KPMG
cutting through complexity

Software review BRP

Ministerie van Binnenlandse zaken en Koninkrijksrelaties,

Den Haag

14.I000814

Rapportage v.1.0
11-09-2014

KPMG Advisory
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Phone +31 (0)20 656 8251
Fax +31 (0)20 656 8125

Persoonlijk & Vertrouwelijk
Gedelegeerd opdrachtgever Operatie BRP
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Operatie BRP

Amstelveen, 11 september 2014

Onderwerp: Software review BRP

Onze referentie: 14.I000814

Geachte heer Franke,

Met deze rapportage willen wij u informeren over de resultaten van ons onderzoek naar de kwaliteitsborging in het programma BRP (voorheen mGBA) op het software aspect. Op uw verzoek heeft KPMG Advisory (hierna: KPMG) dit onderzoek uitgevoerd in overeenstemming met de uitgebrachte offerte van 21 maart 2014 met referentie 14.I000814 v2.

Deze rapportage vormt de afsluiting van onze werkzaamheden van dit onderzoek en bevat de belangrijkste bevindingen en aanbevelingen.

De operatie BRP (voorheen mGBA) bouwt aan een centraal onderdeel van het Nederlandse stelsel van basisregistraties. Dat brengt met zich mee dat er hoge eisen worden gesteld aan de kwaliteit en architectuur van de software. In de voortbrengingsprocessen heeft het programma maatregelen getroffen om deze kwaliteit te borgen. Zo maakt de software-ontwikkelorganisatie gebruik van kwaliteitsdashboards zoals deze door het product SonarQube worden geleverd.

KPMG heeft een onderzoek uitgevoerd waarin werd onderzocht of de kwaliteitsmaatregelen gericht zijn op de belangrijke aspecten, bezien vanuit het perspectief van goede en voldoende betrouwbare software, om in productie te gaan.

Uit dit onderzoek komt naar voren dat de genomen kwaliteitsmaatregelen afdoende faciliteiten bieden om de kwaliteit van de code te monitoren en te verbeteren. Hierbij is het belangrijk dat deze faciliteiten worden gebruikt om de kwaliteit continu te monitoren en te verbeteren. Door een recente migratie van de tooling hebben wij niet kunnen vast stellen of de genomen kwaliteitsmaatregelen over een langere periode van tijd effectief zijn geweest.

Ten aanzien van de software kwaliteit zijn er in dit onderzoek een aantal bevindingen gedaan ten aanzien van onderhoudbaarheid, betrouwbaarheid en veiligheid.
Wij adviseren om deze bevindingen op te lossen.

Hoewel buiten scope van deze opdracht, merken wij graag nog een zaak op die belemmeringen kunnen vormen voor een succesvolle afronding van de operatie BRP. Allereerst zijn de functionele en niet functionele eisen nog niet volledig afgestemd. Dit is een belangrijk projectrisico voor het goed en tijdig afronden van het systeem.

Naast deze rapportage leveren wij afzonderlijk de detail beantwoording van de onderzoeksvragen samen met de bevindingen en overzichten op. Deze bijlagen zijn met het rapport verbonden.

Dit rapport is bedoeld voor de operatie BRP om inzicht te krijgen in de software kwaliteitsbeheersing. Het is niet bedoeld voor andere partijen en het gebruik van dit rapport door andere partijen is dan ook voor eigen risico.
KPMG aanvaardt geen aansprakelijkheid voor het gebruik van dit rapport anders dan waarvoor het is opgesteld en aanvaardt geen aansprakelijkheid jegens andere partijen dan het ministerie van Binnenlandse zaken en Koninkrijksrelaties.

Hoogachtend,

KPMG Advisory N.V

drs. J.M.A. (Joost) Koedijk CISA CISM
Partner

Inhoudsopgave

Uw KPMG contactpersonen:

Joost Koedijk
Partner
KPMG Advisory N.V.
koedijk.joost@kpmg.nl

Deborah Hofland
Senior Manager
KPMG Advisory N.V.
hofland.deborah@kpmg.nl

René Pingen
Adviseur
KPMG Advisory N.V.
pingen.rene@kpmg.nl

1. Management samenvatting (1/2)

Door KPMG is een onderzoek uitgevoerd naar de kwaliteitsmaatregelen binnen de operatie BRP ten aanzien van de software kwaliteit.

De ontwikkelomgevingen bieden afdoende faciliteiten om de broncode kwaliteit te monitoren en te verbeteren.

Naast het actief monitoren van de kwaliteit adviseren wij om de bevindingen ten aanzien van onderhoudbaarheid, betrouwbaarheid en veiligheid op te lossen.

