

Beleidsnotitie Integratiestrategie

Gedraglijn bij het integreren van applicatiecomponenten

1.3

Colofon

EIGENAAR	AUTEUR(S)
Afdelingsmanager Informatie	R. Dijkstra
TITEL	VERTROUWELIJKHEID
Beleidsnotitie Integratiestrategie	Bedrijfsvertrouwelijk
STATUS	TE REVISEREN VOOR
Definitief	
TER VASTSTELLING AANGEBODEN OP	HANDTEKENING
Datum : 5 juli 2021	
Naam : W.J. Sikkes	
Functie : Afdelingsmanager Informatie	

Distributielijst

NAAM	AFDELING	FUNCTIE EN ROL	AKKOORD BETROKKEN GEÏNFORMEERD		
			A	B	G
Wietske Sikkes	INF	Afdelingsmanager Informatie	X		
Pieter Vermeij	INF	Informatiemanager		X	
Ruud Zwaan	INF	Informatiemanager		X	
Robert Woltersom	INF	Informatiemanager		X	
Luc Aarts	INF	Informatiemanager		X	
Chantal Meijerink	Concern	CISO		X	
Peter Visser	INF	ISO		X	
Ronald Schotanus	Concern	CPO		X	
Rindert Dijkstra	INF	Informatieadviseur		X	

Versiegeschiedenis

VERSIE	REDEN WIJZIGING	DATUM	STATUS	SCHRIJVER
0.1	Initiële versie	20-11-2019	Concept	R. Dijkstra
0.2	Afstemming met Pieter Vermeij	27-11-2019	Concept	R. Dijkstra
1.0	Verwerking opmerkingen voorlaatste versie	05-12-2019	Concept	R. Dijkstra
1.1	N.a.v. bespreking door MT-INF	09-12-2019	Definitief	R. Dijkstra
1.2	N.a.v. bespreking door MT-INF, opmerkingen Pieter Vermeij	18-12-2019	Definitief	R. Dijkstra
1.3	Aanpassing procedure en regels extern-extern, bespreking in IMO, bespreking met ISO, definitie koppelingen toegevoegd, verfijning extern-extern, beleid verbreden met bestandsoverdracht.	05-07-2021	Definitief	R. Dijkstra

Inhoudsopgave

1	Inleiding.....	4
2	Doelstelling	4
3	Verwijzingen.....	4
4	Van de eenheid Informatie voor de organisatie.....	4
4.1	Verantwoordelijkheid.	4
4.2	Koppelingen	4
4.3	Patronen	5
4.3.1	Organiseren	5
4.3.2	Intern-intern.....	5
4.3.3	Intern-extern.....	5
4.3.4	Extern-extern	6

1 Inleiding

Tot voor kort stonden alle applicaties 'veilig' bij ons in het rekencentrum (on premises). Steeds meer applicaties worden nu aangeboden waarbij de applicatie draait bij de leverancier (in de cloud). Daar bovenop komt dat de voor het uitvoeren van een bedrijfsfunctie benodigde applicatiefunctionaliteit meer en meer een resultaat is van samenwerkende componenten in plaats van één component die de volledige functionaliteit levert. Ook de Common Ground filosofie past in deze ontwikkeling.

Concrete voorbeelden zijn ons nieuwe zaakstelsel Djuma, iBurgerzaken, het portaal schuldhulpverlening en CityPermit. Deze applicatiecomponenten staan extern bij de leverancier (in de cloud) en werken samen met applicatiecomponenten die in ons eigen rekencentrum staan (on premises), zoals Kofax, Key2Datadistributie, Active Directory, Smartdocuments en de Berichtenboxadapter.

Aan ons de opgave om te zorgen voor een beheersbaar, beschikbaar en veilig geheel.

