Middleware

BIO Thema-uitwerking

Mei 2026 [versie 3.0 definitief]

Het CIP betracht zorgvuldigheid bij het samenstellen van zijn publicaties. Het kan voorkomen dat er toch sprake is van omissies, onjuistheden en/of gedateerdheid. Het is altijd de verantwoordelijkheid van de lezer zelf dit te beoordelen en desgewenst te corrigeren indien hij zich baseert op of gebruik maakt van een CIP-publicatie. Het CIP ontvangt graag correctieverzoeken en suggesties.

©Centrum Informatiebeveiliging en Privacybescherming. Het CIP heeft voor deze publicatie licentie Creative Commons Naamsvermelding-NietCommercieel-GelijkDelen (CC BY-NC-SA 4.0) verleend. Voor meer informatie zie: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.nl.

BIO Thema-uitwerking Middleware

Titel	BIO Thema-uitwerking Middleware
Datum	Mei 2026
Versie en status	2.0 definitief
Opdrachtgever	Centrum Informatiebeveiliging en Privacybescherming (CIP)
Regime	Becommentarieerde praktijk
Auteurs	CIP-kernteamleden
Reviewers	Versie 1.0: Professionals uit het CIP-netwerk en het CIP-kernteam Versie 1.1: CIP-kernteam Versie 1.2: CIP-kernteam Versie 1.3: CIP-kernteam Versie 2.0: CIP-kernteam

Considerans

CIP-producten steunen op kennis van professionals uit verschillende organisaties actief in het CIP-netwerk, zowel uit de overheid als de markt. Opmerkingen en aanvullingen kun je melden op cip-overheid.nl/contact.

Wijzigingsbeheer

In de onderstaande tabel worden alle relevante wijzigingen in dit document bijgehouden, om eenvoudig inzicht te krijgen in de uitgevoerde aanpassingen.

Versie	Datum	Wijziging	Door
1.0	Mei 2026		CIP-kernteam
1.1	Maart 2023		CIP-kernteam
1.2	November 2023	Tekstverbetering, BUC-afbeeldingen in tabelvorm, harde enters vervangen, doelstellingen en risico's geüniformeerd, handreiking BIO2.0-opmaat verwerkt)	CIP-kernteam
2.0	Mei 2026	BIO2 1.3 verwerkt	CIP-kernteam

Leeswijzer

Voorafgaand aan hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en 5 Control-domein, de kern van dit document, heeft elke BIO Thema-uitwerking een inleiding.

Aanvullend geldt:

- Voor de aanduiding van personen wordt de mannelijke vorm aangehouden (hij/hem/zijn) ongeacht het geslacht.
- De controls en maatregelen vermeld in deze thema-uitwerking zijn in het beleids-, uitvoerings- en control-domein georganiseerd, waarmee ze bij de overeenkomstige functionarissen kunnen worden geadresseerd. Deze functionarissen zijn niet benoemd omdat dit organisatie-afhankelijk is.
- Bijlagen zijn opgenomen alleen voor specifieke informatie uit hoofdstuk 3 Beleidsdomein, 4 Uitvoeringsdomein en/of 5 Control-domein.
- Van best practices (open standaarden al dan niet toegankelijk met een licentie) zijn de meest actuele versies afgekort vermeld, tenzij de actuele versie niet toereikend is.

Voor een overzicht van alle gebruikte best practices, afkortingen en begrippen en een generieke toelichting op de opzet van de thema-uitwerkingen, zie de Structuurwijzer BIO Thema-uitwerkingen.

Inhoudsopgave

Leeswijzer 3

1 Inleiding 8

1.1 Toelichting op middleware 8

1.1.1 Functionaliteiten 8

1.1.2 Componenten 9

1.1.3 Integratieservices 9

1.2 Doel middleware 9

1.3 Doelgroepen 9

1.4 Scope en begrenzing middleware 9

2 Beveiligingsobjecten Middleware 11

2.1 Organisatie van applicatieontwikkelingsobjecten 11

2.2 Algemene en specifieke objecten 11

3 Beleidsdomein 13

3.1 Doelstelling 13

3.2 Risico’s 13

3.3 Objecten, controls en maatregelen 13

3.3.1 B.01 Beleid middlewarecomponenten 13

Objectdefinitie 13

Objecttoelichting 13

3.3.2 B.02 Beleid informatietransport 15

Objectdefinitie 15

Objecttoelichting 15

3.3.3 B.03 Data en privacy 16

Objectdefinitie 16

Objecttoelichting 16

3.3.4 B.04 Middlewarearchitectuur en certificering 17

Objectdefinitie 17

Objecttoelichting 17

4 Uitvoeringsdomein 19

4.1 Doelstelling 19

4.2 Risico's 19
4.3 Objecten, controls en maatregelen 19
4.3.1 U.01 Richtlijnen en procedures middlewarefunctionaliteit 20
Objectdefinitie 20
Objecttoelichting 20
4.3.2 U.02 Rollen en verantwoordelijkheden middlewarefunctionaliteit 21
Objectdefinitie 21
Objecttoelichting 21
4.3.3 U.03 Toegang tot middlewarefunctionaliteit 22
Objectdefinitie 22
Objecttoelichting 22
4.3.4 U.04 Hardening middlewarecomponenten 23
Objectdefinitie 23
Objecttoelichting 23
4.3.5 U.05 Configuratie middlewarecomponenten 24
Objectdefinitie 24
Objecttoelichting 24
4.3.6 U.06 Logging en monitoring middleware 25
Objectdefinitie 25
Objecttoelichting 25
4.3.7 U.07 Ontwerpdocumentatie 26
Objectdefinitie 26
Objecttoelichting 26
4.3.8 U.08 Vertrouwelijkheid en integriteit data 26
Objectdefinitie 26
Objecttoelichting 26
4.3.9 U.09 Betrouwbare dataopslag 27
Objectdefinitie 27
Objecttoelichting 27
4.3.10 U.10 Dataherstel 28
Objectdefinitie 28
Objecttoelichting 28

