Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

AANVRAAGFORMULIER RISICOACCEPTATIE

Betreft:	**Acceptatie risico opslag van BSN nummers door Signicat tbv auditrail**
Aanvrager:	Privacy Officer
Telefoonnummer:	NVT
Datum aanvraag:	30-03-2021
Naam verantwoordelijk lijnmanager:	5.1.2e
Naam centrum- of afdelingshoofd:	5.1.2e 5.1.2e 5.1.2e 5.1.2e
Centrum:	CIO office
Naam Informatiemanager:	5.1.2e
Doel:	Acceptatie van het risico omschreven in dit document
Aan:	Stuurgroep
T.b.v. vergadering:	Stuurgroep realisatie
Aantal pagina's:	7
Notitie toegevoegd:	

Quickscan resultaat
Neem hier de resultaten van de Quickscan over

Datum Quickscan: 17 maart 2021

I Samenvatting

STAP 1		STAP 2			STAP 3					
(X)	**Rubricering**	(X)	**Classificatie proces**	(X)	**Classificatie systeem**	(X)	**B**	(X)	**I**	(X)	**V**
	Openbaar		Ondersteunend	X	Nuttig		Laag		Laag		Laag
	XXXX Intern (besloten)	X	Bijdragend		Belangrijk		Midden	X	Midden	X	Midden
X	XXXX Vertrouwelijk		Strategisch		Vitaal	X	Hoog		Hoog		Hoog
	Departementaal Vertrouwelijk		Kritisch strategisch								
	Staatsgeheim Confidentieel										
	Staatsgeheim Geheim										
	Staatsgeheim Zeer Geheim										

Aanvullende opmerkingen of randvoorwaarden

J Resultaat

	Resultaat	**Toelichting**
BBN *1, 2, 3 of VIR-BI*	*BBN-2*	*Voor Cliëntenportaal: BBN-2.* *Een hoger BBN niveau geeft extra eisen aan authenticatie en klant-onboarding.* *Voor aan te sluiten diensten die een zwaarder authenticatiemiddel Het BBN legt eisen op aan de beveiliging van het informatiesysteem. Dit niveau bepaald niet de zwaarte van het authenticatiemiddel. Het zijn de factoren die bepalend zijn voor het basisbeveiligingsniveau of het*

			betrouwbaarheidsniveau. Hier kunnen dezelfde factoren meespelen, maar er zijn ook onafhankelijke factoren. Het is goed mogelijk dat een lichter authenticatiemiddel ingezet mag worden voor een systeem met BBN3, of dat een zwaarder authenticatiemiddel ingezet moet worden voor BBN1 of BBN2. In Cliëntenportaal geen statelijke actoren die BBN3 vragen.
	RTO *5dgn, 2dgn of < 2dgn*	*<2dgn*	*Geen opmerking.*
	RPO *28hr, 24hr of <24hr*	*Nvt*	*Cliëntenportaal slaat zelf geen gegevens op.*
	Externe eisen *NAVO, EU, ketenpartner, andere organisatie, AVG*	*EU, AVG, DigID assessment*	*Verwerkt AVG gevoelige gegevens;* *data binnen EU;* *Het voldoen aan DigID assessment.* *Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg – WABVPZ.*
	Uitvoeren Risicoanalyse? *Ja of nee*	*Ja*	*Internetfacing, AVG data.*

Aanvraagnummer

Geef aan onder welk nummer de aanvraag al in het risk register staat of dat het een nieuwe aanvraag betreft

