Versie 0.2

Datum April 2017

Status [Status]

Documenthistorie

Datum	Versie	Beschrijving	Auteur
April 2017	0.1	Eerste opzet	Operatie BRP
Juni 2017	0.2	Aanpassingen na overleg testen en RviG	Operatie BRP

Reviewhistorie

Versie	Reviewer
0.1	Operatie BRP
0.2	Operatie BRP

Inhoudsopgave

1 Inleiding

1.1 Doel

Doel van dit document om tot in detail te beschrijven hoe de NFRs voor beveiliging te interpreteren zijn in relatie tot de verschillende onderdelen van de BRP en hoe de informatiebeveiliging van de BRP zich in het algemeen verhoud tot de softwarebouw van de BRP applicatie.

1.2 Referenties

Nr.	Documentnaam	Organisatie	Versie	Datum
1	Requirements beveiligbaarheid	Operatie BRP	V2.5	-
2	Koppeling IBP en Requirements Beveiligbaarheid	Operatie BRP	-	-
3	Mastertable NFR's	Operatie BRP	V2	-
4	Informatiebeveiligingsplan BRP	RViG	1.0	03-09-2013
5	Beperking impact NFR BEV	Operatie BRP	V4	12-05-2015
6	Normenkader codekwaliteit Operatie BRP	Operatie BRP	1.2	14-04-2016
7	Beveiliging Authenticatie Autorisatie	Operatie BRP	0.7	-

2 Samenvatting NFRs beveiliging

Hieronder is een korte samenvatting van de NFRs voor beveiliging gegeven. De omgang met de NFRs voor de maatwerkcomponenten van de centrale BRP is verder uitgewerkt in de opvolgende hoofdstukken.

2.1 Herkomst

De non-functional requirements (NFRs) zijn in het verleden opgesteld conform ISO 25010 kwaliteitscriteria waar beveiligbaarheid onderdeel van uit maakt. Alle NFRs zijn opgenomen in een mastertable excel document.

De NFRs die over beveiliging gaan zijn aangeduid met RD-BEV. Een aantal van deze requirements vallen onder de codeerrichtlijnen en zijn in die vorm nader uitgewerkt (normenkader codekwaliteit [6]). Vanuit het overkoepelende informatiebeveiligingsplan zijn aanvullingen aan de NFRs uit de mastertable toegevoegd.

2.2 Structuur

De NFRs zijn te verdelen in algemeen van toepassing, gericht op koppelvlakken en gericht op de gebruikersinterface (in relatie tot beheer van de voorziening).

Iedere NFR omschrijft voor het project Operatie BRP de eisen aan de opzet van de software en documentatie van de software op het vlak van beveiliging. Een enkele regel verwijst naar de risicolijst van het OWASP-project.

Een NFR is generiek van aard opgeschreven los van de functionele beschrijving van de BRP en vraagt daarom interpretatie bij de verschillende functionele onderdelen van de BRP-applicatie.

2.3 Inhoud

De uitwerking van de NFRs die verwant zijn aan de algemene kaders voor kwaliteit van broncode zijn uitwerkt in de codeerrichtlijnen. Deze zijn verantwoordelijk voor de ‘ontbrekende nummers’ in het overzicht van NFRs in de requirements voor beveiligbaarheid [1].

NFRs die verder afstaan van algemene kaders voor kwaliteit van broncode zijn opgenomen in de requirements voor beveiligbaarheid [1]. In deze NFRs zijn ook een aantal principes van defensief programmeren in terug te zien die soms met de codeerrichtlijnen overlappen.

De NFRs voor beveiliging zijn erop gericht dat een BRP-applicatie voldoet aan:

1. Kwalitatief goed te onderhouden broncode.
2. Een defensieve opzet van de applicatie om fouten te voorkomen
3. Controleerbaarheid van het gedrag van de applicatie en gebruikers
4. Robuustheid ten aanzien van de meest voorkomende fouten in software
5. Het voorzien in waarborgen voor gegevensintegriteit en –vertrouwelijkheid.
6. Bij voorkomende fouten deze snel te kunnen detecteren en te herstellen.

3 Beveiliging BRP-applicatie

Voor de beveiliging van de centrale BRP-applicatie vormen de NFRs de basis, in het bijzonder die ten aanzien van beveiliging. Alles wat de software van de applicatie betreft moet deze normen volgen. Deze NFRs spelen een rol in het kader van de integrale beveiliging van de BRP.

3.1 Software perspectief

De definitie Beveiliging volgens de ISO 25010 kwaliteitsnorm luidt als volgt:

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

- Vertrouwelijkheid (Confidentiality)
  De mate waarin een product of systeem ervoor zorgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn.
- Integriteit (Integrity)
  De mate waarin een systeem, product of component ongeautoriseerde toegang tot of aanpassing van computerprogramma's of gegevens verhindert.
- Onweerlegbaarheid (Non-repudiation)
  De mate waarin kan worden bewezen dat acties of gebeurtenissen plaats hebben gevonden, zodat later deze acties of gebeurtenissen niet ontkend kunnen worden.
- Verantwoording (Accountability)
  De mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit.
- Authenticiteit (Authenticity)
  De mate waarin bewezen kan worden dat de identiteit van een onderwerp of bron is zoals wordt beweerd.
  De mate waarin een claim over de oorsprong of de auteur van de informatie verifieerbaar is, bijvoorbeeld aan handschrift.

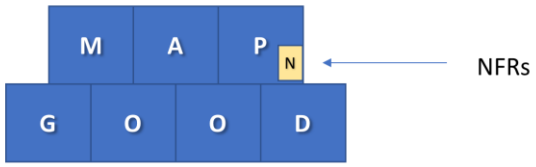
De toepassing van de NFRs onder deze definitie vormt het voornaamste uitgangspunt voor veiligheid in de software. Vanuit de functionele eisen zijn daarnaast in de programmatuur specifieke maatregelen voor de veiligheid van de BRP getroffen. Denk daarbij bijvoorbeeld aan het mechanisme voor authenticatie van aangesloten partijen.