4.3.11 U.11 Schonen data en media 29
Objectdefinitie 29
Objecttoelichting 29
4.3.12 U.12 Beveiliging berichtenverkeer 30
Objectdefinitie 30
Objecttoelichting 30
4.3.13 U.13 Capaciteitsbeheer 31
Objectdefinitie 31
Objecttoelichting 31
5 Control-domein 33
5.1 Doelstelling 33
5.2 Risico's 33
5.3 Objecten, controls en maatregelen 33
5.3.1 C.01 Evaluatierichtlijnen 33
Objectdefinitie 33
Objecttoelichting 33
5.3.2 C.02 Evaluatie naleving beleid 34
Objectdefinitie 34
Objecttoelichting 34
5.3.3 C.03 Beoordeling middlewarefunctionaliteit 35
Objectdefinitie 35
Objecttoelichting 35
5.3.4 C.04 Rapporteren middlewarefunctionaliteiten 36
Objectdefinitie 36
Objecttoelichting 36
5.3.5 C.05 Monitoren gebruikers- en beheerdersactiviteiten 37
Objectdefinitie 37
Objecttoelichting 37
Bijlage 1: Use case Interne applicatie-integratie 39
Integratieservices 39
Oplossing 39
Bijlage 2: Use case Applicaties met integratiefuncties 40

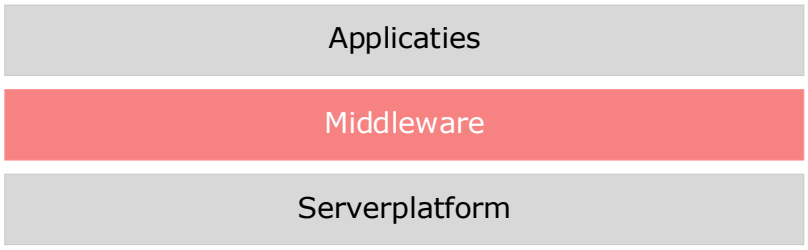
Beveiligingsobjecten 40
Bijlage 3: Use case Gedelegeerde integratiefuncties 41
Beveiligingsobjecten 41
Bijlage 4: Use case End-to-end applicatie-integratie 42
Beveiligingsobjecten 42
Bijlage 5: Use case Enterprise Service Bus (ESB) 43
Beveiligingsobjecten 43
Bijlage 6: Use case End-to-End integratie met API gateway 44
Problematiek 44
Oplossing 44
Bijlage 7: Gespecialiseerde API gateway-toepassing 46
Beveiligingsobjecten 46
Bijlage 8: Context en systeemfuncties middleware 47
Context middleware 47
Systeemfuncties van middleware 47

1 Inleiding

Deze BIO Thema-uitwerking is door het Centrum Informatiebeveiliging en Privacybescherming (CIP) opgesteld. Het omvat een gestructureerd referentiekader voor het thema middleware.

1.1 Toelichting op middleware

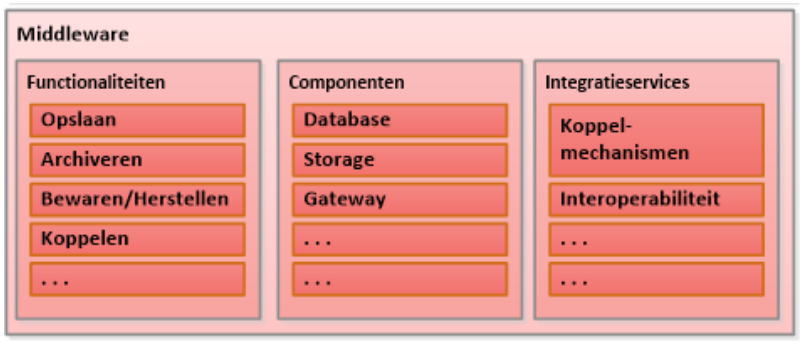
Middleware is een technologie-laag (software en hardware) binnen de technische architectuurstack. Middleware bevindt zich tussen de applicaties (toepassingssoftware) en het serverplatform waarop besturingssoftware draait, zie afbeelding 1.



Afbeelding 1: Positie van middleware in de technische architectuurstack

Het begrip middleware heeft in de loop van de tijd een brede invulling gekregen. Middleware bestaat uit software- en hardwarecomponenten voor databases, storage, gateways en dergelijke, met functies voor onder andere opslag, archiveren, bewaren en herstellen van data en koppelen met andere platformen en applicaties. De middleware-laag voert daarmee allerlei technische verwerkingstaken uit en verzorgt integratieservices voor de koppelingen met andere IT-platformen. Zie bijlage 1 tot en met bijlage 7 voor verschillende toepassingsvoorbeelden.

Middleware wordt in deze thema-uitwerking benaderd vanuit functionaliteiten, componenten en integratieservices, zie afbeelding 2.