2 Doelstelling

Met het in dit document geformuleerde beleid willen we een duidelijke gedragslijn beschrijven hoe we de integratie van de samenwerkende applicatiecomponenten willen realiseren, zodat we een beheersbare en gecontroleerde situatie bewerkstelligen en overzicht houden over de verschillende verbindingen die er tussen ons netwerk en andere netwerken bestaan. Dit alles is essentieel om de bedrijfszekerheid en veiligheid van het steeds groter wordende aantal koppelingen duurzaam te kunnen borgen. Waar hieronder over applicatiecomponenten gesproken wordt, bedoelen we zowel de software als de gegevensverzamelingen.

3 Verwijzingen

Dit document is opgesteld na een tweetal werksessies met direct betrokkenen van de afdeling Informatie en met onze integratiepartner Enable-U. Er is gebruik gemaakt van een door Enable-U opgesteld adviesrapport [1] op basis van deze twee sessies.

[1] Integratie Strategie gemeente Apeldoorn, Ruud Koreman, Enable-U, 19-11-2019

4 Van de eenheid Informatie voor de organisatie

4.1 Verantwoordelijkheid.

De afdeling Informatie heeft de opdracht om de applicatiediensten die de gemeentelijke organisatie nodig heeft te leveren. Vanzelfsprekend moet rekening worden gehouden met kaders voor bijvoorbeeld privacy en security. Maar voor de gebruiker is het de applicatiefunctionaliteit die telt. Wat er 'achter de schermen' gebeurt en waar dat gebeurt is niet zichtbaar. Met andere woorden: hoe die applicatiefunctionaliteit tot stand komt is zaak van de afdeling Informatie. De verantwoordelijkheid en bevoegdheid hiervoor ligt hiermee bij de manager van de afdeling Informatie.

4.2 Koppelingen

We spreken van een koppeling die in aanmerking komt voor de integratievoorziening als er een digitale vorm van berichtenverkeer of gegevensoverdracht is tussen applicaties onderling, tussen een applicatie en een gestructureerde gegevensverzameling of tussen gestructureerde gegevensverzamelingen onderling.

Met een koppeling kan een applicatie bijvoorbeeld gebruik maken van extra functionaliteit of gegevens. De koppeling van Djuma met Ingenico en de koppeling van Djuma met Key2DataDistributie zijn hiervan voorbeelden. Koppelingen die in de toekomst door Common Ground nodig zijn tussen software en data zijn een ander voorbeeld.

Vormen van bestandsoverdracht zoals een export/import vallen ook onder deze definitie, maar omwille van de haalbaarheid vooralsnog alleen de geautomatiseerde bestandsoverdracht extern-intern en v.v. Een ETL-toepassing die iedere nacht data selecteert, overzet, eventueel transformeert en vervolgens wegschrijft is hier een voorbeeld van, net zo als een 'job' waarbij een dataset van een cloud-applicatie wordt opgehaald en weggeschreven. Een ander voorbeeld is het push-bericht waarmee wij sensordata ontvangen.

Zoals in de inleiding al is aangestipt verandert de manier waarop de applicatiefunctionaliteit tot stand komt. Het aantal applicatiecomponenten en koppelingen tussen applicatiecomponenten neemt sterk toe en applicatiecomponenten bevinden zich op verschillende locaties. Dit vraagt om maatregelen en voorzieningen zodat de diverse componenten gezamenlijk de benodigde functionaliteit leveren. Deze veranderingen brengen ook risico's met zich mee ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid. Alle componenten moeten beschikbaar zijn, voldoende performance bieden en onderling veilig kunnen communiceren. Beveiliging, privacy, beheer en besturing zijn hierbij daarom van wezenlijk belang en vereisen meer aandacht dan in de oude situatie.

4.3 Patronen

We onderscheiden drie integratiepatronen voor de samenwerkende applicatiecomponenten: intern-intern, intern-extern, extern-extern. Voor een uitgebreide toelichting wordt verwezen naar [1].