De NFRs die verwant zijn aan de algemene kaders voor kwaliteit van broncode zijn uitwerkt in de codeerrichtlijnen (Document Normenkader codekwaliteit Operatie BRP [6]). De codeerrichtlijnen bestrijken meer aspecten van softwarekwaliteit. De codeerrichtlijnen zijn erop gericht de code automatisch te analyseren en de kwaliteit ervan continu te meten.

Verder is in het algemene uitgangspunt gehanteerd dat broncode 'defensief' moet zijn geprogrammeerd, de codeerrichtlijnen gaan op dat vlak ook verder dan de NFRs. Defensief programmeren is een programmeerstijl die als doel heeft robuuste en fouttolerante applicaties te produceren.

3.2 Integrale beveiliging

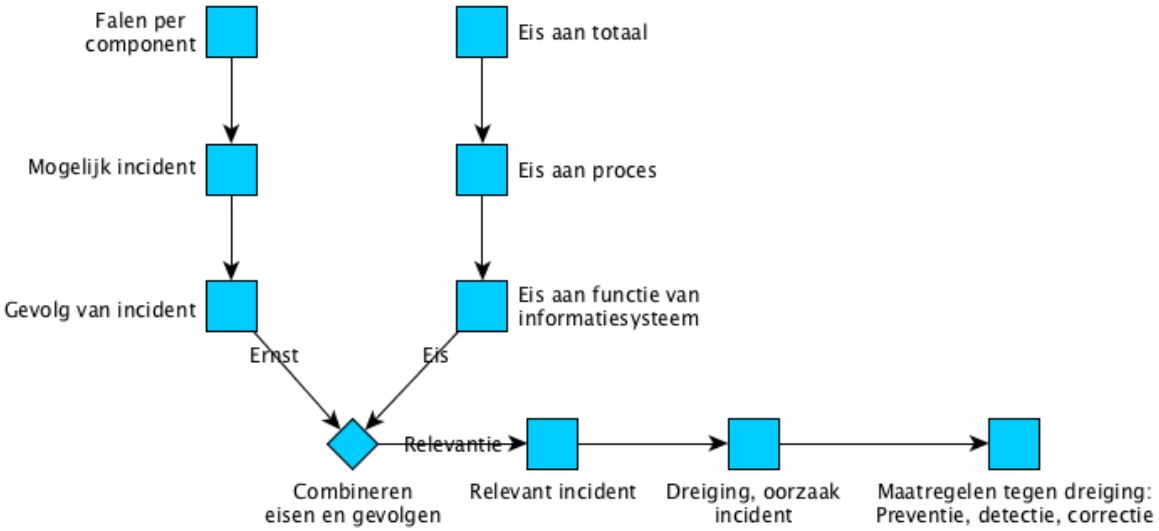
Een informatiesysteem als de BRP omvat logische onderdelen als mensen, apparatuur, programmatuur, gegevens, omgeving, organisatie en diensten. De benadering van beveiliging vraagt een integrale aanpak om te komen tot veiligheidsmaatregelen die een consistent, onderbouwd en passend stelsel vormen. De NFRs vullen een deel van de maatregelen in op het vlak van maatregelen in de programmatuur.



Mensen, Apparatuur, Programmatuur
Gegevens, Organisatie, Omgeving, Diensten

De betrouwbaarheid is de mate waarin de overheid zich kan verlaten op de BRP als geheel systeem voor zijn informatievoorziening. Vanuit de eisen gesteld aan de betrouwbaarheid vloeien eisen voort aan processen en functies van het informatiesysteem. Per onderdeel is in te schatten wat de gevolgen bij falen zijn, welke incidenten er kunnen optreden en wat daarvan de gevolgen zijn. De combinatie van eisen en de ernst van de gevolgen bepalen of een incident relevant is. Is een incident relevant dan is het nodig te voorzien in maatregelen tegen de dreigingen die er ten grondslag aan liggen. Het langs deze weg afleiden van maatregelen noemt men een risicoanalyse.

Bij het uitvoeren van een risicoanalyse over het hele informatiesysteem spreekt met van een integrale aanpak en is de uitkomst een integraal beveiligingsplan. Dit zorgt voor een evenwichtige balans tussen maatregelen ten aanzien van de verschillende onderdelen: niet alles is bijvoorbeeld praktisch op te lossen met fysieke beveiligingsmaatregelen of met logische maatregelen in software.



Voor een informatiesysteem als de BRP is een goede samenhang in maatregelen voor de beveiliging essentieel. Het informatiebeveiligingsplan [4] geeft hier op strategisch, tactisch niveau richting aan.

Er bestaat ten tijde van het opstellen van dit document geen integrale vertaling naar de operationele maatregelen, een operationeel beveiligingsplan. Een dergelijk plan valt buiten de scope van de opdracht voor beveiliging van de door Operatie BRP te ontwikkelen BRP applicatie.

Naast de algemene uitleg dat het informatiebeveiligingsplan op strategisch, tactisch niveau is ingevuld zijn op onderdelen daar ook expliciete delen buiten scope geplaatst:

> *"Het beheer en management van de informatiebeveiliging conform ISO 27001, wordt slechts beperkt behandeld in het IBP. Het voorliggende IBP richt zich primair op de ontwikkeling en bouw van de BRP binnen het project BRP. Het beheer en management van de informatiebeveiliging van de BRP zal door de beheerder van de BRP, het Agentschap BPR, ingericht worden en valt daarom buiten de scope van het IBP."*

Hieronder vallen in het bijzonder de hoofstukken: beveiliging van personeel, fysieke beveiliging en beveiliging van de omgeving, bedrijfscontinuiteitsbeheer en naleving.

Het is noodzakelijk dat de applicatie, de programmatuur, hiervoor een goede aansluiting heeft bij de overige logische onderdelen van mensen, apparatuur, gegevens, omgeving, organisatie en diensten. Zo moet bijvoorbeeld een beheerder vanuit de beheeromgeving kunnen omgaan met de logging van de applicatie waarbij traceerbaar is wat er heeft plaatsgevonden op een zeker moment op basis van tijd. In de infrastructuur zal dan tijdsynchronisatie voorhanden moeten zijn.

Vanuit de bouw van de applicatie is uitgegaan van wat beschreven is in de requirements. Hoe de verschillende onderdelen bij elkaar komen is nog nader in te vullen, ook voor wat betreft de beveiliging.