Afbeelding 2: Benadering van middleware

1.1.1 *Functionaliteiten*

Middleware maakt het mogelijk applicaties te ontwikkelen zonder dat basis functies voor opslag, herstel, etc. moeten worden meegenomen. De middleware verzorgt deze functies en kan die ook ter beschikking aan meerdere applicaties op meerdere platformen.

1.1.2 *Componenten*

Componenten zijn technische objecten zoals databases, hardware en software voor dataopslag en hard- en software voor data-uitwisseling, die als services door applicaties gebruikt worden. De eindgebruikers krijgen uitsluitend toegang tot de data via applicaties; beheerders kunnen via speciale toegangsrechten rechtstreeks toegang krijgen tot systeemdata en componenten, zoals back-up-voorzieningen of integratieservices.

1.1.3 *Integratieservices*

Middleware kan in complexe, gedistribueerde omgevingen de technische integratie verzorgen bij de koppeling tussen meerdere platformen en bij de communicatie tussen de platformen. De instellingen die daarvoor nodig zijn, vereisen speciale kennis en toegangsrechten.

1.2 Doel middleware

Middleware is een categorie technologieën, ontworpen om de compliciteit en heterogeniteit, inherent aan gedistribueerde systemen te beheersen.

Het doel van de BIO Thema-uitwerking Middleware is een beeld te geven van relevante onderwerpen (hierna 'objecten' genoemd) waarover afspraken gemaakt moeten worden, als middlewarefunctionaliteit wordt ingezet.

1.3 Doelgroepen

Dit document is bestemd voor de volgende doelgroepen:

- Functionarissen die verantwoordelijk zijn voor het stellen van beveiligingskaders en voor de controle op naleving hiervan, zoals Beveiligingscoördinatoren, Chief Information Security Officers (CISO's) en Security managers.
- Functionarissen die betrokken zijn bij het ontwerp, de implementatie en het beheer van middleware.
- Controlerende instanties (IT-auditors) die met dit referentiekader een objectieve ICT-beveiligingscontrole uitvoeren.

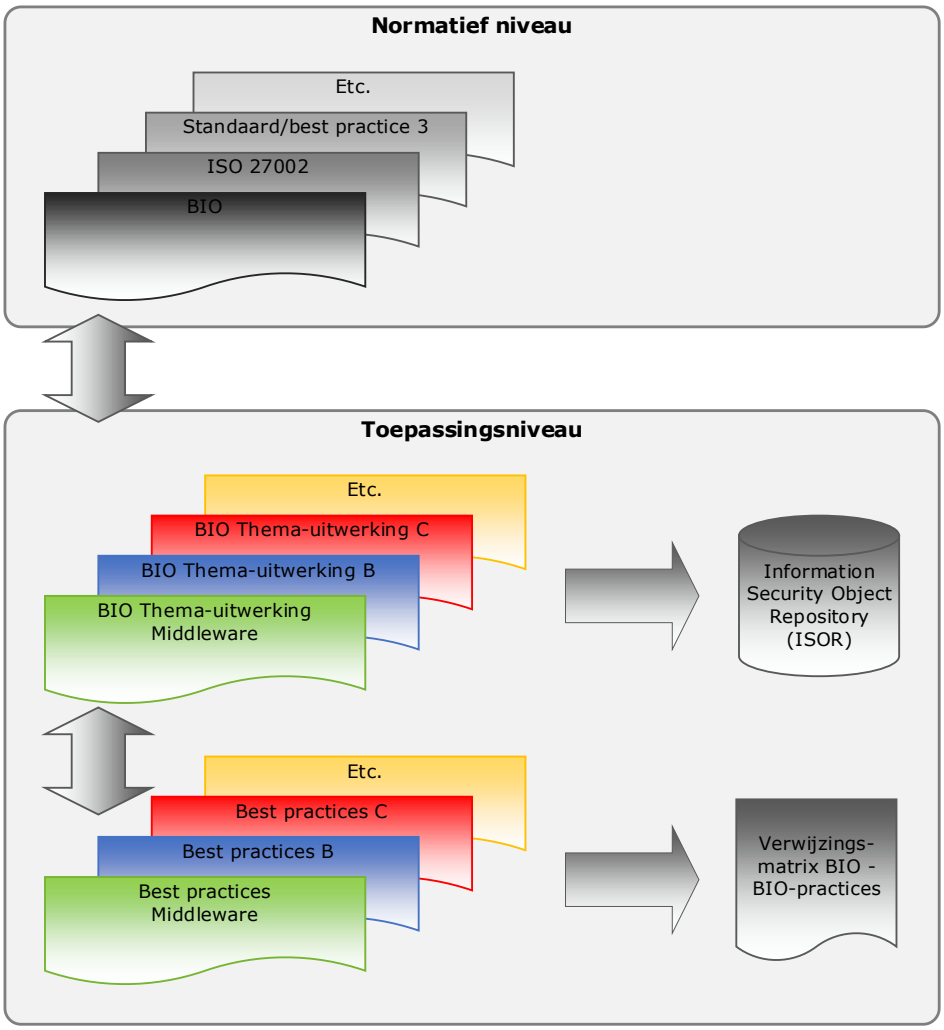
1.4 Scope en begrenzing middleware

De scope van BIO Thema-uitwerking Middleware omvat objecten die relevant zijn voor de beveiliging van middlewarefuncties en de opslag van gestructureerde data. De beveiliging van ongestructureerde data valt buiten de scope van deze thema-uitwerking.

De objecten vormen de inhoudelijke onderwerpen van het thema.

