beroepsonderwijs bedrijfsleven

Project Start Architectuur

Digitaal ontwikkelplatform Kwalificatiestructuur mbo (DoK)

CIO OFFICE

Versie	1.2
Datum	03-12-2024
Opsteller	Rijk Rijkse en Maarten Kok
Input en review	Mike van den Muijsenberg, Jacob Molenaar

1 Managementsamenvatting

De huidige applicatie voor het ontwikkelen, beheren en publiceren van de kwalificatiestructuur mbo (DigiK) is aan vervanging toe. Deze PSA is opgesteld als documentatie ten behoeve van het aanbestedingstraject voor de ontwikkeling, implicatie en integratie van een nieuw ontwikkelplatform.

In dit document is met name beschreven welke plek het Digitaal ontwikkelplatform Kwalificatiestructuur mbo (DoK) in zal nemen in het architectuurlandschap van SBB. Dit is uitgewerkt in de beschrijving van de *koppelvlakken*, oftewel met welke componenten DoK moet kunnen interacteren. Hoofdstuk Informatiebeveiliging geeft het beleid aan van SBB op dit gebied, zodat leverancier hierop is voorbereid.

Na gunning zal de PSA, in afstemming tussen CIO-office, projectleiding en leverancier, verder in detail uitgewerkt worden.

2 Inhoudsopgave

3 Doelstelling PSA

Dit Project Start Architectuur (PSA) -document is opgesteld ten behoeve van het aanbestedingstraject voor de ontwikkeling van DoK. Dit document wordt tegelijkertijd aangeboden met:

- de aanbestedingsleidraad;
- het Programma van Eisen;
- een globale informatieanalyse van de kwalificatiestructuur;
- voorbeelden van producten.

Deze PSA beschrijft niet de primaire functionaliteiten van DoK, maar geeft weer in welk architectuurlandschap DoK moet kunnen opereren. Dit uit zich met name in de beschrijving van de koppelvlakken die DoK moet kunnen leveren of waar DoK op moet kunnen aansluiten. De PSA bevat hiermee aanvullende eisen voor de leverancier.

In de volgende fase, tijdens de ontwikkeling, implementatie en integratie van DoK kunnen de volgende personen gebruik maken van dit document als leidraad (in algemene zin):

- Een bestuurder heeft met een PSA de meest belangrijke 'ins' en 'outs' beschikbaar om een verantwoord besluit te nemen over een project.
- De projectmanager kan met een PSA, aan de hand van kaders en randvoorwaarden, de oplossingsrichting van een project duidelijk maken. Dit geeft inzicht in de oplossing waaraan gedacht wordt en welke consequenties (en risico's) er aan inrichtingskeuzes vastzitten. Dit vergemakkelijkt de uitvoering.
- De architect kan, gedurende het project, grip houden op de uiteindelijke SOLL situatie en tijdig veranderingen opnemen. Het is ook een controlemiddel voor het in de goede richting sturen van een project.
- De professionals kunnen met een PSA gerichter aan de slag om concrete, passende oplossingen voor te stellen.

4 Aanleiding project

4.1 Korte beschrijving van het project

Opdrachtgever: Irene Wolff
Projectleider: Laura Thoma-Eradus

SBB heeft een infrastructuur voor het produceren, beheren en publiceren van de informatie m.b.t. de kwalificatiestructuur mbo: het zogenoemde DigiK-systeem. Dit succesvolle systeem is in zijn huidige vorm na een periode van ongeveer 16 jaar aan het einde van haar levenscyclus gekomen. SBB kan met haar huidige content-infrastructuur onvoldoende aan de nieuwe informatiebehoeften van de eindgebruikers voldoen. Daarom wil SBB zich fundamenteel beraden op een nieuwe strategie voor het beheren en publiceren van de kwalificatiestructuur mbo. Daarbij is ook de vraag actueel naar de mogelijkheden om het huidige DigiK-systeem te vervangen door een nieuw platform. Dit platform heeft als werktitel Digitaal ontwikkelplatform Kwalificatiestructuur mbo (DoK).

