Aansluitvoorwaarden

ARCHITECTUUR, INTEGRATIE, RANDVOORWAARDEN

Architecten
RADBOUD UNIVERSITEIT | INFORMATIE MANAGEMENT
6 JULI 2018

Inhoudsopgave

1. Inleiding

In dit document worden de aansluitvoorwaarden van de Radboud Universiteit beschreven voor nieuwe en gewijzigde applicaties in het bestaande applicatielandschap. Een aan te sluiten applicatie dient gekoppeld te worden aan de concernsystemen en/of flankerende applicaties die de Radboud Universiteit gebruikt en in de toekomst kan gaan gebruiken. De samenhang en wisselwerking met de concernsystemen en de koppelingen met flankerende applicaties vormen een belangrijk onderdeel van elke inbedding van een nieuwe of gewijzigde applicatie, of dit nu via aanschaf of uitbesteding gebeurt, al dan niet na een aanbestedingstraject.

Dit document bestaat uit drie delen:

1. Doelarchitectuur – de missie van de universiteit, architectuurprincipes en de algemene architectuur van het applicatielandschap.
2. Integratiearchitectuur – een toelichting op de infrastructuur waarmee applicaties worden gekoppeld en data worden uitgewisseld, aangevuld met algemene voorwaarden m.b.t. de afbakening van verantwoordelijkheden van de leverancier van de applicatie enerzijds en de Radboud Universiteit anderzijds ten aanzien van koppelingen, interfaces en data-uitwisseling.
3. Applicatiearchitectuur – voorwaarden waaraan elke te integreren applicatie moet voldoen.

2. Doelarchitectuur

Missie van de Radboud Universiteit

De Radboud Universiteit ziet ICT als een van de middelen om de doelstellingen van de instelling te bereiken. De missie en doelstellingen van de Radboud Universiteit zijn daarom vaak bepalend voor keuzes die op ICT-gebied worden gemaakt. Onderstaande teksten geven een beeld van onze missie en komen rechtstreeks uit “De Radboud Universiteit op weg naar 2020”, ons strategisch plan. De volledige tekst van het plan is op verzoek beschikbaar.

“De slogan van de Radboud Universiteit voor de komende periode luidt *Change perspective*. Dat is een uitnodiging en belofte tegelijk. Het is de uitnodiging aan onze studenten en onze medewerkers om in interactie met de ander het eigen perspectief tegen het licht te houden, te verbreden en waar nodig bij te stellen. Maar het is ook de belofte aan onze aankomende studenten en medewerkers dat ze aan onze universiteit hun perspectief en daarmee dat van de samenleving kunnen verleggen.”

Onze missie op het gebied van onderwijs luidt: *Academisch onderwijs van hoog niveau.*

“De Radboud Universiteit wil haar studenten academisch vormen in een internationale context en ze stimuleren de onafhankelijke zoektocht naar het nieuwe aan te gaan, in het besef dat die zoektocht naar kennis ook na de studie aan de universiteit doorgaat. Kwaliteit, binding en duidelijkheid zijn de kernwoorden die ons onderwijs drijven.

De Radboud Universiteit levert – zo blijkt steeds weer uit beoordelingen en enquêtes – academisch onderwijs van hoge kwaliteit. Studenten en docenten werken samen aan de academische vorming van de student. Voor studenten is helder welke prestaties van hen worden verwacht. De universiteit biedt duidelijkheid over de doelen van het onderwijs en procedures en normen bij toetsing. De student is verantwoordelijk voor zijn eigen leerproces, maar toont ook verantwoordelijkheid voor zijn medestudenten en spreekt hen daarop aan. In Nijmegen studeer je niet alleen!

Naast kwaliteit en duidelijkheid is binding met de opleiding een belangrijke voorwaarde voor studiesucces. Daarom zet de Radboud Universiteit in op een substantieel aantal contacturen en kleinschalig onderwijs met oog voor de individuele student. Het onderwijs nodigt uit tot discussie en zelfstudie, de campus biedt de studenten daarvoor de gelegenheid. De Radboud Universiteit kiest er nadrukkelijk voor om een campusuniversiteit te zijn, waar het contact tussen docenten en studenten en studenten onderling centraal staat. ICT wordt ingezet om dit te ondersteunen, als middel om de kwaliteit van het onderwijs te versterken.