Zoals in elke BIO Thema-uitwerking het geval is, is ook in dit document een set beveiligingsobjecten, controls en maatregelen uit de BIO bijeengebracht. Waar uit de SIVA-analyse (Structuur, Inhoud, Vorm en Analysevolgorde) bleek dat objecten ontbraken, werden die aangevuld met gebruikmaking van andere beste practices.

De positionering van dit document ten opzichte van andere documenten is weergegeven in afbeelding 3.



Afbeelding 3: Relatie BIO Thema-uitwerking met aanpalende documenten

Voor nadere duiding van de context en de systeemfuncties van Middleware, zie bijlage 8.

2 Beveiligingsobjecten Middleware

Aan de hand van drie onderzoeksvragen die vanuit de optiek van de BIVC-criteria (Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid) gesteld zijn, zijn de objecten afgeleid en ingedeeld in het beleids-, uitvoerings- en control-domein.

De vragen die hierbij een rol spelen, zijn:

Welke elementen spelen vanuit de optiek van BIVC een rol bij de conditionering en sturing op middleware en wat is de consequentie bij afwezigheid hiervan?

- Welke elementen spelen vanuit de optiek van BIVC een rol bij de exploitatie van middleware en wat is de consequentie bij afwezigheid hiervan?
- Welke elementen spelen vanuit de optiek van BIVC een rol bij de beheersing van middleware en wat is de consequentie bij afwezigheid hiervan?

2.1 Organisatie van applicatieontwikkelingsobjecten

De geïdentificeerde objecten die bij middleware een rol spelen, zijn ingedeeld in het beleids-, uitvoerings- en control-domein. Hiermee worden deze aspecten in de juiste context gepositioneerd. De betekenis die aan elk domein wordt toegekend, is:

Beleid

Binnen dit domein bevinden zich conditionele elementen voor middleware. Hier zijn eisen opgenomen over 'geboden' en 'verboden', zoals het beleid, de te hanteren wet- en regelgeving en andere vormen van reguleringen en beperkingen.

- Uitvoering
  Binnen dit domein bevinden zich:

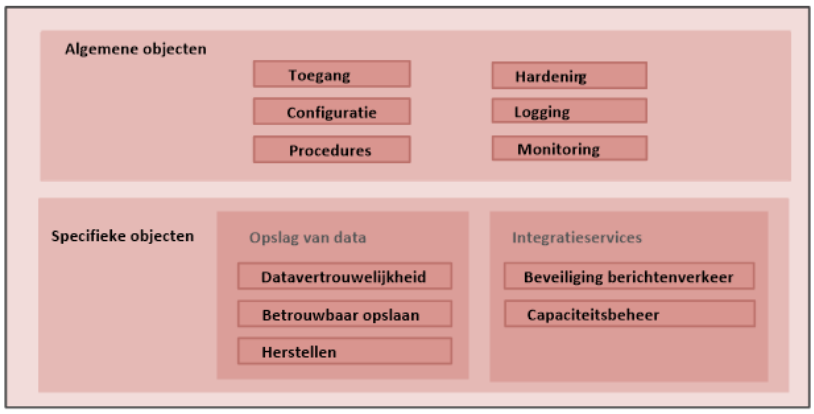
  - elementen die gerelateerd zijn aan de operationele activiteiten rond de exploitatie van middleware;
  - elementen die aangeven hoe deze activiteiten georganiseerd moeten zijn;
  - elementen die gerelateerd zijn aan beveiligingsaspecten die bij de activiteiten in acht moeten worden genomen.

- Control
  Binnen dit domein bevinden zich elementen die zorgdragen voor de beheersing van het geheel van activiteiten betreffende middleware.

2.2 Algemene en specifieke objecten

De objecten kunnen worden onderscheiden in algemene en specifieke objecten. Zie afbeelding 4. De algemene objecten zijn globaal voor alle IT-systemen van toepassing en komen in de meeste BIO Thema-uitwerkingen voor. In deze thema-uitwerking zijn ze toegespitst op middleware.

De specifieke objecten voor opslag van data en voor integratieservices zijn apart uitgewerkt in hoofdstuk 4 Uitvoeringsdomein. Voor de objecten uit het uitvoeringsdomein, zijn zoals bij elke thema-uitwerking, de nodige beleids- en beheersingsobjecten geformuleerd.



Afbeelding 4: Algemene en specifieke objecten van middleware

3 Beleidsdomein

3.1 Doelstelling

Controls en maatregelen uit dit domein geven aan welke specifieke vereisten als uitgangspunten gelden voor middleware. Hiermee geven organisaties de kaders aan waarbinnen de realisatie en operatie van middleware moet plaatsvinden. De controls en de maatregelen bevatten condities en randvoorwaarden die van toepassing zijn op de inrichting, beveiliging en beheersing van middleware.

3.2 Risico's

Als adequaat beleid voor de inrichting en beheersing van functionaliteiten en componenten (zoals gegevensverzamelingen) ontbreekt, is het risico dat onvoldoende sturing wordt gegeven aan een veilige inrichting en exploitatie van middleware. Daardoor kan de informatievoorziening van de organisatie als geheel in gevaar komen en kan de integriteit en vertrouwelijkheid van gegevens worden aangetast.

3.3 Objecten, controls en maatregelen

Tabel 1 toont de objecten die specifiek voor dit domein een rol spelen en ordent de beleidsobjecten per invalshoek (intentie, functie, gedrag of structuur). Dit domein bevat een aantal objecten met vermelding van de objectnaam, de positionering van het object met een basiselement (zie de tekst tussen haken) die in een invalshoek voorkomt en het objectnummer. De geel gemarkeerde objecten komen voor in de BIO2. De wit gemarkeerde objecten zijn betrokken uit andere best practices. Voor de identificatie van de objecten en de ordening is gebruik gemaakt van basiselementen.

