



cutting through complexity

Herhaling onderzoek broncode BRP

Rapportage definitief

Ministerie van Binnenlandse zaken en
Koninkrijksrelaties

Den Haag

14.I000814 Heronderzoek, v1.1

30 april 2015





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 en Vertrouwelijk

Gedelegeerd opdrachtgever Operatie BRP
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Operatie BRP

Amstelveen, 30 april 2015

Onderwerp: Herhaling onderzoek broncode BRP

Onze referentie: 14.I000814 Heronderzoek

Geachte heer Franke,

Met deze rapportage willen wij u informeren over de resultaten van de herhaling van ons onderzoek naar de kwaliteitsborging in het programma BRP (voorheen mGBA) voor zover het kwaliteit van de software betreft. Op uw verzoek heeft KPMG Advisory N.V. (hierna: KPMG) dit onderzoek uitgevoerd in overeenstemming met de uitgebrachte offerte met referentie 14.I000814 heronderzoek d.d. 19 december 2014.

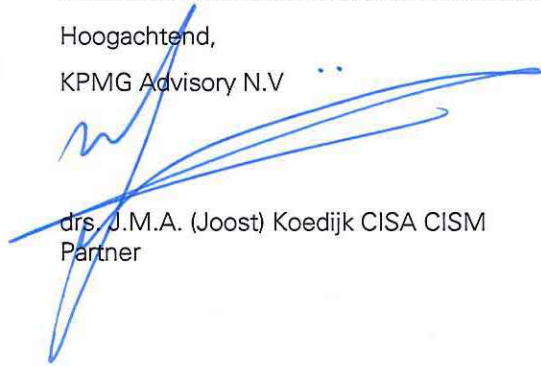
Deze rapportage vormt de afsluiting van onze werkzaamheden en bevat een managementsamenvatting met de context van het onderzoek, alsmede de belangrijkste bevindingen en aanbevelingen. In het vervolg van het rapport zijn de bevindingen in detail uitgewerkt. Wij wijzen erop dat deze managementsamenvatting en factoren niet als zelfstandig stuk moeten worden gezien, doch in samenhang met het gehele rapport dienen te worden beoordeeld.

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

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

Lars Tijhuis

Adviseur

KPMG Advisory N.V.

tijhuis.lars@kpmg.nl

Managementsamenvatting

De opdracht

Aanbevelingen

Pagina

3

5

6

Door KPMG is een onderzoek herhaald naar de kwaliteitsmaatregelen binnen de operatie BRP ten aanzien van de ontwikkelde software waarbij wederom kwaliteitskarakteristieken (conform standaard ISO25010) van de software in kaart zijn gebracht.

Uit het onderzoek blijkt dat er, mede naar aanleiding van eerdere aanbevelingen, duidelijke stappen zijn gezet om de kwaliteit van de software te waarborgen.

Inleiding

Voor u ligt de rapportage van het onderzoek naar de kwaliteitsmaatregelen binnen Operatie BRP ten behoeve van de ontwikkelde software. Doel van dit onderzoek is om, vanuit een onafhankelijke positie, invulling te geven aan de herhaling van het onderzoek naar de kwaliteitsmaatregelen binnen Operatie BRP. Het programma Operatie BRP heeft in de notitie "Normenkader codekwaliteit Centrale BRP-voorzieningen" d.d. 13 januari 2015 een zevental kwaliteitsdoelen opgesteld. In dit onderzoek is tevens in kaart gebracht in welke mate de software reeds aan deze kwaliteitsdoelen voldoet.

KPMG heeft dit onderzoek in maart 2015 uitgevoerd op basis van analyse van kwaliteitsmaatregelen, broncode (versie van 11 maart 2015), documentatiestudie en interviews met de ontwikkelaars. Deze managementsamenvatting bevat de belangrijkste bevindingen.

Dit onderzoek heeft zich geconcentreerd op de beantwoording van een viertal onderzoeksvragen en de mate waarin opvolging is gegeven aan aanbevelingen uit eerdere onderzoeken.