In een operationeel beveiligingsplan (dat kan bestaan uit een op elkaar afgestemde verzameling van plannen) is voor het geheel een samenhangende selectie van praktische maatregelen op te nemen ter voorkoming (preventief), ter signalering (detectief) en/of ter herstel (correctief) van incidenten.

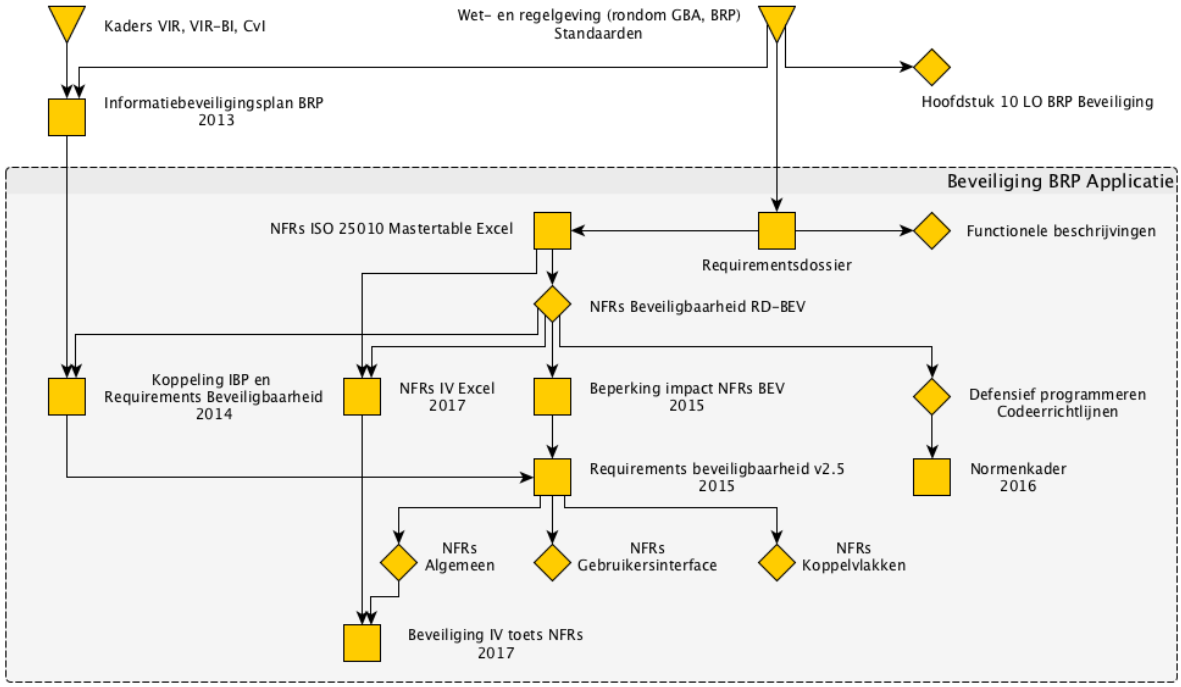
4 Aanpak NFRs ontwikkeling

In dit hoofdstuk is beschreven welke aanpak is gehanteerd bij ontwikkeling om ervoor te zorgen dat de NFRs op een juiste wijze zijn ingevuld.

In de eerste paragraaf met de algemene introductie is aangegeven hoe softwareontwikkeling omgaat met de NFRs waarna in de paragrafen over initiële vulling, levering, bijhouding en beheer de interpretatie van de van toepassing zijnde NFRs is beschreven.

4.1 Algemeen

Voor een project als de BRP is er een veelvoud aan documenten die bijdragen aan de vorming van het softwareproduct. Het distilleren en vertalen van de uiteindelijke eisen aan een stuk software raakt veel facetten en heeft een verloop in tijd van de ontwikkeling.



De NFRs zijn in het verleden opgesteld conform ISO 25010 waar beveiligbaarheid onderdeel van uit maakt. Alle NFRs zijn opgenomen in een mastertable excel document [3].

Merk op: De mastertable (v2) gebruikt soms een andere formulering van de requirements dan de andere documenten. Ook zijn er zo nu en dan inhoudelijke verschillen. De formulering van de NFRs van het type beveiligbaarheid doet vermoeden dat deze zijn geformuleerd in de geest van applicatieontwikkeling voor algemene, openbare internettoepassingen. Bijvoorbeeld in maatregelen die malafide gebruik van buitenaf moeten tegengaan is dit terug te herkennen. Dit sluit niet aan bij het type applicatie en de moderne ontwikkelmethodiek in gebruik bij het project.

Uit het requirementsdossier:

> *"Voor zover het eisen betreft die betrekking hebben op de door oBRP te ontwikkelen software is het informatiebeveiligingsplan in afstemming met RvIG omgezet in requirements beveiligbaarheid (RD-BEV). Met betrekking tot informatiebeveiliging hanteert oBRP deze eisen en niet het informatiebeveiligingsplan."*

Dit is een afbeelding van de eerder gestelde eisen ten aanzien van beveiligbaarheid op de eisen in het beveiligingsplan. Volgens 'Koppeling IBP en Requirements Beveiligbaarheid' [2] zijn de normen uit het beveiligingsplan geconsolideerd of herschikt binnen de requirements beveiligbaarheid [1].

In het document Beperking impact NFR BEV [5] is een subset uitgewerkt. De eisen voor beveiligbaarheid zijn in een subset vervat die buiten de codeerrichtlijnen vallen. De eisen die onder de codeerrichtlijnen vallen zijn uit de requirements beveiligbaarheid v2.5 weggelaten.

Merk op: Enkele van de resterende eisen zijn in de mastertable soms wel onder 'defensief programmeren' geschaard en lijken in voorkomende gevallen oor de codeerrichtlijnen te raken.

Uit requirements beveiligbaarheid v2.5 komt een verdere opdeling:

> *"De requirements zijn opgedeeld in de groepen 'algemeen', 'koppelvlakken' en 'gebruikersinterface'. Aangezien de centrale BRP geen gebruikersinterface ten behoeve van reguliere gebruikers heeft, betreft die laatste groep alleen de gebruikersinterface ten behoeve van beheer van de voorziening."*

In de SAD documentatie bij de verschillende onderdelen van de BRP is beschreven hoe er met beveiliging is omgegaan, in het bijzonder hoe er met de NFRs is omgegaan.

