Herhaling onderzoek broncode BRP en review kwaliteitsdoelen januari 2017

Rapportage voor het ministerie van Binnenlandse Zaken en Koninkrijksrelatie
Referentie 16.A1600007506 F

—

12 april 2017

KPMG Advisory N.V.
Postbus 74500
1070 DB Amsterdam

Laan van Langerhuize 1
1186 DS Amstelveen
Telefoon (020) 656 8251
www.kpmg.nl

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

Amstelveen, 12 april 2017

Onderwerp: Herhaling onderzoek broncode en review kwaliteitsdoelen
Onze referentie: 16.A1600007506 F

Geachte heer Franke,

Met deze rapportage willen wij u informeren over de resultaten van ons onderzoek naar de broncode en de review van de kwaliteitsdoelen ten behoeve van de softwarekwaliteit voor de Basisregistratie Personen (BRP). Op uw verzoek heeft KPMG Advisory N.V. (hierna: KPMG) dit onderzoek uitgevoerd in overeenstemming met de uitgebrachte offerte met referentie '16.A1600007506 F herhaling onderzoek broncode en review kwaliteitsdoelen januari 2017' d.d. 24 januari 2017.

Deze rapportage vormt de afsluiting van onze werkzaamheden en bevat een managementsamenvatting welke de context, scope en resultaten van het onderzoek beschrijft. Een verdere uitwerking van context en resultaten is in de vervolghoofdstukken opgenomen. In de bijlagen zijn de detailbevindingen van zowel het broncodeonderzoek als het onderzoek naar de nieuwe kwaliteitsdoelen te vinden. Wij wijzen erop dat deze managementsamenvatting en resultaten niet als zelfstandig stuk moeten worden gezien, doch in samenhang met het gehele rapport dienen te worden beoordeeld.

Dit rapport is bedoeld voor Operatie BRP (oBRP) om inzicht te geven in de kwaliteit van de BRP-software en de in het programma daartoe genomen kwaliteitsmaatregelen. 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. Koedijk CISA CISM
Partner

Inhoudsopgave

KPMG

Management-samenvatting

Algemeen beeld

Inleiding

Voor u ligt de rapportage van het onderzoek naar de kwaliteit van de broncode van de BRP-software en de binnen het programma Operatie BRP (oBRP) genomen kwaliteitsmaatregelen.

Doel van dit onderzoek is om, vanuit een onafhankelijke positie, invulling te geven aan een herhaling van het periodieke onderzoek naar de kwaliteit van de broncode van de BRP-software.

KPMG heeft dit onderzoek in januari en februari 2017 uitgevoerd op basis van analyse van de bestaande en voorgestelde kwaliteitsdoelen, broncode (versie van 6 december 2016) en documentatiestudie.

Algemeen beeld

Het programma oBRP 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.

KPMG heeft eerdere onderzoeken naar het kwaliteitssysteem rondom de broncode uitgevoerd, namelijk in september 2014, maart 2015, september 2015, april 2016 en augustus 2016. Dit onderzoek naar het kwaliteitssysteem is opnieuw uitgevoerd.

Uit ons onderzoek komt naar voren dat de huidige software, de versie van december 2016, van een hoger kwaliteitsniveau is dan de software zoals onderzocht in augustus 2016. De code van 6 december 2016 voldoet volledig aan de door de stuurgroep vastgestelde kwaliteitsdoelen.

Om aan te sluiten bij ontwikkelingen in de industrie en betere ondersteuning te bieden aan ontwikkelaars heeft oBRP een geactualiseerde set van kwaliteitsdoelen opgesteld. Hiermee geeft het programma opvolging aan onze eerdere aanbevelingen.

Deze voorgestelde nieuwe kwaliteitsdoelen maken gebruik van de meest recente tooling voor softwarekwaliteit, zoals deze eind 2016 als open source beschikbaar was. Met de nieuwe kwaliteitsdoelen wordt een hoger kwaliteitsniveau nagestreefd door het gebruik van een 'strengere' regelset. Een eerste meting op basis van de nieuwe doelen resulteert in meer afwijkingen hetgeen gezien de verhoging van het doel verklaarbaar is. De tussentijdse meting uit maart 2017 laat zien dat al veel van deze afwijkingen met beperkte inspanning opgelost zijn.