Algemeen beeld

Het programma Operatie BRP 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. Deze zijn ingericht conform gestelde kwaliteitsdoelen, wat sturing op deze doelen mogelijk maakt.

KPMG heeft het eerdere onderzoek van september 2014 herhaald om vast te stellen of de kwaliteitsmaatregelen juist zijn geïmplementeerd en of de kwaliteit van de software over de assen Onderhoudbaarheid, Betrouwbaarheid en Veiligheid voldoet om in productie te gaan.

Uit het onderzoek blijkt dat er, mede naar aanleiding van eerdere aanbevelingen, duidelijke stappen zijn gezet om de kwaliteit van de software te waarborgen.

Zo zijn er kwaliteitsdoelen voor de software opgesteld en is er goede progressie te zien in de beschikbare documentatie wat de Onderhoudbaarheid van de software ten goede komt. Hoewel er conform verwachting voortgang is geboekt ten opzichte van het eerdere onderzoek, wordt niet aan alle door Operatie BRP opgestelde kwaliteitsdoelen voldaan; voor "blocking" en "critical" issues, Inline documentatie en code duplicatie zijn de doelen wel gehaald.

Hoewel in de afgelopen periode voortgang is geboekt zijn er punten waarop de softwarekwaliteit verder verbeterd kan worden. Wij adviseren op basis van de ingerichte kwaliteitsmaatregelen te blijven sturen op verbetering van de codekwaliteit en documentatie. Hierbij hoort ook een nieuwe externe review waarvan het goed zou zijn als die samenvalt met de eerste inzage in de broncode.

Onderzoeksvragen

Hieronder is beknopt de beantwoording van de vier onderzoeksvragen opgenomen.

1. Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?

Voor de monitoring van de softwarekwaliteit wordt SonarQube gebruikt. Hierin zijn dashboards ingericht voor zowel BRP als Migratie conform de in de stuurgroep vastgelegde kwaliteitsdoelen (januari 2015) inclusief de codeerregels.

De kwaliteitsdoelen bevatten een afbakening die leidt tot uitzondering van delen van de code voor specifieke regels; dit wordt gedaan aan de hand van markeringen in de code welke worden herkend door de gebruikte tooling. Het aantal markeringen is erg groot en markeringen worden niet altijd op een eenduidige wijze toegepast. Ook missen de markeringen veelal een gedocumenteerde verantwoording. Dit kan voor een buitenstaander overkomen als een tekortkoming in kwaliteit.

In de projecten BRP en Migratie wordt anders omgegaan met uitzonderingen op de codeerregels. Het gemixte gebruik van de twee methoden heeft ertoe geleid dat de huidige Rule Compliance Index, die tevens terugkomt in de kwaliteitsdoelen (kwaliteitsdoel 7), iets positiever uitvalt dan daadwerkelijk het geval is. De impact hiervan is echter beperkt.

Hoewel in de afgelopen periode voortgang is geboekt zijn er punten waarop de softwarekwaliteit verder verbeterd kan worden.

Wij adviseren op basis van de ingerichte kwaliteitsmaatregelen te blijven sturen op verbetering van de codekwaliteit en documentatie. Hierbij hoort ook een nieuwe externe review waarvan het goed zou zijn als die samenvalt met de eerste openbaarmaking van de broncode.

2. Wat is de Onderhoudbaarheid van de software?

In het BRP-project zijn grote vorderingen gemaakt met betrekking tot de (met name) technische documentatie. Dit is echter nog een 'work in progress' en verdient nog verdere aandacht. Door RvIG zijn non-functional requirements (NFR's) opgesteld naar de categorieën uit ISO 25010 hetgeen in lijn is met "good practices". Wel valt op dat de formulering van de requirements in de categorie Beveiligbaarheid aanscherping verdient.

In de afbakening van de kwaliteitsdoelen is aangegeven dat ook gegenereerde code moet voldoen aan deze doelen. Inherent aan het gebruik van deze code generatoren is een herhaling van een afwijking ten aanzien van cyclische afhankelijkheden. Door een hoog aantal uitzonderingen met betrekking tot deze cyclische afhankelijkheden (kwaliteitsdoel 6) is de Onderhoudbaarheid van de gegenereerde code in beperkte mate gewaarborgd.