Een aantal NFRs raakt de regels in het BRP Meta Register. In het BRP Meta Register (BMR) wordt het gegevensmodel, de regels en de basis berichtspecificaties (XSD) onderhouden. Het onderhouden van de regels is de verantwoordelijkheid van de specifiers. Het doel is dat de regels de requirements implementeren en specificeren hoe BRP werkt. Dit raakt ook aspecten van de NFRs.

De overige tooling bij ontwikkeling voor het controleren van de codeerrichtlijnen uit het normenkader bestaat uit Findbugs, PMD, Checkstyle en SonarQube. Hiermee vindt de analyse en kwaliteitsmeting plaats.

In SonarQube zijn de OWASP-regels meegenomen die deel uit maken van NFR RD-BEV-30. Deze OWASP NFR schrijft ook onderbouwing in documentatie voor: "In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software." Doorgaans is dit vastgelegd in het SAD document van het betreffende component.

Naast de OWASP regels zijn onder andere ook CWE en SANS25 regels opgenomen. Dit is dus een bredere groep regels dan die van OWASP zoals gesteld in de NFRs.

Let wel: alle NFRs zijn in algemene zin van toepassing voor de ontwikkeling, echter niet iedere eis is zinnig in de context van het betreffende software onderdeel. Uit dat perspectief spreken teksten wel eens over 'niet van toepassing' wanneer het de bedoeling is aan te geven dat de eis voor het betreffende onderdeel geen effect heeft. Pas na een grondige afstemming binnen het team is deze conclusie te trekken.

4.2 Initiële Vulling

Initiële Vulling (IV) heeft een specifieke taak bij de migratie en is afgebakend in functies en tijd. Voor IV zijn door dit karakter alleen deels de requirements in de groep 'algemeen' effectief van toepassing. Voor IV doen de requirements 'koppelvlakken' en 'gebruikersinterface' niet ter zake (beide aspecten zijn immers niet aanwezig).

Door het team (onderling overleg betrokken expertises) zijn deze aangemerkt als niet van toepassing zijnde in deze context of als afgedekt door specifieke functionele eisen. Dit is beschreven in het Excel overzicht 'NFRs IV'.

In het navolgende overzicht is een interpretatie voor IV gegeven per requirement.

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Interpretatie	In deze maatregel is te lezen dat er sprake zou zijn van malafide handelen van buitenaf. Dit is voor IV als applicatie nauwelijks van toepassing. In zowel de applicatie-architectuur, functionele eisen als de ontwikkelmethodiek komen deze aspecten terug. Het draait om het controleren en bewaken van (gegevens)integriteit en het voorkomen van manipulatie van de applicatie.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Interpretatie	Hier is controle op onterechte toegang beschreven en het melden van fouten voor opvolging, zo mogelijk correctie. Veel van de beschreven punten zijn niet van toepassing voor IV of slechts deels.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Interpretatie	Eis om te loggen op een ander systeem met oog op compartimenteren.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.

Interpretatie	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico's zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.
Interpretatie	De OWASP lijst komt tot stand door jaarlijks bij een aantal organisaties incidenten te inventariseren aangaande webapplicaties. De laatste release van de lijst was in 2013. Wel is er onverwerkte data uit 2014 en 2015. Op basis van 2013 zijn uit de 10 meest voorkomende kwetsbaarheden de volgende relevante punten te herleiden: • Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie. Vergelijk RD-BEV-004. • Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc. Vergelijk RD-BEV-049/032 • Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack. • Bekende kwetsbaarheden in gebruikte standaard software componenten. OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik. Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn. De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'.
RD-BEV-049	Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.
Interpretatie	Autorisatie op onderdelen volgt het principe van 'least privilege'.
RD-BEV-032	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext) Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.
Interpretatie	Veilige omgang met wachtwoorden door de applicatie, goede versleuteling bij opslag. Als opslag in een configuratiebestand van een wachtwoord echt nodig is dan is hier een uitzondering op te maken mits het zorgvuldig gebeurd zodat de omgeving, infrastructuur hier aanvullende maatregelen bij kan treffen.

4.3 Levering

In het navolgende overzicht is een interpretatie voor levering gegeven per requirement.

Onderstaande algemene requirements worden gesteld aan de door het project O&R op te leveren maatwerkcomponenten van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Interpretatie	In deze maatregel is te lezen dat er sprake zou zijn van malafide handelen van buitenaf. Dit is voor IV als applicatie nauwelijks van toepassing. In zowel de applicatie-architectuur, functionele eisen als de ontwikkelmethodiek komen deze aspecten terug. Het draait om het controleren en bewaken van (gegevens)integriteit en het voorkomen van manipulatie van de applicatie.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Interpretatie	Hier is controle op onterechte toegang beschreven en het melden van fouten voor opvolging, zo mogelijk correctie. Veel van de beschreven punten zijn niet van toepassing voor IV of slechts deels.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Interpretatie	Eis om te loggen op een ander systeem met oog op compartimenteren.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
Interpretatie	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico’s zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren

(maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.

Interpretatie De OWASP lijst komt tot stand door jaarlijks bij een aantal organisaties incidenten te inventariseren aangaande webapplicaties. De laatste release van de lijst was in 2013. Wel is er onverwerkte data uit 2014 en 2015.

Op basis van 2013 zijn uit de 10 meest voorkomende kwetsbaarheden de volgende relevante punten te herleiden:

- Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie. Vergelijk RD-BEV-004.
- Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc. Vergelijk RD-BEV-049/032
- Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack.
- Bekende kwetsbaarheden in gebruikte standaard software componenten.

OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik.

Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn.

De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'.

RD-BEV-049 Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.

Interpretatie Autorisatie op onderdelen volgt het principe van 'least privilege'.

RD-BEV-032 Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext)
Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.

Interpretatie Veilige omgang met wachtwoorden door de applicatie, goede versleuteling bij opslag. Als opslag in een configuratiebestand van een wachtwoord echt nodig is dan is hier een uitzondering op te maken mits het zorgvuldig gebeurd zodat de omgeving, infrastructuur hier aanvullende maatregelen bij kan treffen.