Het onderwijs aan de Radboud Universiteit is sterk verweven met onderzoek; iedere student moet tenminste zelf een keer aan onderzoek deelnemen, zelf de weg afleggen naar het onbekende. Voor de docenten betekent dit dat zij onderzoek doen en uit een eigen onderzoekspraktijk kunnen putten.

De Radboud Universiteit stimuleert studenten over de grenzen van de eigen studie heen te kijken. Daarom bevordert ze een roostering die het voor studenten eenvoudiger maakt delen van hun onderwijs bij andere faculteiten te volgen.

Het onderwijsprogramma stimuleert studenten een deel van de studie in het buitenland door te brengen, zodat ze na hun studie kunnen functioneren in een internationale context. Daarom zijn ook in de Nederlandstalige bachelor-opleidingen Engelstalige modules opgenomen. Internationalisering van ons onderwijs betekent ook dat meer buitenlandse studenten aan onze universiteit studeren."

Onze missie op het gebied van onderzoek is: *Wetenschappelijk onderzoek van wereldniveau.*

"De Radboud Universiteit koestert een levendige, succesvolle onderzoeksgemeenschap die nieuwe inzichten en ideeën genereert en zo vanuit het hele spectrum aan wetenschapsgebieden nationaal en internationaal bijdraagt aan de culturele, maatschappelijke en economische ontwikkeling. Het onderzoek voedt het onderwijs; de verbinding tussen onderwijs en onderzoek is de belangrijkste pijler in het streven naar excellentie.

Het onderzoek van de Radboud Universiteit is georganiseerd in onderzoeksinstituten. De onderzoeksinstituten zoeken aansluiting op de nationale en Europese onderzoeksagenda en beïnvloeden deze zoveel als mogelijk is. Dat vraagt een proactieve houding, van zowel de wetenschappelijk staf als van het ondersteunend personeel.

De Radboud Universiteit stimuleert de samenwerking van haar onderzoeksinstituten met sterke partners in binnen- en buitenland. Dat is de basis voor een succesvolle positionering in de Europese onderzoeksruimte, zowel voor het door nieuwsgierigheid gedreven onderzoek (European Research Council) als voor het meer toepassingsgerichte onderzoek (Horizon 2020).

Onderzoeksprogramma's zijn internationaal competitief. De Radboud Universiteit heeft zich de afgelopen decennia ontwikkeld als toonaangevend op tien wetenschapsgebieden: organische chemie, vastestoffysica, astrofysica, microbiologie, cyber security, cognitieve neurowetenschappen, infectieziekten en immunologie, antropogenetica, taalwetenschap en ondernemingsgericht recht. We koesteren onze kracht zoals die is gegroeid en zetten er versterkt op in.

Daarnaast levert de Radboud Universiteit toonaangevende bijdragen aan het debat over de maatschappelijke thema's: Europa en zijn werelden, Taal en communicatie, Ontwikkeling van de samenleving en haar inrichting, Gedrag en opvoeding, Moleculen en materialen, Water en wetlands en Diagnostiek en behandeling op maat (*Personalized Medicine*).

Omdat promovendi voor het overgrote deel hun carrière buiten de wetenschap vervolgen, besteden we in hun opleiding aandacht aan meer algemene academische vaardigheden.

Binnen alle onderzoeksinstituten heerst een onderzoeksklimaat waarin zorgvuldigheid en verantwoordelijkheid gedijen. Wetenschappelijke integriteit is vanzelfsprekend. In een even kritische als veilige cultuur werken onderzoekers samen en bevragen elkaar. Leidinggevende en medewerker zijn hiervoor samen verantwoordelijk."

Architectuurprincipes

De Radboud Universiteit hanteert 8 algemene architectuurprincipes. De principes zijn gebaseerd op het strategisch plan van de Radboud Universiteit, relevante wet- en regelgeving en de Hoger Onderwijs Referentie Architectuur (HORA[1]). Naleving van de architectuurprincipes is geen doel op zich; de principes faciliteren de realisatie van de doelstellingen van de universiteit.

Er bestaat geen rangorde of prioritering bij deze principes, ze wegen even zwaar. De principes worden hieronder gegeven, inclusief hun implicaties. Dit is een uittreksel van het RU Architectuurprincipes document zoals vastgesteld in juni 2015. De volledige tekst is op verzoek beschikbaar.