Omdat de implementatie van de vastgestelde kwaliteitsdoelen in de monitoringsoftware pas in januari is uitgevoerd, zijn trends ten aanzien van de softwarekwaliteit van vóór 21 januari 2015 niet inzichtelijk. Hierdoor kan niet eenduidig worden vastgesteld hoe de Onderhoudbaarheid van de software zich voor deze tijd heeft ontwikkeld.

3. Is de software inherent betrouwbaar?

Ten aanzien van de kwaliteitsdoelen op het gebied van Veiligheid en Betrouwbaarheid (kwaliteitsdoel 2) is geconstateerd dat de onderzochte code nog niet geheel aan deze doelen voldoet. Afwijkingen betreffen veelal de foutafhandeling en logging.

Wij hebben goede vooruitgang geconstateerd ten aanzien van de testdekking bij beide projecten. Het kwaliteitsdoel rond testdekking (kwaliteitsdoel 3) is echter nog niet behaald. Het BRP-project zit dicht tegen het doel aan, het Migratie project loopt iets achter.

Ten behoeve van het gelijktijdig omgaan met verschillende schrijf- en leesoperaties zijn transactiemechanismen nodig om de integriteit van de gegevens te borgen. Wij hebben vooruitgang waargenomen in de documentatie van dit mechanisme.

4. Is de software inherent veilig?

In het onderzoek van september 2014 zijn zwakheden in gebruikte (externe) componenten aangetroffen. Deze zijn tot op heden nog niet opgepakt. Ook zijn er in dit onderzoek bij beide projecten nieuwe zwakheden in gebruikte componenten gevonden, wat de Veiligheid niet ten goede komt.

Het vasthouden aan gemaakte architectuur keuzes (zoals het gebruik van JBoss) heeft als implicatie dat het niet mogelijk is enkele zwakheden op te lossen. Wij hebben begrepen dat wordt onderzocht of deze component vervangen kan worden.

Kwaliteitsdoelen

Hoewel er conform verwachting voortgang is geboekt ten opzichte van het eerdere onderzoek, wordt niet aan alle door Operatie BRP opgestelde kwaliteitsdoelen voldaan; voor "blocking" en "critical" issues (kwaliteitsdoel 1), Inline documentatie (kwaliteitsdoel 4) en code duplicatie (kwaliteitsdoel 5) zijn de doelen wel gehaald.

Tijdens het onderzoek kwam naar voren dat de formulering van de kwaliteitsdoelen zorgt voor enige verwarring. Daarnaast zijn sinds de vaststelling van de kwaliteitsdoelen een aantal aanvullende codeerregels opgenomen in de "de facto" industriestandaard. Deze nieuwe inzichten geven mogelijk aanleiding tot een wijziging in de kwaliteitsdoelen.

Aanbevelingen

Sinds september 2014 is er goede vooruitgang geboekt met betrekking tot kwaliteitsbeheersing. Wij hebben de volgende aanbevelingen die verder in dit rapport in meer detail zijn uitgewerkt:

- Maak uitzonderingen op de gestelde kwaliteitsdoelen inzichtelijk.
- Herformuleer de gestelde kwaliteitsdoelen en overweeg aanvullende codeerregels op te nemen in de regelset.
- Richt een proces in voor het borgen van de Veiligheid van standaard componenten.
- Blijf documentatie uitbreiden.
- Maak broncode gereed voor eerste publieke inzage.

De gedelegeerd opdrachtgever van Operatie BRP 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. Deze opdracht is een vervolg op de eerdere analyse van september 2014 en brengt in kaart wat de vooruitgang is in de kwaliteitsbeheersing.

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

Achtergrond

Na een heroriëntatie zet het programma Operatie BRP de bouw van de Basis Registratie Personen (hierna: BRP) voort. Als aanvullende Quality Assurance (QA) maatregel heeft het programma aan KPMG gevraagd een review uit te voeren op de kwaliteitsmaatregelen rond de softwareontwikkeling die binnen het programma plaatsvindt. Een eerste review hiernaar heeft rond de zomer van 2014 plaatsgevonden.