Het projectdoel is het contracteren van een strategische partner voor de langere termijn die de voor DoK gewenste functionaliteit en technologie levert, configureert en mogelijk nieuwe functionaliteiten ontwikkelt die ondersteuning bieden aan de toekomstvisie ontwikkeling kwalificatiestructuur mbo. Met DoK kan de huidige applicatie DigiK worden vervangen.

4.2 Projectarchitectuur

Het project waarbinnen deze PSA opgeleverd wordt, is de aanbesteding voor DoK. Pas voorafgaand aan en tijdens de volgende fase, bij de Ontwikkeling, migratie en integratie van DoK, zal de PSA, in afstemming met de leverancier, meer in detail uitgewerkt worden.

4.3 Drijfveren

4.3.1 Businessdrijfveren

- Huidige applicatie DigiK voldoet niet meer en kan niet meer worden aangepast of uitgebreid
- Gebruik van de kwalificatiestructuur voor meerdere doelgroepen (LLO) ondersteunen
- Hergebruik van componenten mogelijk maken
- Kwalificatiestructuur kunnen verbinden aan een gemeenschappelijke skillstaal (CompetentNL)

4.3.2 Architectuurdrijfveren

- Applicatie aansluiten op het dataplatform (publicatieproces)
- Referentiedata afnemen van het dataplatform
- Hergebruik van inhoudelijke componenten
- Authenticatie conform SBB-standaarden
- Geïntegreerd workflow management
- Toekomstgerichte flexibiliteit in samenstelling informatieproducten
- Coöperatieve opdrachtgever – leverancier relatie waarbij partijen elkaar versterken

5 Afhankelijkheden en overeenkomsten

5.1 Informatie

Het format en de inhoud van de gepubliceerde kwalificatiestructuur is wettelijk vastgesteld door het ministerie van OCW. De in het Programma van Eisen benoemde paradigmaverschuiving beslaat daarom de manier waarop de producten tot stand komen, niet de vorm van het wettelijke product.

5.2 Applicatie/techniek

Momenteel wordt een deel van de workflow ondersteund door de applicatie Topdesk. De informatie van deze processen moet beoordeeld worden in welke mate en vorm deze gemigreerd dienen te worden naar DoK.

De opslag van DigiK is gebaseerd op een XML-structuur. Voor de herbruikbaarheid van de data, met name voor opname in het dataplatform, wordt nu tijdelijk de data geëxporteerd en getransformeerd naar een relationele database, DigiK-replicatieDb genaamd. Deze database is in principe ook de bron voor migratie naar de opslag van de applicatie DoK.

5.3 Overige projecten

Vanuit het programma ‘Vaardig met vaardigheden’ (voor de ontwikkeling van CompetentNL) wordt gewerkt aan een infrastructuur binnen SBB, waarbij via een dataplatform de kwalificatiestructuur beschikbaar gemaakt wordt voor Linked (open) Data. Gedurende het proces van de aanbesteding voor DoK worden daarbij architecturale keuzes gemaakt die logischerwijs nog niet in deze PSA beschreven kunnen worden. Mogelijk ontstaan er hierdoor accentverschuivingen in de architectuur, die relevant kunnen zijn voor de ontwikkeling van DoK.

6 Architectuur

6.1 Relevante architectuurprincipes

AI02	Beschrijf informatie-objecten systematisch
	Beschrijf de toegepaste informatieobjecten voor een dienst systematisch in een informatiemodel en voorzie de informatieobjecten van een unieke identificatie.
AI07	Gestandaardiseerde koppelvlakken
	Applicaties bieden gestandaardiseerde koppelvlakken.
AI10	Gegevensopslag
	Opslaan bij de bron.
CM01	Eigenaarschap is belegd
	Voor bedrijfsfuncties, bedrijfsprocessen, data en applicaties is het eigenaarschap eenduidig belegd.
DM06	Evolutie van koppelvlakken
	Er wordt nadrukkelijk rekening gehouden met evolutie van de interface die uitwisseling van gegevens tussen informatiesystemen verzorgt.
IB01	Gecentraliseerd, 'Identity Access Management'
	Gecentraliseerd, 'Identity Access Management'.
IB04	Authenticatie eindgebruikers
	Authenticatie vindt plaats op het niveau van eindgebruikers, in de gehele keten.
IB05	Geauthentiseerde en geautoriseerde toegang
	Toegang tot IT systemen wordt geauthentiseerd en geautoriseerd.
IB06	Risicoanalyse is leidend
	Risicoanalyse wordt centraal gecoördineerd en decentraal uitgevoerd. Beveiligingsmaatregelen zijn gebaseerd op het risicoprofiel.
OC07	Geoptimaliseerd inloggen
	Gebruikers worden niet geconfronteerd met overbodige authenticaties
SD01	Hosting
	SaaS vóór (Azure) cloud vóór hosted PaaS
SV03	Webbrowser onafhankelijk
	Websites werken op alle gangbare webbrowsers.
SW04	Automatisering gegevensuitwisseling
	Gegevensuitwisselingen die frequent of in grote aantallen plaats vinden worden geautomatiseerd.
SW05	Administratie koppelvlakken
	Koppelvlakken worden expliciet gedocumenteerd en geregistreerd in een centrale administratie.