Inleiding

Voor u ligt de rapportage van het onderzoek naar de kwaliteitsmaatregelen binnen de operatie BRP ten behoeve van de software kwaliteit. KPMG heeft dit onderzoek tussen mei en september 2014 uitgevoerd op basis van analyse van de kwaliteitsmaatregelen, analyse van de broncode, documentatiestudie en interviews met de ontwikkelaars. Deze managementsamenvatting bevat de belangrijkste bevindingen en aanbevelingen ten opzichte van de kwaliteitsmaatregelen en de softwarekwaliteit.

Scope

In dit onderzoek zijn de daadwerkelijke producten van software ontwikkeling (broncode en documentatie) van de projecten BRP en Migratie getoetst aan de aspecten Onderhoudbaarheid, Betrouwbaarheid en Veiligheid van de ISO 25010 standaard. Van de overige vijf kwaliteitsaspecten uit deze standaard hebben we begrepen dat in het testproces aandacht wordt gegeven aan Functionele geschiktheid en Performance efficiëntie. De aspecten Combineerbaarheid, Bruikbaarheid en Overdraagbaarheid worden vanwege de aard van de systemen als minder relevant beschouwd.

Systeemoverzicht

Binnen de operatie BRP is onderscheid te maken tussen twee deelprojecten, die worden gerealiseerd door twee verschillende teams:

- De BRP software
- De migratie software voor de migratie van GBA naar BRP

Dit onderzoek rapporteert over beide deelprojecten. Waar relevant worden bevindingen expliciet per deelproject gerapporteerd.

Bevindingen en beantwoording onderzoeksvragen

Het onderzoek is gericht op de beantwoording van de volgende vier onderzoeksvragen:

1. Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?

In de ontwikkelomgevingen voor beide deelprojecten wordt gebruik gemaakt van SonarQube ten behoeve van het monitoren van de softwarekwaliteit. De gebruikte set van codeerregels kan gebruikt worden om problemen ten aanzien van o.a. onderhoudbaarheid, betrouwbaarheid en veiligheid detecteren. Voor beter inzicht kunnen er aanvullend een aantal door SonarQube recent geïntroduceerde regels toegevoegd worden.

Door de recente migratie is er slechts beperkt historische informatie van de SonarQube dashboards beschikbaar, waardoor niet vastgesteld kan worden of de kwaliteitsmaatregelen gedurende langere periode effectief zijn geweest. Over de periode eind juni tot eind augustus zijn echter duidelijk verbeteringen geconstateerd.

Wat nog ontbreekt zijn kwaliteitsdoelstellingen waaraan de code moet gaan voldoen.

2. Wat is de onderhoudbaarheid van de applicatie?

De broncode is duidelijk onderverdeeld in subprojecten. Er wordt gebruik gemaakt van open source componenten voor “cross cutting concerns” als logging, webservices en autorisaties.

De migratiesoftware is uitvoerig gedocumenteerd in een architectuurdocument, en de code is grotendeels gedocumenteerd. In de code bevinden zich een aantal grote klassen met een hoge complexiteit en veel afhankelijkheden op externe klassen. Wij hebben begrepen dat een deel van deze complexiteit kan worden verklaard uit het feit dat de migratie software moet werken tussen het oude en nieuwe gegevensmodel. Deze complexiteit bemoeilijkt eventueel toekomstig onderhoud aan de code.

1. Management samenvatting (2/2)

2. Wat is de onderhoudbaarheid van de applicatie? (vervolg)

Van de BRP software is zeer beperkt documentatie beschikbaar. Tevens bevat de code rond het datamodel een aantal bevindingen ten aanzien van complexiteit, cyclische afhankelijkheden en code duplicatie. Dit vormt een beperking voor de onderhoudbaarheid van deze code. Wij hebben begrepen dat een belangrijk deel van de code rond het datamodel is gegenereerd. Het uitgangspunt dat de generatoren niet worden overgedragen aan beheer betekent dat onderhoud aan de broncode rond het datamodel handmatig uitgevoerd dient te worden, en hiermee hoge eisen worden gesteld aan de onderhoudbaarheid van de code.

3. Is de software inherent betrouwbaar?

Beide projecten maken consistent gebruik van foutafhandeling en logging. De dekking van de uitgevoerde tests, is met uitzondering van de code rond het data model, groter dan 60%. Aanvullend wordt er door zowel BRP als migratie gebruik gemaakt van automatische regressietests.