Naar aanleiding van dit eerste kwaliteitsonderzoek heeft KPMG geadviseerd enerzijds kwaliteitsdoelen voor de software op te stellen, hetgeen in een adviesbrief van KPMG nader is geformuleerd. Anderzijds is het advies periodiek een onderzoek naar de kwaliteit van de broncode te laten uitvoeren door een onafhankelijke partij.

Operatie BRP heeft in de notitie “Normenkader codekwaliteit Centrale BRP-voorzieningen” d.d. 13 januari 2015 kwaliteitsdoelen geformuleerd, welke in januari 2015 door KPMG zijn gereviewed. Deze kwaliteitsdoelen zijn daarna door de stuurgroep vastgelegd.

Doel van het onderzoek

Doel van het onderzoek is om, vanuit een onafhankelijke positie, invulling te geven aan de herhaling van het onderzoek naar de kwaliteitsmaatregelen conform ons onderzoeksplan “Software en architectuur review mGBA” van 21 maart 2014 met kenmerk 14.I000814 v2. Hierbij is tevens in kaart gebracht in welke mate de software reeds aan de opgestelde kwaliteitsdoelen voldoet.

Scope

De scope van het onderzoek beperkt zich tot de broncode, documentatie en kwaliteitsdashboards van de software zoals die door het programma Operatie BRP wordt ontwikkeld. Wanneer gerefereerd wordt aan “de kwaliteitsdoelen” worden hiermee de kwaliteitsdoelen uit het document “Normenkader codekwaliteit Centrale BRP-voorzieningen” d.d. 13 januari 2015 bedoeld.

Aanpak

Het onderzoek richt zich op vier deelonderwerpen:

- Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?

- Wat is de Onderhoudbaarheid van de software?
- Is de software inherent betrouwbaar?
- Is de software inherent veilig?

De toetsing van de vier deelonderwerpen heeft op dezelfde wijze plaatsgevonden zoals is beschreven in het genoemde onderzoeksplan dat ook aan de basis stond van het eerdere onderzoek. In de rapportage wordt daarbij tevens in kaart gebracht in welke mate de software reeds aan de gestelde kwaliteitsdoelen voldoet.

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” industriestandaarden, specifieke KPMG checklists en de ervaring van het onderzoeksteam.

Deze bevindingen, gegroepeerd naar onderzoeksvraag, zijn besproken en afgestemd in het kader van hoor en wederhoor.

Er heeft een centrale meeting plaats gevonden om bevindingen aan te scherpen en aanbevelingen op te stellen. Hierna is, 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, de kwaliteitsmaatregelen rond de ontwikkeling en de mate waarin thans aan de gestelde kwaliteitsdoelen wordt voldaan. Daarnaast zijn voor het project (zo mogelijk) aanbevelingen opgenomen voor verbeteringen in de software en de kwaliteitsmaatregelen.

1. ***Maak uitzonderingen op de gestelde kwaliteitsdoelen inzichtelijk***

Delen van de code waarvoor is bepaald dat deze niet aan de kwaliteitsdoelen hoeven te voldoen worden buiten de monitoring geplaatst middels markeringen in de broncode. Deze markeringen missen veelal een gedocumenteerde toelichting. Daarbij is het aantal markeringen erg groot en is niet altijd gespecificeerd om welke codeerregels het gaat.

Ons advies is op een eenduidige manier toelichting te documenteren voor de markeringen. Voorstel is deze te categoriseren en in een document aan te geven waarom verschillende categorieën buiten beschouwing worden gelaten voor de kwaliteitsdoelen. Dit verbetert het inzicht in de omvang en redenen voor het niet voldoen aan de kwaliteitsdoelen. De categorieën zouden bijvoorbeeld kunnen zijn: 'Third party libraries', 'JBoss code', 'Hergebruikte GBA-V code', 'BRP generatoren' en 'Uitgesloten voor controle op cyclische afhankelijkheid'.