Onderzoeksvragen

Hieronder worden de specifieke onderzoeksvragen beknopt beantwoord.

1a. Hoe zijn de kwaliteitsmaatregelen rond de softwareontwikkeling ingericht?

Voor de monitoring van de softwarekwaliteit wordt SonarQube gebruikt. Hiermee wordt inzicht verschaft in de status van de kwaliteitsdoelen en worden ontwikkelaars voorzien van feedback over de kwaliteit van de broncode en op te lossen issues.

1b. Wat is de onderhoudbaarheid van de software?

In vergelijking met het vorige meetmoment laten de onderhoudbaarheidsmetrieken een positieve ontwikkeling zien. De omvang van de code is toegenomen, terwijl er een verbetering is te zien ten opzichte van de kwaliteitsdoelen. De kwaliteitsdoelen ten opzichte van documentatie, testdekking en codeduplicatie worden alle behaald.

1c. Is de software inherent betrouwbaar?

Ten aanzien van de codeerregels op het gebied van betrouwbaarheid voldoet de software op 6 december 2016 volledig aan de bestaande kwaliteitsdoelen. Eerdere bevindingen ten aanzien van betrouwbaarheid uit april 2016 zijn opgelost en er zijn geen nieuwe bevindingen bijgekomen.

Beantwoording onderzoeksvragen

1d. Is de software inherent veilig?

De broncode voldoet aan de bestaande kwaliteitsdoelen ten aanzien van veiligheid. In de broncode worden geen bevindingen over de regels ten aanzien van veiligheid gerapporteerd. Wel merken we op dat de BRP-software gebruikmaakt van componenten die bekende zwakheden ten aanzien van veiligheid bevatten.

2a. In hoeverre sluiten de door operatie BRP opgestelde kwaliteitsdoelen aan bij good practices?

In december 2016 is door oBRP gekozen om te migreren naar de nieuwe versie van de SonarQube tooling (versie 6.2) en de kwaliteitsdoelen te actualiseren. De voornaamste wijziging in de kwaliteitsdoelen is een nieuwe set van codeerregels. Als basis voor de nieuwe codeerregels heeft oBRP het 'Sonar Way'-profiel van SonarQube geselecteerd waarmee, in lijn met onze eerdere adviezen, aangesloten wordt bij de 'de facto' industriestandaard en 'good practices'.

Aanvullend heeft oBRP 69 regels geselecteerd waarmee de kwaliteitsdoelen op een nog hoger niveau komen te liggen.

2b. Wat zijn de verschillen tussen de oude en nieuwe kwaliteitsdoelen, en wat is de impact van de wijziging op de kwaliteitsborging van de codekwaliteit binnen BRP?

De door oBRP voorgestelde 7 kwaliteitsdoelen zijn op hoofdlijnen onveranderd ten opzichte van de bestaande kwaliteitsdoelen. Het belangrijkste verschil is het gebruik van een nieuwe regelset, waardoor kwaliteitsdoelen 1, 2, 6 en 7 op een andere manier worden vastgesteld.

De voorgestelde nieuwe regelset biedt een breder inzicht in de kwaliteit van de code dan de bestaande regelset. De code die voldoet aan de voorgestelde (strengere) regels zal hierdoor van hogere kwaliteit zijn.

2c. Hoe verhoudt de software zich ten opzichte van de oude én nieuwe kwaliteitsdoelen die binnen operatie BRP worden gehanteerd?

De code van 6 december 2016 voldoet volledig aan de door de stuurgroep vastgestelde kwaliteitsdoelen. Ten opzichte van augustus 2016 hebben wij een positieve ontwikkeling vastgesteld van de mate waarin aan de bestaande kwaliteitsdoelen wordt voldaan.

Tevens wordt met de nieuwe kwaliteitsdoelen een hoger kwaliteitsniveau nagestreefd. Een eerste meting op basis van deze nieuwe doelen resulteert in meer afwijkingen, hetgeen gezien de verhoging van het doel verklaarbaar is. De tussentijdse meting uit maart 2017 laat zien dat al veel van deze afwijkingen met beperkte inspanning opgelost zijn.

2d. Wat is de ontwikkeling van de onderhoudbaarheidsmetrieken van de software zoals die periodiek met behulp van de SonarQube tooling worden verzameld?