Ten behoeve van het gelijktijdig omgaan met verschillende schrijf en leesoperaties zijn transactiemechanismen nodig om de integriteit van de gegevens te borgen. De mechanismen rondom transacties en locking zijn ten tijde van dit onderzoek nog niet definitief uitgewerkt, waardoor de technische borging van de integriteit van de gegevens niet kan worden onderzocht. Wél is er door BRP een voorstel voor een transactiemechanisme beschreven, wat nog niet formeel is vastgelegd.

4. Is de software inherent veilig?

Voor de beveiliging wordt grotendeels gebruik gemaakt van standaardcomponenten. Echter hebben wij beperkt documentatie aangetroffen rondom de beveiligingsmechanismen. Uit de functionele documentatie is wel een uitgebreid autorisatiemodel gebleken dat goed moet worden getest. In de software zijn een beperkt aantal, en oplosbare, bevindingen met veiligheidsimpact gedaan.

Wij wijzen er echter op dat voor informatiebeveiliging naast goede software, ook een goede inrichting van standaardcomponenten (besturingssysteem, applicatie servers e.d.), hardware en netwerkbeveiliging noodzakelijk is.

Conclusie en aanbevelingen

Met de inrichting van SonarQube kan de softwarekwaliteit goed worden gemonitord. Wij adviseren om op basis van de ingerichte kwaliteitsmaatregelen actief te sturen op verbetering van de codekwaliteit. Periodieke rapportages en externe reviews dragen hieraan bij. Tevens adviseren wij om kwaliteitsdoelen op te stellen waaraan de uiteindelijke software zal moeten voldoen. Wij zijn graag bereid binnen deze opdracht over beide systemen passende kwaliteitsdoelen te adviseren. De opgestelde doelen dienen daarna met de beheerorganisatie te worden afgestemd.

Om de onderhoudbaarheid en betrouwbaarheid van de BRP software te verbeteren dient er geïnvesteerd te worden in het ontwikkelen van systeemdocumentatie en dienen tevens de bevindingen opgelost te worden. Specifiek dient er een keuze gemaakt te worden voor het opleveren van code rond het datamodel, of het opleveren van verbeterde generatoren hiervan.

2. Opdrachtomschrijving en aanpak

De gedelegeerd opdrachtgever van het programma mGBA wil inzicht in de wijze waarop de kwaliteit van de ontwikkelde software wordt beheerst. De kwaliteitsbeheersing moet daarbij worden getoetst vanuit het perspectief van het goed en voldoende betrouwbaar in gebruik nemen van de software.

Uit het onderzoek komen zo mogelijk pragmatische verbeteradviezen om de kwaliteit en de kwaliteitsbeheersing van de software te verbeteren.

Achtergrond

Na een heroriëntatie is besloten om het programma modernisering GBA (mGBA) voort te zetten en de bouw van de Basis Registratie Personen (hierna: BRP) af te ronden binnen een vastgestelde scope en met een aantal randvoorwaarden. Één van de vereiste ingrepen bij dit besluit is het inrichten van Quality Assurance (QA) en het stelselmatig meten van de productiviteit van het programma.

Als onderdeel van de QA voor het programma in te richten voert KPMG om een software review uit.

In deze review wordt met nadruk gekeken naar de wijze waarop het programma zelf de softwarekwaliteitsbeheersing ingericht heeft.

Doel van het onderzoek

Doel van het onderzoek is te komen tot inzicht in de kwaliteit van de software en de beheersing van deze kwaliteit. Zo mogelijk wordt dit inzicht gekoppeld aan een pragmatisch verbeteradvies.

Scope

De scope van het onderzoek beperkt zich tot de broncode, documentatie en kwaliteitsdashboards van de software zoals die door het programma mGBA wordt ontwikkeld. Ter verduidelijking en toelichting zijn enkele gesprekken met de scrum masters en ontwikkelaars van de software gevoerd.

Aanpak

Doordat binnen het project op basis van SonarQube dashboards over de kwaliteit van de software aanwezig zijn, kan daar in dit onderzoek gebruik van worden gemaakt. Dit heeft geleidt tot de volgende vier onderzoeksvragen:

- Hoe zijn de kwaliteitsmaatregelen rond de software-ontwikkeling ingericht?
- Wat is de onderhoudbaarheid van de software?
- Is de software inherent betrouwbaar?
- Is de software inherent veilig?

Om het onderzoek richting te geven zijn per onderzoeksvraag deelvragen geformuleerd.

Allereerst is in dit onderzoek een inventarisatie gemaakt van de informatie die uit dashboards, documentatie en broncode onderzoek te verkrijgen is.