Betreft nieuwe aanvraag; nummer nog niet bekend

Aanleiding

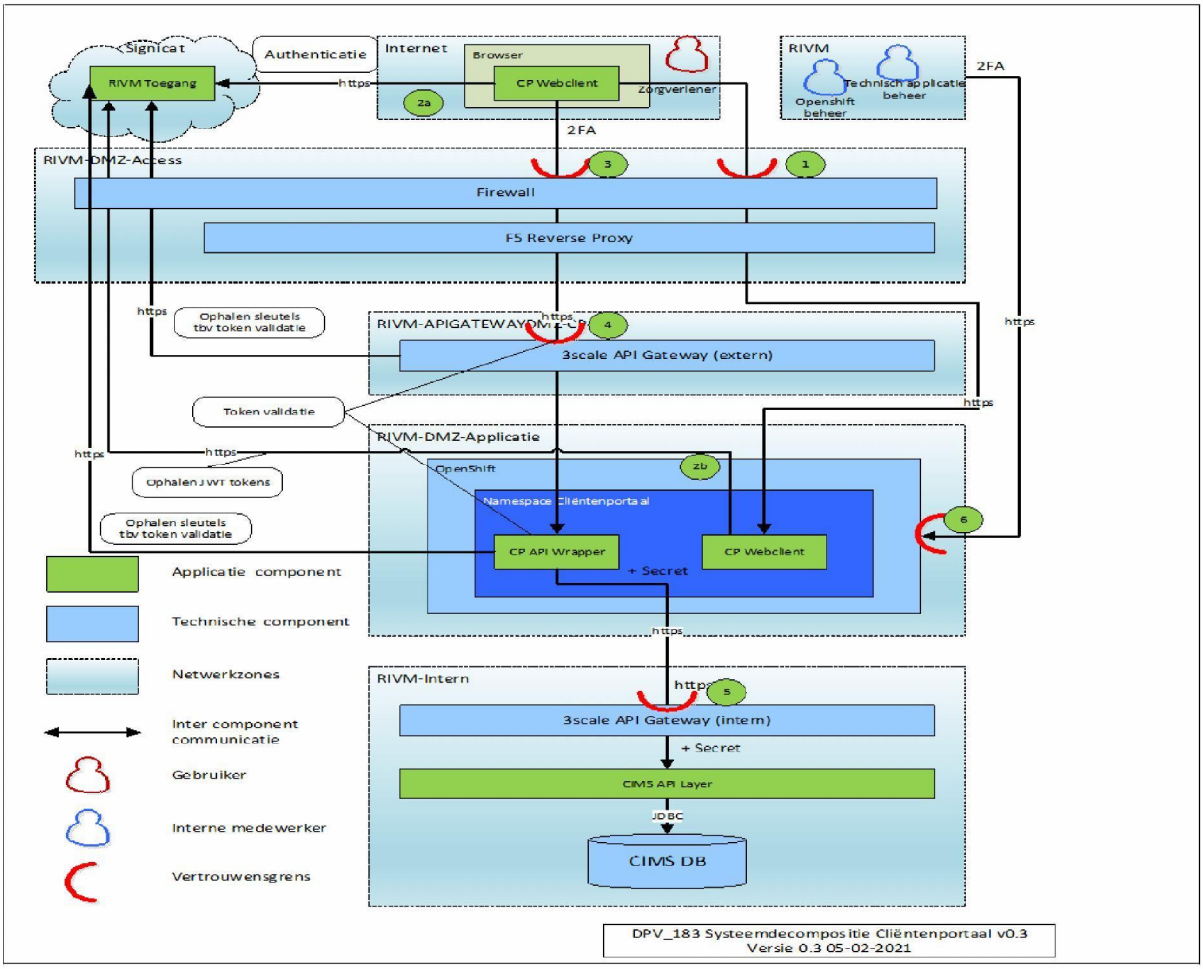
Gerelateerd proces of informatiesysteem (+doelstelling)

Korte omschrijving van proces(sen) en informatiesyste(e)m(en) waar de risicoacceptatie betrekking op heeft en de doelstelling ervan

Clientenportaal; dit portaal faciliteert de rechten van betrokkene onder de AVG conform artikel 15, 16 en 17

Systeemdecompositie

Systeemdecompositie van het betreffende informatiesyste(e)m(en)



	Probleemstelling, risicobeschrijving en mitigatie *Geef hierbij aan welk risico geaccepteerd wordt dan wel voor welk beleid een ontheffing aangevraagd wordt. Geef duidelijk aan wat het risico is, welke mitigerende maatregelen getroffen zijn en wat het managed risico is*
	<u>Probleemstelling:</u> Het is goed om te weten dat er in het Clientenportaal **2 soorten verwerkingen** zijn van het BSN: 1) Het doorgeven van het BSN aan het Cliëntenportaal 2) Het vastleggen van het BSN in het logbestand Deze risicomitigatie gaat alleen over het <u>tweede punt.</u> Het belang van Signicat als verwerker is om via één verbinding authenticatie van eindgebruikers met DigiD mogelijk te maken voor het RIVM en in het kader van fraude detectie (zoals oneigenlijk gebruik van DIGID met als gevolg identiteitsfraude) een zogenaamd messagelog aan te houden. Deze log bevat het originele bericht zoals dat ontvangen is van Logius of het RIVM. Hiermee wordt een audittrail opgebouwd om ook achteraf na te kunnen gaan of de authenticatiepoging veilig en zonder compromittatie verlopen is. Deze maatregel draagt bij aan het garanderen van de integriteit van de verwerking en het verwerkingssysteem. Een ongewijzigde audittrail heeft als doel: • Onderzoek mogelijk maken naar technische incidenten; • Onderzoek mogelijk maken naar oneigenlijk gebruik van DigiD (waaronder fraude) bij specifieke authenticatiepogingen; • Onderzoek mogelijk maken naar specifieke authenticatiepoging bij klachten.