Intentie	Functie	Gedrag	Structuur
B.01 Beleid middlewarecomponenten ((Operationeel) beleid)	/	B.03 Data en privacy (TR Data)	B.04 Middlewarearchitectuur en certificering (IT-organisatiestructuur)
B.02 Beleid informatietransport ((Operationeel) beleid)	/	/	/

Tabel 1: Beleidsobjecten met basiselementen voor middleware per invalshoek

3.3.1 *B.01 Beleid middlewarecomponenten*

Objectdefinitie

Resultaat van besluitvorming over toegestane middlewarefuncties.

Objecttoelichting

Voor de beveiliging van middlewarecomponenten en met name voor de toegang tot - en de verwerking van - data van deze componenten, hebben zowel de gebruikersorganisatie als de IT-leverancier verantwoordelijkheden. De gebruikersorganisatie stelt beleid op en is verantwoordelijk voor de data. De IT-leverancier verleent diensten op basis van beleidsdocumenten voor uitvoerings-, implementatie-,

evaluatie- en rapporteringsactiviteiten. De middlewarecomponenten zijn gerelateerd aan functionaliteiten, zoals aangegeven in afbeelding 2.

Doelstelling	Het beheersen van beveiliging van data in middlewarecomponenten.		
Risico	Ontbrekend of onvoldoende beleid voor het gebruik en de beveiliging van middlewarecomponenten kan leiden tot onbevoegde toegang tot of manipulatie van data, waardoor gevoelige informatie kan uitlekken, gegevens onjuist worden verwerkt en de betrouwbaarheid van informatie en bedrijfsprocessen van de organisatie wordt aangetast.		
Control	De leverancier behoort volgens een overeengekomen middlewarecomponenten**beleid** adequate maatregelen, zoals **classificatie**, te treffen om deze diensten te kunnen leveren.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beleid	1.	Er is een middlewarecomponentenbeleid vanuit de klant-organisatie waarin de eisen voor deze componenten zijn gedefinieerd en vastgesteld. Er moet speciale aandacht zijn voor het beschermen van de componenten tegen ransomware-aanvallen.	BIO2: 8.13.01
	2.	De leverancier heeft het beleid voor middlewarecomponenten gereviewd en zo nodig verbeteringen daarop voorgesteld.	CIP-netwerk
	3.	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is (in de middlewareomgeving) en wat de maximale hersteltijd is na een incident.	BIO2: 8.13.02
	4.	Het back-upproces via middlewarecomponenten voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere locatie.	BIO2: 8.13.03
	5.	De restoreprocedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.	BIO2: 8.13.04
	6.	De opzet en de instelling van integratiefuncties in middleware voldoet aan de geldende eisen voor softwareontwikkeling.	CIP-netwerk
	7.	Voor de toegang tot configuratie en beheer van integratiefuncties worden speciale toegangsrechten gehanteerd.	CIP-netwerk
Classificatie	8.	Aan data en middelen waarin/waarop zich data bevindt, wordt door de verwerkingsverantwoordelijke een classificatie toegekend, die gebaseerd is op datatype, waarde, gevoeligheid en kritische gehalte voor de organisatie.	CCM 2022 v4.05 (en hoger) (Cloud Security Alliance) Beleid informatietransport
	9.	Data gerelateerd aan e-commerce en verstuurd via publieke netwerken is adequaat geclassificeerd en beschermd tegen fraude, ongeautoriseerde toegang en aantasten/corrumperen van data.	CCM 2022 v4.05 (en hoger) (Cloud Security Alliance) Beleid informatietransport

3.3.2 *B.02 Beleid informatietransport*

Objectdefinitie

Beleid voor toegestane uitwisseling van data via berichtenverkeer.

Objecttoelichting

Integratiefuncties van middleware maken het mogelijk om data uit te wisselen met andere applicaties, zoals bijvoorbeeld basisregistraties. De technische functies bieden daarbij de mogelijkheid om voorafgaand aan het transport de verschillende data-elementen te rangschikken en bijvoorbeeld via aggregatie nieuwe data te genereren. Als brondata ook persoonsgebonden informatie bevat, dan is speciale aandacht voor de borging van privacy (onder andere Algemene Verordening Gegevensbescherming (AVG)-bepalingen) noodzakelijk.

Doelstelling	Het maken van beleid over welke informatie, in welke vorm via integratiefuncties uitgewisseld mag worden.		
Risico	Ontbrekend of onvoldoende beleid voor informatietransport via middleware-integratiefuncties kan ertoe leiden dat gegevens zonder duidelijke kaders worden uitgewisseld of bewerkt, waardoor informatie onbevoegd wordt verstrekt, privacy- en beveiligingseisen worden overtreden en de betrouwbaarheid en rechtmatigheid van gegevensuitwisseling en bedrijfsprocessen wordt aangetast.		
Control	Er behoren **regels, procedures of overeenkomsten voor informatieoverdracht** te zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.		BIO2: 5.14 ISO 27002:2022: 5.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Regels, procedures of overeenkomsten voor informatieoverdracht	1.	Het beleid voor informatieoverdracht omvat ten minste de volgende elementen: • de regels en procedures zijn afgestemd op het classificatieniveau van de informatie; • de regels en procedures bieden bescherming tegen risico's zoals ongeautoriseerde toegang, wijziging, onderschepping, kopiëren, vernietiging of denial-of-service; • onderwerp-specifieke richtlijnen over toegestane en aanbevolen methoden voor informatieoverdracht (digitaal, fysiek, verbaal, intern/extern); • richtlijnen voor de opslag en verwijdering van bedrijfsgegevens, inclusief berichten en overgedragen informatie; • aandacht voor relevante wettelijke, regelgevende en contractuele verplichtingen; • gedefinieerde verantwoordelijkheden, inclusief contactgegevens van betrokken partijen (zowel intern als extern). • eisen voor het waarborgen van traceerbaarheid en de integriteit van de bewakingsketen, bijvoorbeeld middels registratie van overdrachten en mechanismen voor onweerlegbaarheid (elektronische handtekening).	ISO 27002:2022: 5.14