Wij zorgen voor klantvriendelijke en betrouwbare informatiediensten

- Processen zijn leidend bij de inrichting van informatiediensten.
- Informatie is geïntegreerd beschikbaar.
- Voor elk relevant gegeven is één authentieke bron beschikbaar.
- Er wordt gebruik gemaakt van een eenduidig gedefinieerd gegevensmodel.
- De kwaliteit van alle onderdelen van de informatiediensten is geborgd.
- De beveiliging en privacy van gegevens is geborgd.
- Gegevensuitwisseling tussen applicaties geschiedt op een gestandaardiseerde manier.

De primaire processen onderwijs en onderzoek bepalen hoe wij onze informatiediensten inrichten

- Veranderingen in de primaire processen zijn leidend voor veranderingen in de informatiediensten.
- Alle veranderingen in de informatiediensten worden beoordeeld op de mate waarin ze bijdragen aan onderwijs en onderzoek.
- Plannen en voorgenomen initiatieven worden afgeleid van de doelstellingen van de instelling en beoordeeld en geprioriteerd via een portfolio managementproces.
- De inrichting van de informatiediensten houdt rekening met het gewenste onderscheidend vermogen op het gebied van onderwijs en onderzoek door hier specifieke functionaliteit voor te bieden.
- Studenten en medewerkers worden betrokken bij de inrichting van de informatiediensten, zodat deze optimaal aansluiten bij hun leefwereld en behoeften.
- Bij veranderingen in de informatiediensten ten behoeve van de primaire processen en van valorisatie is kwaliteit de focus.
- Bij veranderingen in de informatiediensten ten behoeve van ondersteunende processen is efficiency de focus.

[1] Een van de resultaten van het SURF project "Regie in de Cloud" is de Hoger Onderwijs Referentie Architectuur (HORA). De HORA is continu in ontwikkeling en wordt beheerd door de werkgroep Architectuur, vaak aangeduid als het "Hoger Onderwijs Architectenberaad (HO-AB)", bestaande uit enkele tientallen architecten van universiteiten en hogescholen door heel Nederland. De Radboud Universiteit participeert in dit beraad.

Onze informatiediensten overschrijden de organisatiegrenzen

- Externen hebben gecontroleerd toegang tot relevante delen van de informatiediensten.
- Er is een vertrouwde identity managementvoorziening.
- Er zijn eenduidige richtlijnen en afspraken voor het gegevensverkeer met externe informatieleveranciers/-gebruikers.

Onze informatie is gemakkelijk te raadplegen voor medewerkers en studenten

- Studenten en medewerkers kunnen (hun eigen) mobiele apparatuur meenemen naar de instelling en daarmee controleerbaar toegang krijgen tot de informatiediensten.
- De inrichting en beveiliging van het campusnetwerk maakt het mogelijk voor gebruikers om zowel intern als extern toegang te krijgen tot voor hen relevante informatiediensten.

Wij zorgen dat onze informatiediensten een duidelijke eigenaar hebben

- Binnen de informatiediensten wordt onderscheid gemaakt tussen de onderdelen: processen, gegevens, applicaties en infrastructuur.
- het eigenaarschap van processen, gegevens, appicaties en infrastructuur is eenduidig belegd.
- De verantwoordelijkheid voor het inrichten en testen van ketens van processen is eenduidig belegd.
- De eigenaar van een onderdeel van de informatiediensten is verantwoordelijk voor het – binnen gemaakte afspraken – functioneren van dat onderdeel.

Bij ons staat standaardisatie en hergebruik van onderdelen van informatiediensten voorop

- Er wordt gebruik gemaakt van gestandaardiseerde processen.
- Er wordt gebruik gemaakt van instellingsbrede applicaties.
- Er wordt gebruik gemaakt van bewezen technologie.
- Hergebruik gaat voor aanschaf, aanschaf gaat voor zelfbouw.
- Er wordt gebruik gemaakt van open standaarden.
- Open source oplossingen worden onder voorwaarden als mogelijkheid in selectietrajecten meegenomen.