In de messagelog van de Signicat IdP-broker wordt het BSN-nummer - als 9-cijferig nummer zonder BSN referentie - en het IP-adres van de burger opgeslagen. Deze messagelog wordt encrypted opgeslagen op het Signicat systeem en deze is in te zien door de systeembeheerders van SSC-Campus en de systeembeheerders van Signicat welke daarvoor expliciet geautoriseerd zijn. De bewaartermijnen van deze messagelog zijn in te stellen van één dag tot en met drie jaar. Recentelijk is besloten om het bewaartermijn op 1 week te zetten dit wordt als afdoende gezien door de beheerders van SSC-Campus. Deze messagelog is te benaderen via een internet ingang, welke afgeschermd wordt met gebruikersnaam, wachtwoord en OTP-multifactor. Deze log kan worden gedownload naar bv. het SIEM ten behoeve van monitoring en debugging.
Vanuit de FG werd het volgende advies ontvangen; de AVG vereist dat persoonsgegevens worden verwerkt op een wijze met inachtneming van de beginselen van noodzakelijkheid en dataminimalisatie. **Deze beginselen vereisen dat de hoeveelheid persoonsgegevens én het aantal betrokken personen en organisaties tot het noodzakelijk minimum worden beperkt**. Bovendien moet de verwerkingsverantwoordelijke op grond van artikel 25 van de AVG **passende technische en organisatorische maatregelen treffen om de gegevensbeschermingsbeginselen**, zoals dataminimalisatie, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen ('privacy by design'). Het opslaan van BSN nummers schiet hierin –door de inzet van een externe partij (de identity broker) welke toegang tot de gegevens heeft, en vastgelegd (te weten BSN en andere tot op persoon herleidbare gegevens) - tekort.

Risicobeschrijving:

Volgens de mening van de FG zijn de gegevens die de externe broker verwerkt in deze context een **gevoelig gegeven**, omdat als gevolg van het inzage verzoek het vaccinatiegegeven af te leiden is. De FG heeft op dit punt (toegang door externe partij tot de persoonsgegevens, en met name BSN) bezwaar tegen de voorgenomen verwerking en adviseert de voorgenomen verwerking in de huidige vorm niet voort te zetten, tenzij het bezwaar is weggenomen.

Mitigatie

Er zijn al verschillende mitigerende maatregelen (zowel technisch als organisatorisch) genomen om het risico van verkeerd gebruik van BSN en de toegang van de externe partij zoveel mogelijk te beperken:

1. **BSN nummers worden zoals aangegeven niet herkenbaar maar als 9 cijfers verpakt in tokens**; aangezien de berichten van DigiD 1-op-1 worden opgeslagens, wordt ook het BSN opgeslagen zoals het door DigiD verstuurd wordt. Dit is bijvoorbeeld: <saml:Subject><saml:NameID>s00000000:900026236</saml:NameID> (waarbij in dit voorbeeld 900026236 het (test)BSN is). Er staat dus niet expliciet bij dat dit een BSN nummer is. De voorbeeldregel is slechts een onderdeel van een bericht, waardoor het 'extraheren' van alle BSN's dus nog lastiger is. Bovendien worden de berichten geëncrypt opgeslagen.
2. **Om aan het data minimalisatie principe te voldoen slaat Signicat het BSN op zonder context** op deze manier is Signicat niet in staat om het BSN te gebruiken voor het herleiden van de vaccinatiegegevens. De context is niet relevant en wordt ook niet opgeslagen. laat staan de individuele vaccinatiegegevens. Aangezien de berichten die Signicat ontvangt en verstuurd 1-op-1 worden opgeslagen, is er wel een link te leggen tussen het 'subject' (zie hierboven), dat dit van DigiD afkomt, en dat het naar een applicatie van RIVM gaat. Wat er verder binnen RIVM met het BSN gebeurt heeft Signicat uiteraard geen zicht op. Er is dus op geen mogelijkheid om een link te leggen met de toepassing bij RIVM, dus ook niet met bijvoorbeeld vaccinatiegegevens.
3. **Het messagelog is in te zien door systeembeheerders van SSC-Campus en specifieke administrators van Signicat welke daarvoor expliciet geautoriseerd zijn** dit is op een need to know basis, en toegang wordt alleen gegeven indien het nodig is en het wordt gelogd
4. **Inloggen in de broker configuratie applicatie en daarbij de toegang tot de messagelog is afgeschermd** met gebruikersnaam, wachtwoord en OTP-multifactor.
5. **Het bewaartermijn is gezet op 1 week**, het minimale termijn wat vanuit beheer oogpunt noodzakelijk waarbij het risico geaccepteerd wordt dat navraag, fraudeanalyse en -opsporing na die week niet meer mogelijk is.