6.2 Bedrijfsarchitectuur

In hoofdlijnen raakt de ontwikkeling, migratie en integratie van DoK de volgende bedrijfsprocessen:

- Ontwikkelen kwalificatiestructuur
- Onderhouden kwalificatiestructuur
- Publiceren kwalificatiestructuur
- Uitvoeren onderwijsvergelijking
- Uitvoeren diplomawaardering

Daarnaast is in het PvE ook aangegeven dat er multidisciplinair gewerkt moet kunnen worden met DoK. Primair heeft dat impact op de bovengenoemde processen. In welke mate de processen van andere disciplines hiermee ook veranderen, is voor dit project buiten scope.

6.3 Informatie-architectuur

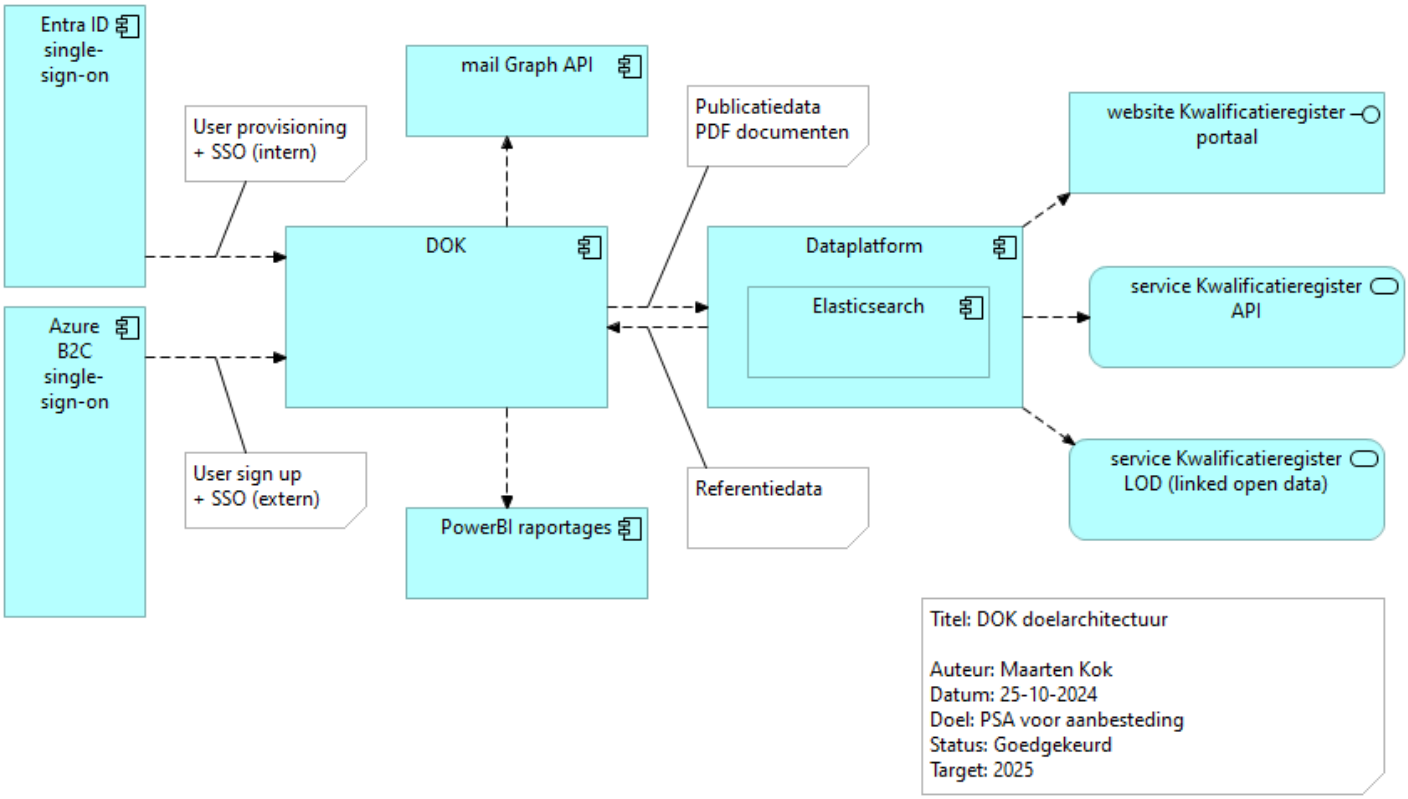
De globale informatie-architectuur wordt separaat opgeleverd bij de documentatie voor de aanbesteding. Conceptueel vindt er geen wijziging plaats in de te publiceren data. Wel vindt er, gerelateerd aan de genoemde paradigmaverschuiving, een grote wijziging plaats in hoe de producten tot stand komen. Er wordt meer gebruik gemaakt van standaard waardelijsten en herbruikbare componenten ten opzichte van de huidige situatie. Er zal dus een uitgebreide analyse moeten plaatsvinden welke elementen uit de huidige data alleen als product moeten worden overgenomen en welke aanvullend als waardelijsten en herbruikbare componenten dient worden opgeslagen.