Wij beschermen de gegevens van onze medewerkers en studenten

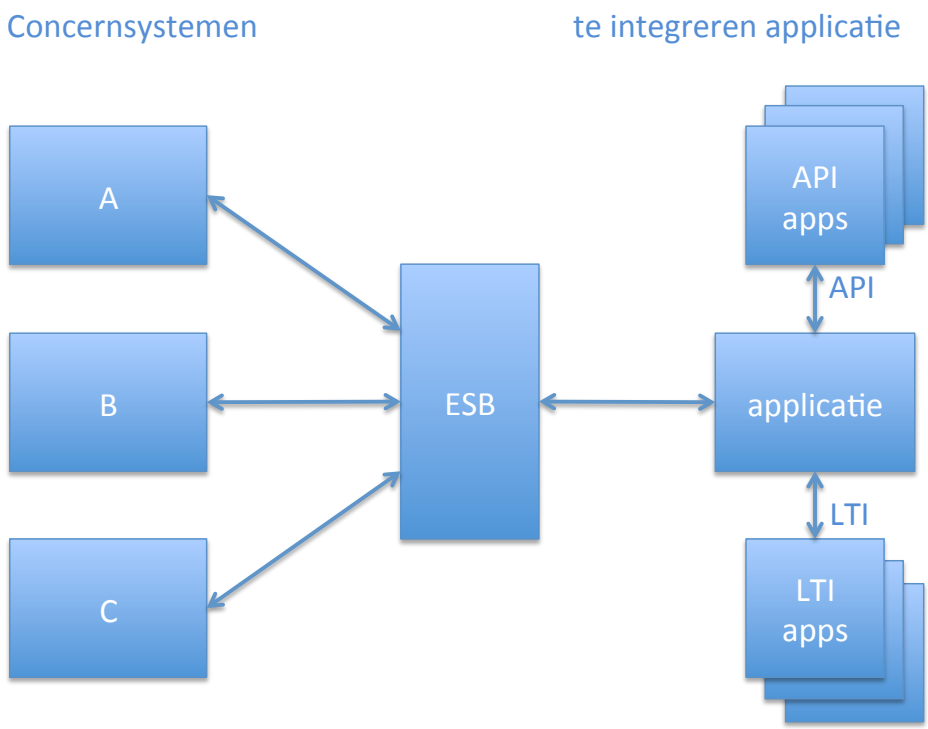
- Het RU informatiebeveiligingsbeleid wordt geïmplementeerd en gehandhaafd.
- Wettelijke verplichtingen met betrekking tot bescherming van privacy worden geïmplementeerd.
- Er zijn eenduidige bronsystemen voor gegevens.

Duurzaamheid speelt een belangrijke rol bij het inrichten en gebruiken van onze informatiediensten

- Er wordt gewerkt vanuit een Groen ICT-inkoopbeleid.
- ICT-componenten worden op een energiezuinige wijze gebruikt en beheerd en zoveel mogelijk hergebruikt of gerecycled.
- Informatiediensten worden RU-breed ingezet voor het verduurzamen van werkprocessen door het reduceren van onder meer reisbewegingen en ruimtegebruik.
- Het SURF Groene ICT Maturity Model wordt gebruikt voor periodieke toetsing.

Doelarchitectuur

De Radboud Universiteit heeft een applicatielandschap waaraan steeds nieuwe of gewijzigde applicaties dienen te worden aangesloten. Onderstaande figuur geeft de generieke architectuur van het applicatielandschap weer. In deze figuur worden drie soorten koppelingen tussen de nieuwe of gewijzigde applicatie en de rest van het landschap weergegeven. In het volgende hoofdstuk wordt ingezoomd op deze koppelingen, de dataoverdracht en voorwaarden.



Figuur 1: Algemene architectuur van het applicatielandschap

Het uitgangspunt is dat een te integreren applicatie een web-API heeft welke gebruikt kan worden om via de Enterprise Service Bus (ESB) van de Radboud Universiteit informatie te leveren aan of te ontvangen van de concernapplicaties. Hoe de ESB aan deze informatie komt dan wel verder verspreidt is de verantwoordelijkheid van de Radboud Universiteit. Daarnaast zijn directe koppelingen met flankerende applicaties (apps) op basis van LTI of API's (onder voorwaarden, zie verder) ook mogelijk. N.b. de te integreren applicatie kan een concernapplicatie worden en voor concernapplicaties geldt dezelfde doelarchitectuur.