1. Intern-intern: applicatiecomponenten werken samen binnen het rekencentrum van de gemeente.
2. Intern-extern: applicatiecomponenten binnen het rekencentrum van de gemeente werken samen met applicatiecomponenten buiten de gemeente
3. Extern-extern: applicatiecomponenten werken samen buiten het rekencentrum van de gemeente

De drie voorzieningen voor de samenwerkende applicatiecomponenten die in dit document een centrale rol spelen zijn de zogenaamde API-gateway, in de huidige situatie het product Enable-U 2 Secure, de Enterprise Service Bus, in de huidige situatie het product Enable-U 2 Orchestrate en de voorziening voor Managed File Transfer (MFT), in de huidige situatie het product VLTrader. Deze producten kunnen ook in combinatie worden ingezet.

De API-gateway wordt ingezet voor de beveiliging van de verbinding tussen externe en interne applicatiecomponenten, denk aan toegangscontrole en security controles, contract management / SLA en protocol conversie. De Enterprise Service Bus (ESB) wordt ingezet voor orkestratie, transformatie en routing. De MFT-voorziening wordt ingezet voor het overzetten van bestanden van intern naar extern of andersom middels verschillende TCP/IP protocollen.

4.3.1 Organiseren

Het hier geformuleerde beleid geldt voor iedere koppeling. Wanneer er gefundeerde redenen zijn om af te wijken van het beleid, dan stelt degene die wil afwijken (bijvoorbeeld een projectmanager) een onderbouwd afwijkingsvoorstel op en legt dit voor aan het IMO (het InformatieManagersOverleg). Het IMO beoordeelt het afwijkingsvoorstel. Bij akkoord van het IMO wordt het voorstel ter vaststelling voorgelegd aan de manager van de afdeling Informatie.

Het IMO laat zich bij de beoordeling bijstaan door de (C)ISO, CPO, de informatieadviseur met aandachtsgebied architectuur, projectmanager, functioneel specialist en applicatiespecialist / technisch integratiespecialist, zodat alle relevante perspectieven meegewogen worden. Het IMO bewerkstelligt een consistente gedragslijn voor koppelingen.

4.3.2 Intern-intern

Hiervoor geldt het principe: applicatiecomponenten koppelen via de Enterprise Service Bus indien er sprake zal zijn van interne orkestratie, transformatie en routing.

Door te koppelen via de ESB worden afhankelijkheden zichtbaar en beter beheersbaar, bijvoorbeeld als een applicatie wordt vervangen of gewijzigd.

Bij de koppelingen van Key2DataDistributie met leverende en afnemende applicaties zorgt Key2DataDistributie zelf voor transformatie (naar StUF-BG) en distributie naar afnemers. Het is dan niet zinvol om de ESB daar tussen te zetten.

4.3.3 Intern-extern

Hiervoor geldt het principe: externe met interne (en vv) applicatiecomponenten koppelen altijd via de API-gateway en/of de MFT voorziening en indien er sprake zal zijn van interne orkestratie, transformatie en routing bovendien via de Enterprise Service Bus.

Bij de koppelingen van Key2DataDistributie met de leverende (interne en) externe basisregistraties, bijvoorbeeld het HandelsRegister, zorgt Key2DataDistributie zelf voor transformatie naar StUF-BG en distributie naar interne en externe afnemers. Het is dan niet zinvol om de ESB tussen Key2DataDistributie en de leverende basisregistraties te zetten, maar wel de API-gateway.

4.3.4 Extern-extern

Hiervoor geldt het principe: applicatiecomponenten koppelen via de API-gateway als er sprake is van uitwisseling van privacygevoelige of vertrouwelijke informatie tussen die applicatiecomponenten. In afwijking hiervan kan een directe koppeling, d.w.z. niet via de API-gateway, gerealiseerd worden mits voor beide componenten is voorzien in passende beveiligingsmaatregelen. Voor privacygevoelige gegevens moeten deze aansluiten bij wat de AVG zegt over passende organisatorische en technische maatregelen. De (C)ISO kan dit namens de proceseigenaar beoordelen.

Voor extern-extern-koppelingen die direct worden gelegd, d.w.z. niet via onze API-gateway, zijn contractuele afspraken met de leveranciers nodig. Een dergelijke koppeling moet opgenomen zijn in de verwerkersovereenkomst. Op basis hiervan kan monitoring plaatsvinden.