Requirements voor koppelvlakken:

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-026 Gebruikerstoegang anders dan via GBA koppelvlakken of BRP koppelvlakken is niet mogelijk.

Interpretatie Bij het benaderen van de applicatie van buiten zijn alleen deze koppelvlakken toegankelijk.

RD-BEV-027 Functies voor bijhouding en voor levering zijn logisch gescheiden binnen de BRP koppelvlakken.

Interpretatie	De functies draaien binnen een eigen instantie op de applicatieserver met ieder een eigen koppelvlak.
RD-BEV-028	Gebruikerstoegang via BRP koppelvlakken verloopt uitsluitend met berichtuitwisseling conform Digikoppeling 3.0, profielen "2W-be-s", "2W-R-S" of "osb-rm-s".
Interpretatie	Vanuit beveiliging gezien gaat het om een betrouwbare uitwisseling (waarbij er verschillen in de profielen zitten) binnen deze standaard gebruikmakend van het digitaal ondertekenen van berichten (signing).
RD-BEV-029	Gebruikerstoegang via GBA koppelvlakken verloopt uitsluitend met berichtuitwisseling conform het Logisch Ontwerp GBA.
Interpretatie	Het Logisch Ontwerp GBA stelt specifieke eisen aan berichtuitwisseling op het vlak van beveiliging.
RD-BEV-042	Niet integere berichten krijgen een antwoordbericht met een standaard melding die geen inhoudelijke informatie geeft over de authenticatie en autorisatie die de stelselapplicatie uitvoert.
Interpretatie	Het koppelvlak mag geen informatie lekken. Alleen juiste, integere, berichten krijgen een inhoudelijk antwoord.
RD-BEV-043	De volledigheid en juistheid van de uitvoer van het systeem via de BRP koppelvlakken is vast te stellen door een digitale handtekening (of anderszins via een checksum of hash).
Interpretatie	Met het gebruik van deze mechanismen is zonder twijfel vast te stellen dat de gegevens correct zijn overgedragen bij uitwisseling.
RD-BEV-044	De applicatie verstrekt niet meer gegevens dan de gegevens die op grond van de autorisatie mogen worden verstrekt.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-045	Bij een vraag aan de applicatie verstrekt de applicatie geen andere gegevens dan de gegevens die zijn gevraagd.
Interpretatie	De BRP applicatie geeft niet ongevraagd in bijvoorbeeld een foutmelding gegevens die niet zijn gevraagd of een ander soort antwoord waaruit gegevens af te leiden zijn.
RD-BEV-046	Gegevens worden alleen verstrekt aan op voorhand bekende afleveradressen.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-013	Het systeem biedt de mogelijkheid aan de beheerder om het gebruik van het systeem via de koppelvlakken te blokkeren. De niveau's die daarbij worden onderscheiden zijn (juridisch) geautoriseerde partij, ondertekenende partij, aangesloten partij en de toegang (de combinatie van geautoriseerde partij, ondertekenende partij, aangesloten partij en de verzameling functies die op het systeem mogen worden uitgevoerd)
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.

4.4 Bijhouding

In het navolgende overzicht is een interpretatie voor bijhouding gegeven per requirement.

Onderstaande algemene requirements worden gesteld aan de door het project O&R op te leveren maatwerkcomponenten van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Interpretatie	In deze maatregel is te lezen dat er sprake zou zijn van malafide handelen van buitenaf. Dit is voor IV als applicatie nauwelijks van toepassing. In zowel de applicatie-architectuur, functionele eisen als de ontwikkelmethodiek komen deze aspecten terug. Het draait om het controleren en bewaken van (gegevens)integriteit en het voorkomen van manipulatie van de applicatie.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Interpretatie	Hier is controle op onterechte toegang beschreven en het melden van fouten voor opvolging, zo mogelijk correctie. Veel van de beschreven punten zijn niet van toepassing voor IV of slechts deels.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Interpretatie	Eis om te loggen op een ander systeem met oog op compartimenteren.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
Interpretatie	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico’s zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren

(maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.

Interpretatie De OWASP lijst komt tot stand door jaarlijks bij een aantal organisaties incidenten te inventariseren aangaande webapplicaties. De laatste release van de lijst was in 2013. Wel is er onverwerkte data uit 2014 en 2015.

Op basis van 2013 zijn uit de 10 meest voorkomende kwetsbaarheden de volgende relevante punten te herleiden:

- Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie. Vergelijk RD-BEV-004.
- Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc. Vergelijk RD-BEV-049/032
- Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack.
- Bekende kwetsbaarheden in gebruikte standaard software componenten.

OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik.

Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn.

De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'.

RD-BEV-049 Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.

Interpretatie Autorisatie op onderdelen volgt het principe van 'least privilege'.

RD-BEV-032 Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext)
Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.

Interpretatie Veilige omgang met wachtwoorden door de applicatie, goede versleuteling bij opslag. Als opslag in een configuratiebestand van een wachtwoord echt nodig is dan is hier een uitzondering op te maken mits het zorgvuldig gebeurd zodat de omgeving, infrastructuur hier aanvullende maatregelen bij kan treffen.

Requirements voor koppelvlakken:

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-026 Gebruikerstoegang anders dan via GBA koppelvlakken of BRP koppelvlakken is niet mogelijk.

Interpretatie Bij het benaderen van de applicatie van buiten zijn alleen deze koppelvlakken toegankelijk.

RD-BEV-027 Functies voor bijhouding en voor levering zijn logisch gescheiden binnen de BRP koppelvlakken.