6.4 Applicatie/technische architectuur

Hoewel het ontwikkelplatform een SAAS-oplossing zal zijn, dient het te interacteren met het architectuurlandschap van SBB. Onderstaande schets geeft de relevante onderdelen daarvan weer, met de nadruk op de koppelvlakken waarmee DoK zal dienen te functioneren.

De koppelvlakken zijn:

- SSO en userprovisioning voor internen
- SSO en sign-up voor externen
- Mailfunctionaliteit via MSGraph
- Dataplatform (referentiedata ophalen)
- Dataplatform (data leveren)
- PowerBI
- Toekomstige (AI) systemen



Single-sign-on en userprovisioning voor internen

SBB medewerkers loggen in op DoK met hun SBB account. Single-sign-on wordt gerealiseerd met één van de drie technische profielen van Micorosoft Azure EntraID: OAuth 2.0, OpenID connect of SAML 2.0. In overleg met SBB wordt userprovisioning gerealiseerd door een koppeling met HelloID, EntraID, of op basis van claims tijdens de inlog. Met de userprovisioning zijn geen verdere handmatige acties benodigd tijdens in- of uit- diensttreding.
Bij hun eerste inlog krijgen internen een standaard rol toegewezen. Op basis van claims kunnen specifieke rollen worden toegekend. Op basis van een workflowproces kunnen verdere rollen en/of machtigingen in DoK worden toegekend.
Let op: Userprovisioning op basis van claims tijdens de inlog is alleen mogelijk wanneer het (beveiligings- en licentietechnisch) niet nodig is om een account te deactiveren.

Single-sign-on en sign-up voor externen

Externen waarmee SBB samenwerkt loggen in op DoK met een lokaal of federated account vanuit de Azure Bussines to Consumer omgeving van SBB. In overleg met SBB wordt een technisch profiel van AzureB2C gekozen en ingericht om DoK te koppelen voor single-sign-on en user-sign-up van accounts van externen.
Bij hun eerste inlog krijgen externen een standaard rol toegewezen. Op basis van een workflowproces kan een uitnodiging worden verstuurd voor inloggen en verdere rollen en/of machtigingen in DoK worden toegekend.