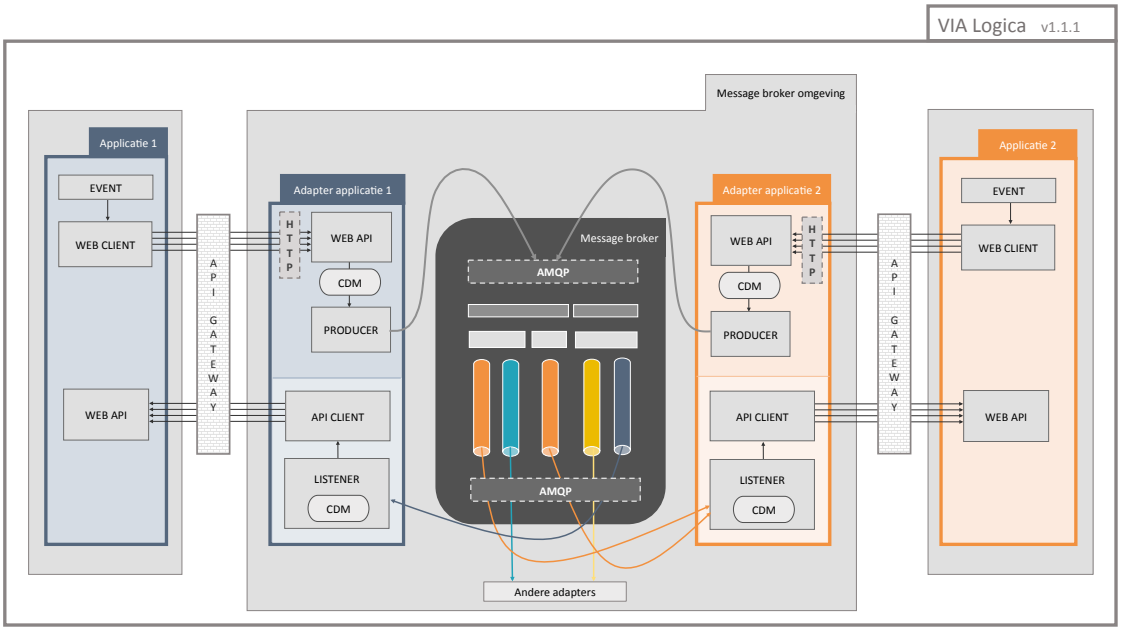
De relaties tussen de te integreren applicatie en de Radboud Universiteit concernsystemen vereisen *meestal* real-time interfaces waarin data worden uitgewisseld op het moment dat deze in het bronsysteem een bepaalde status bereiken. Zo wordt gewaarborgd dat administratieve en logistieke wijzigingen direct worden verwerkt in de relevante systemen waaronder de te integreren applicatie. De Radboud Universiteit gebruikt een ESB platform om het berichtenverkeer tussen concernsystemen te realiseren. Batch-processen dienen te worden voorkomen. Daarnaast maken we gebruik van andere integratiekanalen op basis van REST interfaces met JSON berichten.

3. Integratiearchitectuur

Enterprise Service Bus

De Radboud Universiteit maakt gebruik van een Enterprise Service Bus (ESB) voor het koppelen van applicaties c.q. het uitwisselen van berichten en gegevens. De EBS bestaat uit een *message broker* (routering en queueing) en een adapter voor elke applicatie die op de ESB is aangesloten (productie en consumptie van berichten en gegevens, zie verder). De message broker is gebaseerd op de open source software RabbitMQ.

De adapters zijn applicaties die door de Radboud Universiteit worden ontwikkeld en beheerd. Onderstaande figuur geeft de architectuur schematisch weer.



Figuur 2: Architectuur van de Radboud Universiteit ESB infrastructuur

De communicatie tussen de applicatie en zijn adapter vindt plaats over de web-API's van de betreffende component via de API-gateway.

Uitwisseling van gegevens

Op basis van *events* die in beginsel dienen te ontstaan in de applicatie, genereert de bijbehorende adapter *berichten* voorzien van nul of meer standaard *data-elementen* ter verwerking door andere systemen. Het is ook mogelijk dat de adapter zelf op grond van een bepaalde situatie of statusverandering in de applicatie of op basis van externe factoren overgaat tot het versturen van een bericht. De adapter levert het bericht af bij de broker en mag er daarna van uitgaan dat de broker het bericht correct verwerkt (fire and forget principe). Er kunnen meerdere afnemers zijn; berichten kunnen door de broker gedupliceerd en voor meerdere afnemers klaargezet worden in de queues van de ontvangende adapters.

De adapter van de applicatie die een event genereert vertaalt de gegevens uit de applicatie naar *standaard data-elementen* conform het Radboud Universiteit canonieke datamodel (CDM). Berichten en de bijbehorende voorgeschreven data-elementen zijn daarmee onafhankelijk van de ontvangende systemen (agnostisch model). De adapters van de doelsystemen zijn verantwoordelijk voor de juiste

interpretatie van het bericht en de vertaling van de meegestuurde data vanuit het CDM naar het datamodel van de ontvangende applicatie (symmetriebeginsel).