	2.	Organisaties hanteren op basis van bewuste keuzes, procedures voor de uitwisseling van data via integratiefuncties van middlewarecomponenten.	CIP-netwerk
	3.	De (klant)organisatie heeft met een Privacy Impact Assessment (PIA) bepaald en vastgelegd welke applicaties en systemen berichten met elkaar en met partner organisaties uit mogen wisselen.	CIP-netwerk

3.3.3 *B.03 Data en privacy*

Objectdefinitie

Beleid voor de verwerking van data in middlewaretoepassingen.

Objecttoelichting

Integratiefuncties van middleware maken het mogelijk om berichten uit brondata samen te stellen en deze berichten met verschillende doelsystemen binnen de eigen organisatie of met andere organisaties uit te wisselen. Daarbij kunnen berichten door middlewarefuncties worden geaggregeerd en getransformeerd tot nieuwe data, bijvoorbeeld als input voor basisregistraties. Het is van belang dat organisaties zich bewust zijn van deze mogelijkheden voor dataverwerking en daar beleid over formaliseren. Als brondata persoonsgebonden informatie bevat, dan is speciale aandacht voor privacy (waaronder de AVG-bepalingen) noodzakelijk.

Doelstelling	Het formaliseren van de wijze waarop middleware de bedrijfs- en persoonsgebonden data mag verwerken.		
Risico	Ontbrekend of onvoldoende beleid voor de verwerking van bedrijfs- en persoonsgegevens binnen middlewaretoepassingen kan ertoe leiden dat data ongecontroleerd wordt geaggregeerd, getransformeerd of uitgewisseld, waardoor privacy-risico's onvoldoende worden onderkend en de organisatie niet voldoet aan wettelijke verplichtingen en maatschappelijke verwachtingen ten aanzien van gegevensbescherming.		
Control	Er behoort ter bescherming van bedrijfs- en persoonlijke data, beleid te zijn geformuleerd voor verwerking van data, tenminste voor: de vertrouwelijkheid en **versleuteling** van data, voor **transformatie en aggregatie**, voor toegang en **privacy**, classificatie en labelen en **bescherming tegen verlies** van gegevens.		ITU-T Part 5 2012: 8.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Versleuteling	1.	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: • Wanneer cryptografie ingezet wordt. • Wie verantwoordelijk is voor de implementatie. • Wie verantwoordelijk is voor het sleutelbeheer. • Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum Standaardisatie worden toegepast. • De wijze waarop het beschermingsniveau vastgesteld wordt. • Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	BIO2: 8.24.01

Transformatie en aggregatie	2.	Middlewarefuncties mogen uitsluitend, toegestane en geformaliseerde bewerkingen uitvoeren op bedrijfs- en persoonsgebonden data.	CIP-netwerk
Privacy	3.	Ter bescherming van data en van privacy zijn beveiligingsmaatregelen getroffen, in de vorm van een data-analyse, PIA, sterke toegangsbeveiliging en encryptie.	ITU-T Part 5 2012: 8.5
Bescherming tegen verlies	4.	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er moet speciale aandacht zijn voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.	BIO2: 8.13.01
	5.	Opslagsystemen zijn opgenomen in een disaster recovery- en de bedrijfscontinuïteitsplanning.	ISO 27040 2016: 7.3.4

3.3.4 *B.04 Middlewarearchitectuur en certificering*

Objectdefinitie

Op marktstandaards gebaseerde en gecertificeerde middleware-inrichting en –dienstverlening.

Objecttoelichting

Het beperken van beveiligingsrisico's begint bij het selecteren van de juiste IT- of cloud-leverancier. Klantorganisaties zijn bij hun selectieproces in hoge mate afhankelijk van relevante certificeringen van leveranciers en van onafhankelijke onderzoeken naar de actuele status daarvan. Cruciaal is dat leveranciers de kwaliteit van hun dienstverlening baseren op internationale standaarden, zoals National Institute of Standards and Technology (NIST) en Cloud Industry Forum (CIF) voor Cloud en dat zij hun processen uit eigen beweging, periodiek laten toetsen.

Voor klant-organisaties die hun IT-diensten betrekken van interne IT-leveranciers of organisaties die hun integratieservices delen met partnerorganisaties, geldt dat er naast certificeringen voldoende wederzijdse transparantie moet bestaan om connectiviteit en interoperabiliteit in samenhang veilig in te richten en te beheersen.