Interpretatie	De functies draaien binnen een eigen instantie op de applicatieserver met ieder een eigen koppelvlak.
RD-BEV-028	Gebruikerstoegang via BRP koppelvlakken verloopt uitsluitend met berichtuitwisseling conform Digikoppeling 3.0, profielen "2W-be-s", "2W-R-S" of "osb-rm-s".
Interpretatie	Vanuit beveiliging gezien gaat het om een betrouwbare uitwisseling (waarbij er verschillen in de profielen zitten) binnen deze standaard gebruikmakend van het digitaal ondertekenen van berichten (signing).
RD-BEV-029	Gebruikerstoegang via GBA koppelvlakken verloopt uitsluitend met berichtuitwisseling conform het Logisch Ontwerp GBA.
Interpretatie	Het Logisch Ontwerp GBA stelt specifieke eisen aan berichtuitwisseling op het vlak van beveiliging.
RD-BEV-042	Niet integere berichten krijgen een antwoordbericht met een standaard melding die geen inhoudelijke informatie geeft over de authenticatie en autorisatie die de stelselapplicatie uitvoert.
Interpretatie	Het koppelvlak mag geen informatie lekken. Alleen juiste, integere, berichten krijgen een inhoudelijk antwoord.
RD-BEV-043	De volledigheid en juistheid van de uitvoer van het systeem via de BRP koppelvlakken is vast te stellen door een digitale handtekening (of anderszins via een checksum of hash).
Interpretatie	Met het gebruik van deze mechanismen is zonder twijfel vast te stellen dat de gegevens correct zijn overgedragen bij uitwisseling.
RD-BEV-044	De applicatie verstrekt niet meer gegevens dan de gegevens die op grond van de autorisatie mogen worden verstrekt.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-045	Bij een vraag aan de applicatie verstrekt de applicatie geen andere gegevens dan de gegevens die zijn gevraagd.
Interpretatie	De BRP applicatie geeft niet ongevraagd in bijvoorbeeld een foutmelding gegevens die niet zijn gevraagd of een ander soort antwoord waaruit gegevens af te leiden zijn.
RD-BEV-046	Gegevens worden alleen verstrekt aan op voorhand bekende afleveradressen.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-013	Het systeem biedt de mogelijkheid aan de beheerder om het gebruik van het systeem via de koppelvlakken te blokkeren. De niveau's die daarbij worden onderscheiden zijn (juridisch) geautoriseerde partij, ondertekenende partij, aangesloten partij en de toegang (de combinatie van geautoriseerde partij, ondertekenende partij, aangesloten partij en de verzameling functies die op het systeem mogen worden uitgevoerd)
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.

4.5 Beheer

In het navolgende overzicht is een interpretatie voor beheer gegeven per requirement.

Onderstaande algemene requirements worden gesteld aan de door het project O&R op te leveren maatwerkcomponenten van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Interpretatie	In deze maatregel is te lezen dat er sprake zou zijn van malafide handelen van buitenaf. Dit is voor IV als applicatie nauwelijks van toepassing. In zowel de applicatie-architectuur, functionele eisen als de ontwikkelmethodiek komen deze aspecten terug. Het draait om het controleren en bewaken van (gegevens)integriteit en het voorkomen van manipulatie van de applicatie.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Interpretatie	Hier is controle op onterechte toegang beschreven en het melden van fouten voor opvolging, zo mogelijk correctie. Veel van de beschreven punten zijn niet van toepassing voor IV of slechts deels.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Interpretatie	Eis om te loggen op een ander systeem met oog op compartimenteren.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
Interpretatie	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico’s zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren

(maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.

Interpretatie De OWASP lijst komt tot stand door jaarlijks bij een aantal organisaties incidenten te inventariseren aangaande webapplicaties. De laatste release van de lijst was in 2013. Wel is er onverwerkte data uit 2014 en 2015.

Op basis van 2013 zijn uit de 10 meest voorkomende kwetsbaarheden de volgende relevante punten te herleiden:

- Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie. Vergelijk RD-BEV-004.
- Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc. Vergelijk RD-BEV-049/032
- Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack.
- Bekende kwetsbaarheden in gebruikte standaard software componenten.

OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik.

Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn.

De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'.

RD-BEV-049 Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.

Interpretatie Autorisatie op onderdelen volgt het principe van 'least privilege'.

RD-BEV-032 Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext)
Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.

Interpretatie Veilige omgang met wachtwoorden door de applicatie, goede versleuteling bij opslag. Als opslag in een configuratiebestand van een wachtwoord echt nodig is dan is hier een uitzondering op te maken mits het zorgvuldig gebeurd zodat de omgeving, infrastructuur hier aanvullende maatregelen bij kan treffen.

Requirements voor koppelvlakken:

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-026	Gebruikerstoegang anders dan via GBA koppelvlakken of BRP koppelvlakken is niet mogelijk.
Interpretatie	Bij het benaderen van de applicatie van buiten zijn alleen deze koppelvlakken toegankelijk.
RD-BEV-027	Functies voor bijhouding en voor levering zijn logisch gescheiden binnen de BRP koppelvlakken.
Interpretatie	De functies draaien binnen een eigen instantie op de applicatieserver met ieder een eigen koppelvlak.
RD-BEV-028	Gebruikerstoegang via BRP koppelvlakken verloopt uitsluitend met berichtuitwisseling conform Digikoppeling 3.0, profielen "2W-be-s", "2W-R-S" of "osb-rm-s".
Interpretatie	Vanuit beveiliging gezien gaat het om een betrouwbare uitwisseling (waarbij er verschillen in de profielen zitten) binnen deze standaard gebruikmakend van het digitaal ondertekenen van berichten (signing).
RD-BEV-029	Gebruikerstoegang via GBA koppelvlakken verloopt uitsluitend met berichtuitwisseling conform het Logisch Ontwerp GBA.
Interpretatie	Het Logisch Ontwerp GBA stelt specifieke eisen aan berichtuitwisseling op het vlak van beveiliging.
RD-BEV-042	Niet integere berichten krijgen een antwoordbericht met een standaard melding die geen inhoudelijke informatie geeft over de authenticatie en autorisatie die de stelselapplicatie uitvoert.
Interpretatie	Het koppelvlak mag geen informatie lekken. Alleen juiste, integere, berichten krijgen een inhoudelijk antwoord.
RD-BEV-043	De volledigheid en juistheid van de uitvoer van het systeem via de BRP koppelvlakken is vast te stellen door een digitale handtekening (of anderszins via een checksum of hash).
Interpretatie	Met het gebruik van deze mechanismen is zonder twijfel vast te stellen dat de gegevens correct zijn overgedragen bij uitwisseling.
RD-BEV-044	De applicatie verstrekt niet meer gegevens dan de gegevens die op grond van de autorisatie mogen worden verstrekt.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-045	Bij een vraag aan de applicatie verstrekt de applicatie geen andere gegevens dan de gegevens die zijn gevraagd.
Interpretatie	De BRP applicatie geeft niet ongevraagd in bijvoorbeeld een foutmelding gegevens die niet zijn gevraagd of een ander soort antwoord waaruit gegevens af te leiden zijn.
RD-BEV-046	Gegevens worden alleen verstrekt aan op voorhand bekende afleveradressen.
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.
RD-BEV-013	Het systeem biedt de mogelijkheid aan de beheerder om het gebruik van het systeem via de koppelvlakken te blokkeren. De niveau's die daarbij worden onderscheiden zijn (juridisch) geautoriseerde partij, ondertekenende partij, aangesloten partij en de toegang (de combinatie van geautoriseerde partij,