De Radboud Universiteit hanteert strikte regels omtrent de proliferatie van data vanuit bronsystemen naar afnemende systemen. Het principe van data-minimalisatie wordt gehanteerd en vindt plaats in de *ontvangende* adapter. Voor de proliferatie van persoonsgegevens is goedkeuring van de data-eigenaar evenals doelbinding nodig; de broker ziet toe dat alleen voor applicaties waarvoor beide zijn geregeld de betreffende data-elementen klaargezet kunnen worden.

Koppelingen op basis van de ESB

In beginsel worden koppelingen tussen applicaties gerealiseerd via de hierboven beschreven ESB infrastructuur. In de onderstaande tabel worden de vereisten met betrekking tot de integratie van applicaties gegeven alsmede de verantwoordelijkheden voor de leverancier resp. de Radboud Universiteit (de instelling) bij het realiseren van zulke koppelingen.

Implementatie vereisten leverancier	• Koppelingen van de te integreren applicatie aan concern-applicaties dienen gebruik te maken van de ESB en dus nadrukkelijk niet via een rechtstreekse - point-to-point - koppeling te worden gerealiseerd. • Het is niet toegestaan een nieuw koppelvlak (of aparte ESB) te introduceren tenzij dit koppelvlak volledig geïntegreerd is met de te integreren applicatie en op geen enkele wijze beheer- en/of licentieconsequenties heeft voor de Radboud Universiteit en het voorgaande uitgangspunt gehandhaafd blijft. • Er mogen enkel en alleen incrementele, (near) real-time koppelingen worden gerealiseerd (messaging). Hierbij moet gebruik worden gemaakt van webservices. Het uitwisselen van batch bestanden is niet toegestaan. • Indien de technische oplossing van de leverancier een koppeling vereist tussen meerdere technische instanties van de applicatie, dan valt het ontwikkelen van deze koppeling onder verantwoordelijkheid van de leverancier. • Wanneer de koppeling encryptie vereist, dan dient deze tenminste TLSv1.2 te gebruiken.
Verantwoordelijkheid instelling	• De instelling levert aan de leverancier een beschrijving van de relevante event-types en data-elementen op basis waarvan de uitwisseling van data geïmplementeerd gaat worden. • De instelling is verantwoordelijk voor de uitwisseling van gegevens tussen de ESB en de betreffende concern-applicatie (niet zijnde de te integreren applicatie). De Instelling is verantwoordelijk voor het verzenden van API messages dusdanig dat deze door de te koppelen applicatie verwerkt kunnen worden. De Instelling is verantwoordelijk voor de juiste verwerking van API responses van de webservice van de te integreren applicatie.
Verantwoordelijkheid leverancier	• Van de leverancier wordt verwacht dat hij gedurende de contractperiode, op projectbasis participeert in het (ontwikkel)team en zich conformeert aan de gekozen methodiek binnen de Instelling (bijvoorbeeld SCRUM) en meehelpt met het opstellen van de betreffende documentatie, indien zo'n participatie noodzakelijk is om het product op te leveren, te beheren of te onderhouden zoals is overeengekomen • Leverancier voorziet in webservices die de relevante gegevens uit de bronsystemen in de applicatie verwerkt c.q. opslaat, dan wel relevante gegevens uit de applicatie kan ophalen teneinde deze te verwerken in bronsystemen van de instelling. • De leverancier levert vóór gunning uitputtende documentatie van de voornoemde webservice(s) waaruit blijkt dat de door de instelling opgegeven event-types en data-elementen uitgewisseld kunnen worden. • De leverancier is verantwoordelijk voor het compleet en up-to-date houden van alle documentatie over webservices en API's die door de applicatie worden ondersteund.

	• De leverancier is verantwoordelijk voor het consistent en operationeel houden van het leverende en ontvangende koppelvlak in relatie tot de applicatie, ook na updates en upgrades daarvan.

Tabel 1: Verantwoordelijkheden en vereisten m.b.t. koppelingen via de ESB infrastructuur

Koppelingen op basis van LTI

In toenemende mate worden (onderwijs-)applicaties op basis van wereldwijde standaarden ontsloten. Dit heeft belangrijke voordelen zowel initieel (bij het realiseren van de koppeling) als ook in de exploitatie (het beheer van de koppeling). In de onderstaande tabel worden de vereisten met betrekking tot koppelingen via LTI gegeven alsmede de verantwoordelijkheden voor de leverancier resp. de instelling bij het realiseren van de koppelingen.

