig systeem dat niet overal datasporen trekt. Een Data Protection Impact Assesment wordt gemaakt door het RIVM in samenwerking met de landsadvocaat onder regie van professor 5.1.2e 5.1.2e

Hoewel het niet het domein is van het project nemen we de vragen hier over, omdat het zo verbonden is met de inzet van het projectteam. Een aantal vragen:

- *Hoe wordt gegeven toestemming aangetoond?*

Hiervoor zijn meerdere methodieken denkbaar. De landsadvocaat geeft nu aan dat het denkbaar is dat deze toestemming mondeling wordt gegeven. Het geven van toestemming gebeurt in principe aan de verwerkingsverantwoordelijke, die ook de vaccinatie toedient.

- *Wat als deze toestemming weer wordt ingetrokken?*

Via de Functionaris voor de Gegevensbescherming kan een betrokkene aangeven dat deze zijn of haar toestemming wenst in te trekken. Bij lancering is er een voorziening getroffen om aan de uitwerking van de wet binnen de gestelde termijn gevolg te geven.

- *Wat als een betrokkene zijn of haar gegevens wil inzien?*

Via de Functionaris voor de Gegevensbescherming kan een betrokkene aangeven dat inzage te geven. Bij lancering is er een voorziening getroffen om aan de uitwerking van de wet binnen de gestelde termijn gevolg te geven. Een dergelijke uitdraai zal zeer laagdrempelig zijn, omdat er slechts heel beperkt gegevens worden verwerkt.

Bijlagen

Formulier Vaccinregistratie

VACCIN REGISTRATIE FORMULIER COVID19

NAAM CLIËNT

BSN

☐ MEDISCH BEROEP ☐ KWETSBARE GROEP

DATUM

LOCATIE

PLAATS

AGB-CODE

NOTITIES

VACCIN ☐ **1e dosis** ☐ **2e dosis**

FABRIKANT

BATCHNUMMER

NAAM VACCINEERDER

BIG-REGISTRATIENUMMER

HANDTEKENING VACCINEERDER

INVULLEN INDIEN HANDMATIG

VOORNAAM

ACHTERNAAM

STRAAT HUISNUMMER

POSTCODE PLAATS

TELEFOONNUMMER

E-MAIL ADRES

GEBOORTEDATUM

ZORGNUMMER