	ondertekenende partij, aangesloten partij en de verzameling functies die op het systeem mogen worden uitgevoerd)
Interpretatie	In de notitie 'Beveiliging Authenticatie Autorisatie' [7] is dit in detail uitgewerkt voor de BRP.

Requirements voor de (beheer)gebruikersinterface:

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-018	Bij client/server applicaties dienen validaties ook altijd op de server-kant plaats te vinden.
Interpretatie	Na normalisatie volgt altijd validatie door de applicatie voordat verdere verwerking plaatsheeft.
RD-BEV-020	Beheerfunctionaliteit binnen de (maatwerk)software is verdeeld in rollen.
Interpretatie	Een beheerder als persoon heeft een bepaalde rol. Toegang tot functionaliteit is afhankelijk van de rol.
RD-BEV-021	Een beheerder krijgt binnen de (maatwerk)software slechts toegang tot beheerfunctionaliteit toegewezen aan één rol.
Interpretatie	Meerdere rollen per beheerder is niet mogelijk.
RD-BEV-022	Een beheerder wordt door de (maatwerk)software geauthentiseerd en voor maximaal één rol geautoriseerd via het IAM (Identity Access Management) systeem van de Rijksdienst voor Identiteitsgegevens.
Interpretatie	De applicatie is te koppelen aan het bestaande IAM.
RD-BEV-024	Er mag geen gebruik kunnen worden gemaakt van mobiele code anders binnen een web gebruikersinterface het gebruik van Javascript.
Interpretatie	Alleen vertrouwde code is in de interface toegestaan.
RD-BEV-031	Na het succesvol aanmelden moet de beheerapplicatie van de stelselomgeving de sessiegegevens vernieuwen.
Interpretatie	Om het eventueel kapen van sessies tegen te gaan krijgt een gebruiker een nieuwe sessie na het aanmelden.
RD-BEV-033	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
Interpretatie	De procedure voor het aanmelden lekt geen gegevens.
RD-BEV-034	Er mag geen informatie (zoals bijvoorbeeld een vooraf ingevulde gebruikersnamen) getoond worden voordat een beheerder geauthenticeerd en aangelogd is.
Interpretatie	De procedure voor het aanmelden lekt geen gegevens.
RD-BEV-035	Een sessie van een beheerder met de beheerapplicatie is strikt gebonden aan het IP-adres en aan de user-agent (browser) van de beheerder (ter preventie Session Hijacking).
Interpretatie	Ongebruikelijke wijzigingen in de sessie zorgen voor het afmelden van de gebruiker, het beëindigen van de sessie.

5 Testen van NFRs

5.1 Algemeen

Gezien de aard van IV staat functioneel het bewaken van de integriteit van de gegevens bovenaan de doelstellingen gevolgd door controle op het proces dat de applicatie ondersteunt. Het aspect beschikbaarheid is functioneel gezien vanuit gebruik van de applicatie minder van belang. De waarborgen voor vertrouwelijkheid bij IV zijn hoofdzakelijk buiten de applicatie belegd wanneer de ISC beheerder gebruik maakt van de IV applicatie.

De maatregelen voor ontwikkeling en de uit te voeren testen bij IV zijn per NFR opgenomen in het Excel overzicht 'NFRs IV'. Deze betreffen:

- Peer reviews (ontwikkeling)
- Steekproefsgewijs testen (ontwikkeling)
- Expertreviews (ontwikkeling en test)
- Vastlegging in SAD (ontwikkeling)
- Vastlegging in TO (ontwikkeling)
- Expliciet testen (test)

Merk op: In voorkomende gevallen kan een NFR beveiligbaarheid een relatie hebben met een ander type NFR zoals bijvoorbeeld betrouwbaarheid als het gaat om logging. De NFRs liggen soms dicht tegen elkaar aan.

In de invulling van het normenkader codekwaliteit is ook aandacht voor maatregelen die de NFRs van beveiligbaarheid ondersteunen. In het bijzonder de tooling die op punten toeziet die beveiliging direct raken zoals de "security" categorie voor Findbugs en PMD.

De ontwikkelaars maken gebruik van SonarQube voor het bewaken van de gestelde normen. De regels uit de normen dekken op het gebied van beveiligbaarheid de OWASP RD-BEV-030 NFR af. Naast de OWASP regels zijn onder andere ook CWE en SANS25 regels opgenomen. Dit is dus een bredere groep regels dan die van OWASP zoals gesteld in de NFRs.

Naar de letter is er tot dusver geen invulling gegeven aan het gevraagde OWASP argumentatie per punt in softwaredocumentatie, wel is er gelet op de onderliggende aspecten. Om verwarring te voorkomen is het nodig deze (als verwijzing) toe te voegen en daarbij gebruik te maken van de hier opgenomen interpretatie, of deze van toepassing is en een verwijzing naar de inzet van SonarQube met de OWASP regels.

Bij de controle op nieuwe versies van de onderliggend gebruikte softwarecomponenten komt nu niet expliciet het aspect veiligheid aan bod. De controle vindt nu incidenteel plaats. Dit zou het project in een periodieke afweging moeten betrekken voor het doorvoeren van de inzet.

5.2 Initiële Vulling

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.
Testen	Het testen van validatie, integriteit zit verwerkt in de functionele testen van IV. Zo is er de syntax- en preconditie-controle waarin dit aan bod komt. Daarnaast is er sprake van codereviews in de teams en de inzet van tooling.