In vergelijking met het vorige meetmoment in augustus 2016 is de BRP-software verder doorontwikkeld en zijn er meer regels broncode bijgekomen. Deze doorontwikkeling heeft geen negatief effect gehad op onderhoudbaarheidsmetrieken als codeduplicatie. Zoals hierboven aangegeven laat een tussentijdse meting in maart 2016 verdere verbeteringen ten aanzien van de onderhoudbaarheidsmetrieken zien.

KPMG

Aanbevelingen

Aanbevelingen

1. Leg de voorgestelde kwaliteitsdoelen vast

Wij bevelen aan de voorgestelde kwaliteitsdoelen voor te leggen aan de stuurgroep en deze daarmee te bekrachtigen.

2. Blijf aandacht geven aan de kwaliteit van de broncode (ook tijdens het ontwikkelproces) zodat bij een volgend onderzoek de broncode aan de voorgestelde kwaliteitsdoelen voldoet

De broncode zoals bekeken in dit onderzoek voldoet aan de bestaande kwaliteitsdoelen uit het bestaande kwaliteitssysteem. Om aan de voorgestelde kwaliteitsdoelen te voldoen, adviseren wij om de verbeterslag voort te zetten en actief te blijven sturen op de kwaliteit van de broncode zodat de broncode aan alle nieuwe voorgestelde kwaliteitsdoelen gaat voldoen. Het is daarbij verstandig om de voortgang in de verbetering van de broncode ten opzichte van de kwaliteitsdoelen extern te laten vaststellen over circa zes maanden.

3. Expliciteer de kosten-en-batenafweging die binnen de projectgroep is gemaakt voor de keuze voor aanvullende kwaliteitsregels (bovenop de reeds voorgestelde maatregelen)

We hebben 10 regels geïdentificeerd die mogelijk in de voorgestelde regelset kunnen worden opgenomen. Wij bevelen aan om te overwegen of de impact van het gebruiken van (enkele van) deze regels opweegt tegen de te bereiken kwaliteitsverbetering.

Wij adviseren bij de overweging prioriteit te geven aan de regels die de meeste impact hebben op de kwaliteit van de code. Dit zijn bijvoorbeeld regels zoals regel Squid:S1698 in SonarQube (zie ook bijlage II).

4. Vermijd onderdrukkingen van bevindingen in de tooling

Door annotaties in de broncode kunnen bevindingen in de SonarQube tooling worden onderdrukt. Wij adviseren grondig te kijken naar het gebruik van deze onderdrukkingen en deze (zo veel mogelijk) te vermijden.

Daar waar onderdrukkingen (vooralsnog) noodzakelijk zijn draagt goede documentatie bij aan de onderhoudbaarheid en algemene kwaliteit van de software.

5. Optimaliseer de rapportage in de dashboards over de voorgestelde kwaliteitsdoelen

Er zijn kleine afwijkingen tussen de dashboardrapportage en het precieze kwaliteitsdoel. Wij adviseren om de dashboards en de kwaliteitsdoelen precies op elkaar aan te laten sluiten.

6. Houd de ontwikkelingen binnen de industrie in de gaten

Het product SonarQube is in ontwikkeling en er worden periodiek nieuwe codeerregels ontwikkeld om aanvullende kwetsbaarheden, bugs en andere issues te detecteren. Hiermee wordt aangesloten bij ontwikkelingen in de industrie.

Wij adviseren om, zoals ook in het verleden is gebeurd, deze ontwikkelingen te volgen. Het is daarbij goed om, eventueel na inbeheername, een volgend moment te prikken waarin de kwaliteitsdoelen worden getoetst aan de dan actuele inzichten in de industrie.

7. Gebruik de nieuwste versies van externe libraries

Wij adviseren nieuwere versies van de libraries te gebruiken of andere maatregelen te treffen die de zwakheden in de gebruikte libraries mitigeren. Tevens adviseren wij om hier regelmatig op te controleren, bijvoorbeeld voor iedere oplevering. Ook adviseren wij om de gebruikte versies in één Maven-bestand te definiëren. Dit is reeds de opzet, maar is niet consequent doorgevoerd.

KPMG on social media

KPMG app