Doelstelling	Het bieden van het gewenste niveau van zekerheid aan klant-organisaties.	
Risico	Ontbrekende of onvoldoende geborgde middlewarearchitectuur en certificering kan ertoe leiden dat klantorganisaties onvoldoende zekerheid hebben over de kwaliteit en beveiliging van middleware-dienstverlening, waardoor zij beperkt kunnen sturen op de beschikbaarheid, integriteit en vertrouwelijkheid van data en onvoldoende garanties hebben dat de benodigde functionaliteit voor hun bedrijfsprocessen betrouwbaar beschikbaar is.	
Control	De leverancier hanteert relevante industriestandaards voor de **structuur** en beheersing van haar IT dienstverlening en draagt zorg voor relevante periodieke **certificeringen** van haar dienstverlening.	ISO 27040 2016: 7.7.4 of 7.7.5
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Structuur	1.	De structuur van organisatie en techniek, geleverd door interne IT-leveranciers of partnerorganisaties bevat de volgende aspecten: • beveiligingsbeleid van de klantorganisatie op basis van principes en wet- en regelgeving; • functioneel: type en scope van de middlewarediensten; • zoneringsmodel voor scheiding tussen organisatie van klanten; • trust framework (afspraken en maatregelen ter bevordering van vertrouwensrelatie); • risicomanagement; • beschrijving van de samenhang op hoofdlijnen.	BSI C5 2020: 5.1
	2.	De structuur geleverd door de externe IT- en cloud-leveranciers voldoet aan relevante internationale standaarden zoals bijvoorbeeld NIST en CIF of gelijkwaardig.	ISO 17789 2014: H7
Certificeringen	3.	IT-leveranciers die de CIF-Code of Practice (of gelijkwaardig) naleven, zullen zich op een open en transparante manier gedragen, wat rationele besluitvorming en beheer door inkopers van hun diensten mogelijk maakt.	CIP- netwerk

4 Uitvoeringsdomein

In het uitvoeringsdomein worden controls en maatregelen voor middlewarefunctionaliteiten opgenomen. Hiermee wordt onder andere gerefereerd naar functionaliteiten zoals het opslaan van gegevens (databases of database services, opslag, storage e.d.), het veiligstellen en herstellen van data (back-up en herstel) en de integratie van applicaties met hun omgeving, al dan niet via berichtenverkeer.

Eerst worden de objecten genoemd die voor middleware als geheel van belang zijn en vervolgens enkele specifieke objecten voor opslag en integratieservices.

4.1 Doelstelling

De doelstelling van het uitvoeringsdomein is het waarborgen dat organisatorische en technische voorzieningen voorhanden zijn om te garanderen dat middlewarefuncties voldoen aan de eisen van beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.

4.2 Risico's

Wanneer een adequate inrichting en operationeel beheer van middlewarefunctionaliteiten ontbreekt, is het risico dat:

- onbevoegden zich toegang verschaffen tot middlewarefaciliteiten en dat gebruikers met te ruime bevoegdheden ongewenste acties uitvoeren;
- de integriteit van gegevensverwerking geschaad wordt.
- Per object zijn specifieke risico's geformuleerd in de navolgende paragrafen.

4.3 Objecten, controls en maatregelen

Binnen het uitvoeringsdomein zijn specifieke inrichtings- en beveiligingsobjecten voor middleware beschreven en uitgewerkt naar controls en conformiteitsindicatoren. Zie tabel 2 voor het overzicht van beveiligingsobjecten in het uitvoeringsdomein. De rood gemarkeerde objecten komen voor in de BIO2. De wit gemarkeerde objecten zijn ontleend aan andere best practices. De objecten zijn ingedeeld naar de invalshoeken intentie, functie, gedrag en structuur.

Disclaimer: de mate waarin bepaalde objecten, controls en maatregelen van toepassing zijn, is sterk afhankelijk van het type leverancier dat de IT-diensten in samenhang levert aan de klantorganisatie en van de wijze van informatie-uitwisseling van de klant en leverancier met partnerorganisaties.

Voor de afname van middlewarefunctionaliteit van externe IT-leveranciers en SaaS-/iPaaS-leveranciers, zullen afnemers moeten sturen op certificering van leveranciers en het verplicht stellen van frequente audits en ethical hacking, waarbij de afnemer mee mag denken inzake de te valideren aspecten. (SaaS staat voor Software as a Service. iPaaS staat voor integration Platform as a Service).

Zie voor relevante objecten en maatregelen voor clouddiensten de BIO Thema-uitwerking Clouddiensten.

Intentie	Functie	Gedrag	Structuur

U.01 Richtlijnen en procedures middlewarefunctionaliteit ((Operationeel) beleid)	U.02 Rollen en verantwoordelijkheden middlewarefunctionaliteit (Taak/rol)	U.06 Logging en monitoring middleware (Eigenschap)	U.13 Capaciteitsbeheer (Proces)
/	U.03 Toegang tot middlewarefunctionaliteit (Autorisatie)	U.07 Ontwerpdocumentatie (Documentatie)	/
/	U.04 Hardening middlewarecomponenten (Eigenschap)	U.08 Vertrouwelijkheid en integriteit data (Kwaliteitsfactor)	/
/	U.05 Configuratie middlewarecomponenten (Handeling)	U.09 Betrouwbare dataopslag (Proces)	/
/	/	U.10 Dataherstel (Proces)	/
/	/	U.11 Schonen data en media (Proces)	/
/	/	U.12 Beveiliging berichtenverkeer (Kwaliteitsfactor)	/

Tabel 2: Uitvoeringsobjecten met basiselementen voor middleware per invalshoek

4.3.1 *U.01 Richtlijnen en procedures middlewarefunctionaliteit*

Objectdefinitie

Toepassing van gedocumenteerde inrichting en beheeractiviteiten.