	Advies: Voor deze eis zijn geen aanvullende testen nodig.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
Testen	Het gedrag van de applicatie bij storingen en foutmeldingen is te testen bij voorkomende scenario's. Een aantal zit al in functionele testen verwerkt. Op onderdelen is mogelijk foutinjectie in testscenario's uit te voeren (de vraag is hoeveel dit toevoegt). Deze eis zal in relatie tot infrastructuur ook terugkomen in testen. Advies: Voor deze eis testen de teams IV zelf op foutsituaties. I&T gaat na hoe de teams dit afdekken en toetsen dit zo mogelijk aan het technisch ontwerp.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
Testen	Advies: Maak een test die naar een andere locatie de log wegschrijft.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
Testen	Het moet mogelijk zijn op basis van de log een beheerder te informeren, alarmeren. Advies: Review of dit technisch mogelijk is.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico's zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.
Testen	OWASP heeft een sterke focus op manipulatie van buitenaf. Voor de IV applicatie is dit niet relevant gezien het gebruik. Aangevuld met de gegevens uit 2014 en 2015 levert dit geen andere, nieuwe punten op die van toepassing kunnen zijn. De uitwerking van de interpretatie voor de OWASP lijst is achteraan opgenomen onder de kop 'Interpretatie OWASP'. Nagaan of in de documentatie is vastgelegd dat een punt van toepassing is. Controle via SOnarQube regels, review van gebruikte software componenten op bekende kwetsbaarheden en expertreview van configuratie op foutgevoeligheid.

	Advies: Ga na of er geen openstaande issues zijn in het SonarQube dashboard. Review de documentatie of in het SAD is opgenomen welke punten van toepassing zijn, of er een verwijzing is naar een overzicht van relevante punten.
RD-BEV-049	Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.
Testen	Autorisatie op onderdelen volgt het principe van 'least privilege'. Nalopen van documentatie op resource toegang en review op het principe. Uiteindelijk komt dit aan bod bij de inrichting van de infrastructuur, systeemsoftware. Advies: Verifieer of in het SAD is beschreven wat de resources zijn die de applicatie gebruikt en of dit overeenkomt met de werkelijkheid.
RD-BEV-032	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintext) Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.
Testen	Advies: Nalopen van de documentatie en review van configuratiebestanden op wachtwoorden. Gebruiker en wachtwoord aanpassen in een testscenario.

5.3 Levering

De uitwerking van dit onderdeel, het opstellen van testen bij de NFRs is niet afgerond.

5.4 Bijhouding

De uitwerking van dit onderdeel, het opstellen van testen bij de NFRs is niet afgerond.

5.5 Beheer

De uitwerking van dit onderdeel, het opstellen van testen bij de NFRs is niet afgerond.

A. Bijlage OWASP

Laatste versie uit 2013 (daarna is geen top 10 meer gepubliceerd – zie owasp.org).

- A1-Injection
    - Een specifieke manipulatie techniek. Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie.
- A2-Broken Authentication and Session Management
    - Het onbedoeld verkrijgen van toegang tot (delen) van functies, het verkrijgen van sleutels, wachtwoorden, etc.
- A3-Cross-Site Scripting (XSS)
    - Validatiefouten in webapplicaties in combinatie met een webbrowser bij de gebruiker. Niet van toepassing.
- A4-Insecure Direct Object References
    - Een specifieke manipulatie techniek. Het verwerken van onvertrouwde data zonder controle of het uitvoeren van functies zonder autorisatie.
- A5-Security Misconfiguration
    - Foutieve configuratie van de applicatie of van de onderliggende lagen in de gebruikte software stack.
- A6-Sensitive Data Exposure
    - Het lekken van gevoelige informatie. Niet van toepassing.
- A7-Missing Function Level Access Control
    - Het onbedoeld verkrijgen van toegang tot (delen) van functies.
- A8-Cross-Site Request Forgery (CSRF)
    - Een aanval gericht op de webbrowser van een gebruiker waarbij een webapplicatie dit kan voorkomen. Niet van toepassing.
- A9-Using Components with Known Vulnerabilities
    - Bekende kwetsbaarheden in gebruikte standaard software componenten.
- A10-Unvalidated Redirects and Forwards
    - Validatie problemen op websites. Niet van toepassing.

Op basis van de in 2016 gepubliceerde ruwe data over 2014 en 2015, in volgorde van het aantal meldingen zou de lijst er als volgt uitzien:

- Number of Cross-Site Scripting (XSS) Vulnerabilities Found (CWE-79)?
    - A3
- Number of SQL Injection Vulnerabilities Found (CWE-89)?
    - A1
- Number of Unchecked Redirect Vulnerabilities Found (CWE-601)?
    - A10
- Nieuw: Number of XML eXternal Entity Injection (XXE) Vulnerabilities Found (CWE-611)?
    - URI referenties buiten het verwachte domein. Niet van toepassing
- Nieuw: Number of Path Traversal Vulnerabilities Found (CWE-22)?
    - Externe invoer die paden in de applicatie beïnvloedt. Niet van toepassing.
- Number of Security Misconfiguration Vulnerabilities Found (CWE-2)?
    - A5
- Nieuw: Number of Cryptographic Vulnerabilities Found (CWEs-310/326/327/etc)?
    - Verkeerd gebruik van cryptografie of verouderde cryptografische software. Variant van A2. Niet van toepassing voor IV.
- Nieuw: Number of Command Injection Vulnerabilities Found (CWE-77)?
    - Commando's doorgeven vanuit externe invoer. A4 en A7 gerelateerd. Niet van toepassing.
- Nieuw: Number of Mass Assignment Vulnerabilities Found (CWE-915)?
    - Externe invoer die attributen, eigenschappen van de applicatie beïnvloedt. Niet van toepassing.
- Number of Session Fixation Vulnerabilities Found (CWE-384)?
    - A2
- Input Validation
    - Generalisatie van A1, A4, A7 en A10.

CWE staat voor Common Weakness Enumeration, een standaard voor het aanduiden van de veelvoorkomende kwetsbaarheden in software.