Implementatie vereisten leverancier	• De Radboud Universiteit heeft een sterke voorkeur de koppeling met onderwijs-apps waar mogelijk te realiseren op basis van LTI. • Wanneer de koppeling encryptie vereist, dan dient deze tenminste TLSv1.2 te gebruiken. • De leverancier dient de koppeling mogelijk te maken dan wel te realiseren op basis van LTI, minimaal versie 1.2 maar bij voorkeur versie 2.0 of hoger, tenzij: a. de onderwijs-app zelf nog geen LTI integratie aanbiedt of b. de te integreren applicatie een standaard integratie met de onderwijs-app heeft waarbij de door de Radboud Universiteit vereiste en gewenste functionaliteit geboden wordt. In beide gevallen kan in onderlinge afstemming de integratie gerealiseerd worden op basis van een API (zie verder).
Verantwoordelijkheid instelling	• De Instelling is verantwoordelijk voor het op tijd aanleveren van informatie zoals licentie-sleutels, toegang etc. die nodig zijn om de verbinding tot stand te brengen. De Instelling stelt applicatie-deskundigheid en test-capaciteit (personele resources) beschikbaar.
Verantwoordelijkheid leverancier	• Van de leverancier wordt verwacht dat hij verantwoordelijkheid neemt voor de realisatie op basis van het received IMS-LTI protocol. De te integreren applicatie heeft de rol van IMS consumer bij het koppelen van een onderwijs-applicatie. De onderwijs-app heeft de rol van IMS producer.

Tabel 2: Verantwoordelijkheden en vereisten m.b.t. koppelingen via LTI

Koppelingen op basis van een API

Zoals hierboven aangegeven kunnen er situaties zijn dat er geen koppeling wordt gerealiseerd op basis van LTI maar van een API. De situaties waarin dit is toegestaan zijn in Tabel 2 beschreven. In zulke gevallen wordt de integratie gerealiseerd op basis van een API koppeling. In de onderstaande tabel worden de vereisten m.b.t. API-koppelingen met de te integreren applicatie gegeven, alsmede de verantwoordelijkheden voor de leverancier resp. de instelling bij het realiseren van de koppelingen.

Implementatie vereisten leverancier	• Een koppeling gebaseerd op IMS-LTI standaard heeft de voorkeur. • De voorwaarden waaronder een API-koppeling is toegestaan worden gegeven in Tabel 2. • Wanneer de koppeling encryptie vereist, dan dient deze tenminste TLSv1.2 te gebruiken.
Verantwoordelijkheid instelling	• De Instelling is verantwoordelijk voor het op tijd aanleveren van informatie zoals licentie-sleutels, toegang etc. die nodig zijn om de verbinding tot stand te brengen. • De Instelling stelt applicatie-deskundigheid en test-capaciteit (personele resources) beschikbaar.
Verantwoordelijkheid leverancier	• Van de leverancier wordt verwacht dat hij, gedurende de contractperiode: a. op projectbasis participeert in het team dat zich richt op de API integraties, b. zich conformeert aan de gekozen methodiek binnen de instelling (bijvoorbeeld SCRUM) en c. verantwoordelijkheid neemt voor het (correct) aansluiten van de (onderwijs-)app op de te integreren applicatie.

Tabel 3: Verantwoordelijkheden en vereisten m.b.t. koppelingen via een API

4. Applicatiearchitectuur

In dit hoofdstuk worden de eisen die de Radboud Universiteit stelt aan de architectuur van de te integreren applicatie gegeven.

Privacy

De Radboud Universiteit hecht grote waarde aan de privacy van alle personen van wie wij persoonsgegevens verwerken. Wij hanteren het “privacy by design” beginsel en verwachten *aantoonbaar* dezelfde houding en werkwijze van leveranciers van applicaties welke door de RU voor de verwerking van persoonsgegevens worden ingezet.

De Radboud Universiteit hanteert strikte regels omtrent de proliferatie van data vanuit bronsystemen naar afnemende systemen. Het principe van data-minimalisatie wordt gehanteerd en wordt afgedwongen in de integratie-infrastructuur. Voor de proliferatie van persoonsgegevens is altijd doelbinding en goedkeuring van de data-eigenaar nodig. Dit betekent dat applicaties waarvoor overheveling van persoonsgegevens niet strikt noodzakelijk is, moeten kunnen omgaan met gepseudonimiseerde of geanonimiseerde data. Indien binnen de applicatie met persoonsgegevens moet worden gewerkt zijn additionele eisen van toepassing m.b.t. (controle op) toegang tot de applicatie en de in de applicatie beschikbare data. Zulke bepalingen dienen in de overeenkomst met de leverancier te worden opgenomen.