Mailfunctionaliteit via MSGraph

Het verzenden van e-mail vanuit DoK vindt plaats met Microsoft Graph REST API v1.0 van de Azure omgeving van SBB.

Dataplatform (data leveren)

Het dataplatform is een centrale *hub* voor alle uitwisseling van data binnen SBB, alsook voor de publicatie van data naar externen. Het dataplatform is nog in ontwikkeling en op termijn zullen er aanvullende componenten op worden aangesloten. Momenteel is de kwalificatiestructuur al opgenomen op het dataplatform, via de eerder genoemde DigiK-replicatieDB als tussenstap. Van DoK verwachten wij dat de ontwikkelde en onderhouden data van de kwalificatiestructuur beschikbaar wordt gesteld aan het dataplatform. Het dataplatform bestaat uit een centraal Azure datalake, waarvoor de inname van data wordt gedaan door Azure Synapse. DoK dient dus een geschikte connector te leveren die aangeroepen kan worden door Synapse. We gaan ervan uit dat zowel data (van componenten, producten en workflow) als PDF's van producten worden opgenomen in het dataplatform.

Binnen het dataplatform maakt SBB gebruik van Elastic Search. Wanneer DoK geïntegreerd werkt met Elastic Search wil SBB met de opdrachtnemer onderzoeken om Elastic Search enkelvoudig te implementeren. Hetzij in DoK hetzij in de instantie van SBB Dataplatform.

Dataplatform (referentiedata ophalen)

Het dataplatform heeft daarnaast ook als functie om generieke en externe data voor heel SBB beschikbaar te stellen. Dit impliceert dat alle data die niet in DoK beheerd wordt, ook niet specifiek voor DoK opgeslagen wordt. Het dataplatform voorziet in REST API's, die waar nodig op maat gemaakt kunnen worden, waarmee de referentiedata *live* opgehaald kan worden.

PowerBI

Standaardrapportage wordt binnen DoK geleverd. Rapportages over gepubliceerde kwalificatiegegevens en dossiers kunnen worden gemaakt vanuit het dataplatform. Voor specifieke SBB werkprocessen, SBB KPI's en ongepubliceerde gegevens levert DoK een (API-) interface waar vanuit SBB hiervoor zelf PowerBI rapportages kan opstellen die automatisch worden geactualiseerd.

Toekomstige (AI) systemen

SBB wil in de toekomst externe systemen kunnen koppelen om gegevens te kunnen analyseren, vergelijken en bewerken. Denk aan AI-systemen die voorstellen kunnen doen voor ontdubbelen van componenten of het toevoegen van (gewogen) relaties tussen componenten.
DoK biedt een API-interface die toegang heeft tot componenten, elementen en producten, relaties en (workflow) processen voor het analyseren, aanpassen, en voorstellen van aanpassingen, ontdubbelingen en toevoegingen met CRUD-operaties (create, read, update, delete).

6.5 Ontwikkelarchitectuur

Gezien het feit dat SBB een SAAS-oplossing uitvraagt is de ontwikkelarchitectuur hier nu niet relevant. Wel willen we inzicht hierin, zie de vragen in de gunningscriteria over 'ontwikkelstack online platform'.

7 Informatiebeveiliging

Informatiebeveiliging is erop gericht de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te waarborgen en het bewust nemen van informatiebeveiligingsrisico's om digitaliseringskansen optimaal te benutten. De rol van de Information Security Officer hierin is faciliterend, richtinggevend, kaderstellend en toetsend. De ISO zorgt voor de juiste balans tussen innovatie en risicobeheersing, in lijn met de strategische doelen van SBB en borging en continue verbetering van informatiebeveiligingsmaatregelen.

7.1 Toetsingskader

Het toetsingskader voor informatiebeveiliging moet worden ingevuld bij de aanschaf van elke IT-applicatie of -component. Dit geeft een overzicht van de criteria waaraan de applicatie is getoetst en biedt een gedocumenteerde onderbouwing. Dit document kan tijdens (onaangekondigde) audits uitgevoerd door SBB als basis worden gebruikt.

Bovendien dienen er duidelijke KPI's voor de applicatie vastgesteld te worden en dient de beoordeling van prestaties opgenomen te worden in het proces van leveranciersbeoordelingen. Dit zorgt ervoor dat leveranciers aan de gestelde eisen blijven voldoen en ondersteunt een continue monitoring van de kwaliteit en veiligheid van DOK.