Waar mogelijk is, vanuit de onderzoeksvragen, de verkregen informatie direct vergeleken met van toepassing zijnde kwaliteitsstandaarden en “good practices” uit “de facto” industrie standaarden, specifieke KPMG checklists en de ervaring van het onderzoeksteam. Op deze wijze is een eerste verzameling ruwe bevindingen ontstaan.

Deze bevindingen, gegroepeerd naar onderzoeksvraag, waren de input voor een workshop waarin de bevindingen zijn besproken en afgestemd.

De uitkomsten van de workshop zijn gebruikt om bevindingen aan te scherpen en aanbevelingen op te stellen. Hierna wordt, met afstemming tussen partijen, de rapportage vorm gegeven.

Resultaat

Het resultaat van het onderzoek is deze geschreven rapportage. De bijlagen van deze rapportage omvatten de detail beantwoording van de onderzoeksvragen, bevindingen en overzichten.

De rapportage is bedoeld de gedelegeerd opdrachtgever inzicht te geven in de kwaliteit van software en de kwaliteitsmaatregelen rond de ontwikkeling. Daarnaast worden voor het project (zo mogelijk) aanbevelingen opgenomen voor verbeteringen in de software en de kwaliteitsmaatregelen.

3. Systeembeschrijving

In dit onderzoek wordt gerapporteerd over zowel de BRP als de migratie software.

In de beantwoording van de onderzoeksvragen wordt waar nodig onderscheid gemaakt tussen beide projecten.

Binnen de operatie BRP is onderscheid te maken tussen twee deelprojecten, die worden gerealiseerd door twee verschillende teams:

- De BRP software;
- De migratie software.

In de beantwoording van de onderzoeksvragen van dit rapport wordt waar nodig onderscheid gemaakt tussen deze projecten.
De gedetailleerde bevindingen worden per project gerapporteerd.

Overzicht BRP

De onderzochte versie van BRP bestaat uit de volgende componenten:

- Gegenereerde code rondom het datamodel. Het datamodel beschrijft de entiteiten. Dit model is gegenereerd met zelf ontwikkelde generatoren, waarbij in de code geen duiding van generatie is opgenomen. De generatoren zijn niet meegenomen in dit onderzoek;
- Een expressietaal om o.a. bevragingen met behulp van business rules mogelijk te maken;
- Webservices voor afnemers en gemeenten:
  - Bijhouding;
  - Bevraging.
- Levering voorziet o.a. in toegang tot de gegevens, protocollering en synchronisatie services.

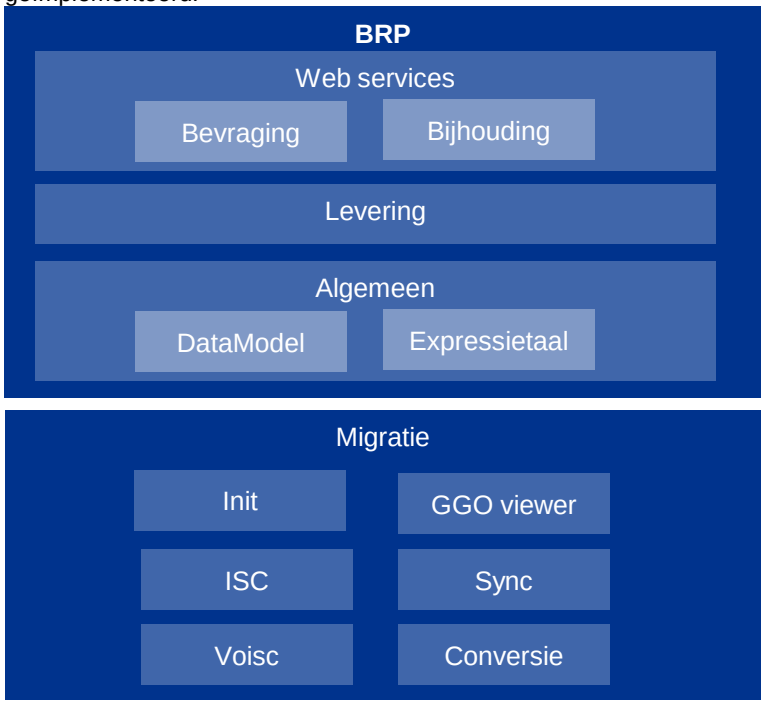
Overzicht Migratie

Het migratie project bestaat uit de volgende componenten:

- Initiële vulling (Init) van de BRP-voorziening;
- Conversie van persoonsgegevens tussen GBA en BRP;
- Synchronisatie service (Sync) voor het synchroniseren met de BRP database;
- Verzend en ontvangst interstelsel communicatie (Voisc) voor het verzenden en ontvangen van berichten van en naar afnemers;
- Interstelsel communicatie (ISC) voorziet in de transformatie en uitwisseling van berichten tussen de systemen;
- GGO Viewer is een beheertool waarmee inzicht wordt verschaft in de conversieresultaten.