2. ***Herformuleer de gestelde kwaliteitsdoelen en overweeg aanvullende codeerregels op te nemen in de regelset***

De formulering van de kwaliteitsdoelen zorgt voor enige verwarring. Wij adviseren deze doelen iets anders te formuleren zodat duidelijk is dat goed gemotiveerde uitzonderingen ook mogelijk zijn rond Veiligheid en Betrouwbaarheid (kwaliteitsdoel 2) en dat (alle) uitzonderingen niet meetellen in de RCI berekening (kwaliteitsdoel 7). De voorgestelde herformulering van de tekst op pagina 5 van de kwaliteitsdoelen luidt:

"Explains" maken geen onderdeel uit van de telling ten behoeve van de normen 1 t/m 6. Ten aanzien van norm 7 wordt de specifieke bijdrage van de issues die de "Explains" veroorzaken in de berekening van de Rule Compliance Index in kaart gebracht; de berekening van de index wordt voor deze bijdrage gecorrigeerd door de door "explains" veroorzaakte bevindingen niet in de telling mee te nemen.

Tevens zijn sinds de vaststelling van de kwaliteitsdoelen een aantal aanvullende codeerregels opgenomen in de "de facto" industriestandaard. Deze regels leveren aanvullende bevindingen op, ook op de aspecten Veiligheid en Betrouwbaarheid. Wij adviseren deze aanvullende regels na te lopen en zo nodig in de kwaliteitsdoelen op te nemen.

3. ***Richt een proces in voor het borgen van de Veiligheid van standaard componenten***

Naar "good practice" wordt veelal gebruik gemaakt van standaard (externe) componenten. Een groeiend aantal componenten bevatten echter zwakheden ten aanzien van de Veiligheid. Gezien deze bevinding ook terugkwam in september 2014, adviseren wij wederom een periodiek en controlebaar proces in te richten waarin wordt onderzocht of er nieuwe zwakheden zijn ontstaan of ontdekt in de externe componenten. Hierbij kan tevens een check naar nieuwere versies worden meegenomen.

4. ***Blijf documentatie uitbreiden***

In het BRP-project is veel vooruitgang te zien in de beschikbare (technische) documentatie. Vanuit deze documenten zou nog explicieter opgenomen kunnen worden welke requirements worden vervuld met de beschreven componenten. Daarnaast is het een 'work in progress' en adviseren wij de beschikbare documentatie te blijven uitbreiden.

Het SAD van het Migratie project had in september 2014 een aantal openstaande TODO's, deze zijn sindsdien nog niet opgepakt. Wij adviseren de documentatie te updaten naar de huidige stand van zaken.

Door RvIG zijn NFR's opgesteld naar de categorieën zoals beschreven in ISO25010. De NFR's in de categorie Beveiligbaarheid geven voornamelijk de praktische invulling voor dit onderwerp. Wij adviseren het programma de herformulering van deze doelen tot verifieerbare requirements te bespreken met RvIG. De huidige requirements kunnen dienen als de praktische invulling van de categorie Beveiligbaarheid.

5. ***Maak broncode gereed voor eerste publieke inzage***

De broncode bevat in-line commentaar wat in een aantal gevallen duidt op het niet volledig afronden van een taak. Wij adviseren voor de eerste publieke inzage een kritische blik te werpen op deze (reeds met de ontwikkelteams gedeelde) commentaren en bijbehorende stukken code.

Tevens adviseren wij het uitvoeren van een volgende review op de kwaliteit van de broncode tegelijk te laten plaatsvinden met de eerste inzage in de broncode zodat bekend is wat het publiek te zien krijgt.



cutting through complexity™

© 2015 KPMG Advisory N.V., ingeschreven bij het handelsregister in Nederland onder nummer 33263682, is lid van het KPMG-netwerk van zelfstandige ondernemingen die verbonden zijn aan KPMG International Cooperative ("KPMG International"), een Zwitserse entiteit. Alle rechten voorbehouden. Gedrukt in Nederland.

De naam KPMG, logo en 'cutting through complexity' zijn geregistreerde merken van KPMG International Cooperative.