7.2 Rollen en verantwoordelijkheden

Het schriftelijk vaststellen en duidelijk definiëren van de juiste rollen en verantwoordelijkheden is het startpunt voor het beschermen van onze informatievoorziening. Dit is de basis voor een effectieve governance. Eigenaarschap voor applicatie, proces en data dient worden te belegd.

7.3 Bedrijfsimpactanalyse

De verantwoordelijken zullen een bedrijfsimpactanalyse (BIA) uitvoeren om een gedegen classificatie van de informatievoorziening vast te stellen. Deze classificatie is gebaseerd op zowel interne als externe afspraken en houdt rekening met stakeholders en de te leveren waarde. De classificatie bepaalt het vereiste beveiligingsniveau en vormt de basis voor de implementatie van passende beveiligingsmaatregelen. Afhankelijk van de toegewezen classificatie zal het volgende beleid van toepassing zijn:

- Beleid voor logisch toegangsbeheer;
- Cryptografiebeleid;
- Beleid voor logging en monitoring;
- Beleid voor gebruikersapparatuur en systemen;
- Backupbeleid;
- Bedrijfscontinuïteitsbeleid;
- Etc.

Standaarden zorgen voor de baseline van het beleid. Het beleid wordt ten uitvoer gebracht aan de hand van vast te stellen procedures.

7.4 Risicobeoordeling

Risicomanagement is het proces van het identificeren, analyseren, beoordelen, mitigeren en accepteren van informatiebeveiligingsrisico's. Samen met de verantwoordelijken zal een risicobeoordeling worden uitgevoerd, zodat alle risico's worden gemitigeerd tot een voor SBB acceptabel risiconiveau.

Er zijn vooraf vastgestelde risico acceptatiecriteria en alleen de proceseigenaar kan risico's accepteren of vermijden. Indien risico's niet volledig kunnen worden gemitigeerd, zal er in overleg met de proceseigenaar een risico-acceptatieovereenkomst (RAO) worden opgesteld. In deze overeenkomst worden de aard van het risico en de termijn van acceptatie vastgelegd, waarbij er afspraken worden gemaakt over herbeoordeling en aanvullende/ compenserende maatregelen.

In het risicoregister worden de risico's opgenomen en jaarlijks geëvalueerd. Kritische risico's worden overlegd met het MT of DT. Door dit proces kunnen risico's beheersbaar blijven en vinden er transparante afspraken plaats over de acceptatie van resterende risico's binnen SBB.

7.5 Wettelijk kader

Bij het uitbreiden of implementeren van nieuwe functionaliteiten moet worden getoetst of deze voldoen aan geldende en toekomstige wet- en regelgeving. In paragraaf 6.4 wordt de (toekomstige) toepassing van AI beschreven. Zoals bij Security en Privacy by Design, moeten ook bij AI-toepassingen dezelfde processen te doorlopen en moet AI by design worden toegepast, in overeenstemming met de nationale wetgeving: de AI-verordening die op 1 augustus 2024 in werking is getreden. Deze verordening zal naar verwachting de komende jaren verder worden aangescherpt.

Wanneer de AI-verordening niet wordt nageleefd, kan dit (aanzienlijke) consequenties hebben. Deze sancties omvatten boetes tot 35 miljoen euro per overtreding of 7% van de wereldwijde omzet van de organisatie. Voor kleinere administratieve overtredingen kunnen boetes oplopen tot 7,5 miljoen euro of 1,5% van de wereldwijde omzet.

8 Monitoring en nazorg

Gedurende de ontwikkeling, implementatie en integratie wordt van de leverancier van DoK verwacht (naast de reguliere projectafstemming) periodiek af te stemmen met het CIO-office van SBB. De doelen van deze afstemming zijn:

- toetsen/ verantwoorden van de ontwikkeling ten opzichte van de PSA;
- in gezamenlijkheid verdere invulling te kunnen geven aan de gekozen architectuur;
- adviseren/ beoordelen wat de Project Eind Architectuur kan en moet zijn.