Security

De Radboud Universiteit hanteert het principe dat de leverancier van een applicatie de garantie geeft alles in het werk te stellen om ongeoorloofde toegang tot het systeem te voorkomen en te voorkomen dat het systeem of de data van de RU worden gecompromitteerd. Bij een security-breach van enige component van een oplossing die een leverancier bij de Radboud Universiteit inzet, verwachten wij proactief actie van de leverancier. Bepalingen van deze aard en de nadere invulling dienen in de overeenkomst met de leverancier te worden opgenomen.

Autorisatie en authenticatie

De Radboud Universiteit hanteert het principe dat toegang tot applicaties uitsluitend is toegestaan met bestaande accounts; eigen accounts en accounts die door de universiteit als vertrouwd zijn aangemerkt. Opslag van wachtwoorden in applicaties is in geen geval toegestaan. Authenticatie tegen één van onze authenticatie-proxy’s (AD, LDAP, Radius) is toegestaan, maar uitsluitend indien het zeker is dat de applicatie nooit door gebruikers zonder Radboud Universiteit account gebruikt hoeft te worden. Anders dient gebruik te worden gemaakt van federatieve authenticatie, b.v. via SURFconext. Ondersteuning hiervan door de te integreren applicatie is een vereiste.

Provisioning van accounts in het systeem gebeurt uitsluitend vanuit het Radboud Universiteit Identity en Access Management Systeem (IdM/IAM), via de voorgeschreven integratiearchitectuur. Gebruikersbeheer binnen de applicatie is in beginsel alleen toegestaan voor noodsituaties. Toegang tot de applicatie dient eveneens te worden geprovisioned vanuit IdM/IAM.

Cloud of on premise

Beide zijn onder voorwaarden mogelijk.

Bewerkersovereenkomst

Er is altijd een bewerkersovereenkomst conform RU-model noodzakelijk als de te integreren applicatie persoonsgegevens verwerkt.

Modulariteit

De Radboud Universiteit verwacht dat ICT-oplossingen van leveranciers alle kernfunctionaliteiten bieden conform het overeengekomen programma van wensen en eisen. Functionaliteiten die in de specificaties als optioneel zijn aangemerkt *mogen* door een ICT-oplossing worden geleverd, maar moeten uitgeschakeld kunnen worden binnen de ICT-oplossing wanneer de Radboud Universiteit ervoor kiest om zulke functionaliteit d.m.v. een andere oplossing te realiseren. In dat geval moet een integratie van beide oplossingen mogelijk zijn *en* mag de in de te integreren applicatie aanwezige optionele functionaliteit (die niet wordt gebruikt) de door een andere oplossing geleverde overeenkomstige functionaliteit niet belemmeren of beperken.

Rapportages

Het beleid van de Radboud Universiteit staat verwerking van belangrijke stuurgegevens buiten de bronsystemen toe, maar besluiten en rapportages dienen plaats te vinden op basis van gegevens in het bronsysteem dan wel op basis van afgeleide data in het data warehouse (DWH). De reden is dat we willen kunnen garanderen dat besluiten en rapportages uitsluitend gebaseerd worden op uniek vastgestelde gegevens. Hieruit volgt dat het van belang is hoe resultaten die in de te integreren applicatie ontstaan, geconsolideerd worden voor latere consultatie. Bij voorkeur wordt dit gerealiseerd door resultaten terug te halen naar de bronsystemen en/of naar het DWH. Als om wat voor reden dan ook hiervan wordt afgeweken, dan dient de applicatie toegang tot de resultaten te garanderen voor tenminste de wettelijk vastgestelde of de door de Radboud Universiteit vastgestelde termijn.

Indien gegevens ten behoeve van rapportages worden overgeheveld naar een bronsysteem of het DWH, dan hoeft dat in de regel niet real time, maar mag het één keer per etmaal in een batch gebeuren.

Documenthistorie

versie	datum	auteur	wijzigingen t.o.v. vorige versie
0.1	25-06-2018	Architecten	Startdocument
0.2	06-07-2018	Architecten	Verduidelijking doelarchitectuur