Verdere mitigerende maatregelen die genomen kunnen worden zijn:

- Acceptatie van dit risico met een maximaal termijn totdat Logius over is gestapt naar het

		het nieuwe koppelvlak (versie 4.5) van DigiD hier is TVS DICTU alreeds op aangesloten. Op dit koppelvlak wordt het BSN encrypted doorgegeven. De tussenliggende partij kan het BSN dan niet ontsleutelen. Logius gaat dit koppelvlak op termijn aan de rest van de afnemers aanbieden. Signicat geeft aan deze koppeling binnen 6 maanden ter beschikking te hebben. **Aangeraden wordt om dit risico dan ook met een termijn van 6 maanden te accepteren en dan weer een review te doen.**			
Ref.	**Risico**	**Maatregel**	**Gerelateerde BIO norm** *Geef hier aan welk BIR-norm van toepassing is*	**Status** *(CISO RIVM)*	**Bijzonderheden** *(CISO RIVM)*
A	Volgens de mening van de FG zijn de gegevens die de externe broker verwerkt in deze context een **gevoelig gegeven,** omdat als gevolg van het inzage verzoek het vaccinatiegegeven af te leiden is. De FG heeft op dit punt (toegang door externe partij tot de persoonsgegevens, en met name BSN) bezwaar tegen de voorgenomen verwerking en adviseert de voorgenomen verwerking in de huidige vorm niet voort te zetten, tenzij het bezwaar is weggenomen.	Er zijn al verschillende mitigerende maatregelen (zowel technisch als organisatorisch) genomen om het risico van verkeerd gebruik van BSN en de toegang van de externe partij zoveel mogelijk te beperken: • **BSN nummers worden zoals aangegeven niet herkenbaar maar als 9 cijfers verpakt in tokens** • **Signicat slaat het BSN op zonder context** op deze manier is Signicat niet in staat om het BSN te gebruiken voor het herleiden van de vaccinatiegegevens. • **Het messagelog wordt encrypted opgeslagen** op het Signicat systeem • **Het messagelog is in te zien door systeembeheerders van SSC-Campus en specifieke administrators** van Signicat welke daarvoor expliciet geautoriseerd zijn • **De toegang tot de messagelog is afgeschermd** met gebruikersnaam, wachtwoord en OTP-multifactor. • **Het bewaartermijn is gezet op 1 week,** het minimale termijn wat vanuit beheer oogpunt noodzakelijk is Verdere mitigerende maatregelen die genomen kunnen worden zijn: • Acceptatie van dit risico met een **maximaal termijn van 6 maanden** totdat Logius over is gestapt naar het burgerservicenummerkoppelpunt (BSNk) Deze	NVT		

		voorziening zet BSN's om naar versleutelde pseudoniemen die, ongeacht eventuele tussenliggende partijen, alleen leesbaar zijn voor de dienstverlener waarbij de burger inlogt.			

Advies

- Acceptatie van dit risico met een maximaal termijn **van 6 maanden** totdat Logius over is gestapt naar het het nieuwe koppelvlak (versie 4.5) van DigiD hier is TVS alreeds op aangesloten. Op dit koppelvlak wordt het BSN encrypted doorgegeven. De tussenliggende partij kan het BSN dan niet ontsleutelen.

Risicomatrix

Geef in de matrix aan waar het risico zich bevindt (dit op basis van de risicoanalyse; in te vullen door CISO of FCC/S&S)

Risicomatrix

kans / impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)	3	12	A	48	75
2 (midden)	2	A	18	32	50
1 (laag)	1	4	9	16	25

Mitigerende maatregelen niet van toepassing

Geef aan waarom geen additionele maatregelen getroffen kunnen worden en/of waarom het beleid niet geïmplementeerd kan worden
Geef dit bij voorkeur per risico aan

NVT

Consequenties andere partijen

Geef aan of andere partijen (domeinen, centra, leveranciers, klanten) consequenties kunnen ondervinden van dit risico
Geef dit bij voorkeur per risico aan

Dit kan leiden tot reputatie schade, en substantiële impact op de persoonlijke levenssfeer van het individu door bijvoorbeeld indentiteitsfraude

Periode

Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is

Acceptatie totdat Logius overstapt op het burgerservicenummerkoppelpunt (BSNk) over maximaal 6 maanden een review

Evaluatie

Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden

Periodieke review over 6 maanden

Gevraagd besluit:	**Acceptatie van het in dit document beschreven risico en dus de verwerking van het BN nummer ten bate van identificatie en audit door derde partij (Signicat) toe te staan**		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, CISO, CIO, Compliance, Legal, Privacy en*	***Akkoord***

		DR)	
Hoofd centrum	5.1.2e		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	5.1.2e		Akkoord: ja/nee
Compliance (Facultatief)			Akkoord: ja/nee
Legal (facultatief)			Akkoord: ja/nee
Privacy (facultatief)	5.1.2e		Akkoord: ja/nee
CIO *(mandatory voor medium en hoger risico)*			Akkoord: ja/nee
DR *(mandatory voor hoog en zeer hoog risico)*			Akkoord: ja/nee