Huidige versie systeem

Ten tijde van dit onderzoek is zowel de migratie als BRP software nog in ontwikkeling, waardoor nog niet alle componenten volledig zijn geïmplementeerd.



Figuur 1: Vereenvoudigd overzicht van BRP en Migratie.

4. Aanbevelingen

1. Maak gebruik van de genomen kwaliteitsmaatregelen, stuur op verbetering van de codekwaliteit

De ontwikkelomgeving omvat met o.a. SonarQube en Jenkins, faciliteiten om de kwaliteit van de ontwikkelde code te monitoren. Door gebruik te maken van een uitgebreide set regels in SonarQube is het mogelijk om verschillende kwaliteitsaspecten van de code te monitoren. Hoewel subtiele stijlverschillen mogelijk zijn, adviseren wij om zowel BRP als migratie gebruik te maken van eenzelfde set regels. Deze set kan gebaseerd zijn op de huidige set van migratie aangevuld met de additionele squid metrieken. Hiermee wordt aangesloten op “good practices” uit de industrie.

Wij adviseren om continue te sturen op verbetering van de codekwaliteit, waarbij weloverwogen keuzes worden gemaakt. Concreet kunnen hiervoor de volgende maatregelen worden genomen:

- Stel kwaliteitsdoelstellingen op ten aanzien van de codekwaliteit en neem deze op in het Sonar dashboard. Wij zijn graag bereid binnen deze opdracht over beide systemen passende kwaliteitsdoelstellingen te adviseren.
- Stem de kwaliteitsdoelstellingen af met de beheerorganisatie.
- Monitor de codekwaliteit door middel van periodieke rapportages uit SonarQube, bijvoorbeeld aan het eind van iedere sprint.
- Herhaal over 3 maanden een extern softwarekwaliteitsonderzoek. Afhankelijk van de resultaten is daarna herhaling iedere 6 maanden opportuun.

2. Ontwikkel documentatie, voornamelijk voor BRP

Ten tijde van dit onderzoek bleek de beschikbare documentatie voor BRP zeer beperkt. Van de migratie is een uitgebreid architectuurdocument aanwezig. Wel ontbreken nog aspecten rondom transacties en beveiliging. Wij adviseren om te investeren in het ontwikkelen van (technische) documentatie, waarbij wij alvast aandacht willen geven aan:

- Technische architectuur van de applicatie;
- Transactie- en lockingmechanismen;
- Web services en hieraan gerelateerde berichtdefinities, inclusief foutberichten;
- Documentatie met betrekking tot veiligheidsmechanismen, waaronder authenticatie en sessiemanagement.

3. Verbeter de codekwaliteit BRP datamodel

Het datamodel is gegenereerd met behulp van zelfgeschreven generatoren. Het uitgangspunt ten tijde van dit onderzoek is dat de generatoren niet worden opgeleverd en dat daarmee wijzigingen na oplevering handmatig in de code gemaakt moeten worden.

Dit betekent dat de onderhoudbaarheid van de gegenereerde code voldoende moet zijn. Gezien de hoeveelheid bevindingen rondom complexiteit, code duplicatie en cyclische afhankelijkheden adviseren wij om de codekwaliteit van de gegenereerde code te verbeteren zodat deze gaat voldoen aan de kwaliteitsdoelstellingen.

Indien er alsnog besloten wordt om de generatoren op te leveren, dient er:

- Aanvullend onderzoek gedaan te worden naar de codekwaliteit van de generatoren, waarbij ook strenge eisen ten aanzien van onderhoudbaarheid moeten gelden;
- Duidelijk onderscheid gemaakt te worden tussen gegenereerde code en code die aan te passen is door de ontwikkelaar.

4. Werk het transactie en locking model verder uit, en implementeer en test dit

Een robuust transactie- en lockingmechanisme is noodzakelijk om onder andere in geval van gelijktijdige schrijf en leesoperaties en foutsituaties de integriteit van gegevens te borgen:

- Werk het voorgestelde transactiemechanisme verder uit op basis van de functionele en niet-functionele eisen, waarbij de integriteit van gegevens geborgd kan worden;
- Implementeer, documenteer en test dit mechanisme uitvoerig.

KPMG

cutting through complexity™