Objecttoelichting

Middlewarefunctionaliteiten voeren de benodigde interactie en transacties uit tussen applicaties en het operating system en tussen de applicaties onderling. De functies kunnen binnen één enkele server uitgevoerd worden, maar ook via een keten van systemen (gedistribueerde omgeving). Richtlijnen en procedures zijn nodig voor het veilig uitvoeren van activiteiten als installeren, het verlenen van toegang tot middlewarefuncties en het operationele beheer.

Doelstelling	Het zorgen dat uitsluitend de juiste en gedocumenteerde activiteiten worden uitgevoerd.	
Risico	Ontbrekende of onvoldoende toegepaste richtlijnen en procedures voor middlewarefunctionaliteit kunnen ertoe leiden dat installaties, toegangsverlening en beheeractiviteiten niet eenduidig of gecontroleerd worden uitgevoerd, waardoor mogelijk datalekken kunnen ontstaan en de performance en beschikbaarheid van middleware en onderliggende bedrijfsprocessen onder druk komen te staan.	
Control	**Richtlijnen en procedures** voor middlewaremanagement en middlewarefunctionaliteiten behoren te worden gedocumenteerd en beschikbaar gesteld aan alle beheerders die ze nodig hebben.	BIO2: 5.37 ISO 27002:2022: 5.37

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Richtlijnen en procedures	1.	De leverancier past formele richtlijnen en procedures toe voor het installeren, onderhouden en toekennen van de toegang tot de middlewareomgeving/producten en het verzorgen van back-up/herstel.	CIP-netwerk
	2.	Er zijn formele intake-procedures voor het in beheer nemen van middlewareproducten.	CIP-netwerk
	3.	Middlewareproducten mogen als onderdeel van de IT-infrastructuur pas na het doorlopen van een formeel afgesproken acceptatietraject beschikbaar worden gesteld.	CIP-netwerk
	4.	De bedieningsprocedures voor middleware omvatten onder meer: • verantwoordelijkheden van betrokken personen; • instructies voor beveiligde installatie, configuratie en onderhoud van de systemen; • instructies voor het omgaan met fouten, uitzonderlijke omstandigheden en beperkingen op systeemhulpmiddelen; • ondersteunings- en escalatiecontacten, inclusief externe contacten; • procedures voor opnieuw opstarten en herstellen bij systeemstoringen; • beheer van audittrajecten, systeemlogs en videobewakingssystemen. • monitoring van capaciteit, prestaties en beveiliging.	ISO 27002:2022: 5.37

4.3.2 *U.02 Rollen en verantwoordelijkheden middlewarefunctionaliteit*

Objectdefinitie

Formele toewijzing van verantwoordelijkheden voor middleware.

Objecttoelichting

Beheerderstaken vereisen voor bepaalde middlewarefunctionaliteiten, zoals bijvoorbeeld de instelling van integratiefuncties, vergaande bevoegdheden met risico's voor de gebruikersorganisatie. Het beleggen van de juiste verantwoordelijkheden en het toezien op het beoogde gebruik daarvan vergt extra aandacht.

Doelstelling	Het zorgen dat de juiste verantwoordelijkheden worden gedefinieerd en toegewezen.	
Risico	Als rollen en verantwoordelijkheden voor middlewarefunctionaliteit niet duidelijk zijn gedefinieerd of toegewezen, bestaat het risico dat beheeractiviteiten met vergaande bevoegdheden onjuist of ongecontroleerd worden uitgevoerd, waardoor mogelijk datalekken kunnen ontstaan en de performance en beschikbaarheid van middleware en ondersteunende bedrijfsprocessen onder druk komen te staan.	
Control	Alle rollen en **verantwoordelijkheden** voor het installeren en onderhouden van middlewarefunctionaliteiten behoren te worden gedefinieerd en toegewezen.	BIO2: 5.02 ISO 27002:2022: 5.2
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Verantwoordelijkheden	1.	De verantwoordelijkheden aan beheerders zijn toegewezen op basis van beleidsregels voor de beveiliging van middlewarefunctionaliteiten.	ISO 27002:2022: 5.2
	2.	Verantwoordelijkheden voor bovengenoemde activiteiten bij middlewarefunctionaliteiten zijn toebedeeld aan specifieke functionarissen en rollen.	ISO 27002:2022: 5.2
	3.	De rollen en (speciale) bevoegdheden van beheerders van middlewarefunctionaliteiten zijn gedefinieerd en gedocumenteerd.	ISO 27002:2022: 5.2

4.3.3 *U.03 Toegang tot middlewarefunctionaliteit*

Objectdefinitie

Toegangscontrole voor middlewarefuncties en beheerinterfaces daarvan.

Objecttoelichting

Het verlenen van de logische toegang van personen en systeemfuncties tot middlewarefunctionaliteit is een essentiële beveiligingsmaatregel. Zie voor een bredere context het thema Toegangsbeveiliging. Toegang is nodig voor het opslaan van gegevens (databases en databaseservices), voor beheerinterfaces van opslagsystemen en voor het activeren of gebruiken van integratiefuncties. Het 'least privilege'-principe wordt bij voorkeur gebruikt voor toegang tot configuraties, operationeel beheer en wijzigingsbeheer.

Voor opslagsystemen worden rollen gebruikt zoals Security Administrator, Storage Administrator, Security Auditor en Storage Auditor (of soortgelijke benamingen). Elke logische toegang moet gekoppeld worden aan 'Security' of aan 'Storage', om daarmee functiescheiding in de beheerstaken te kunnen bewerkstelligen.

Vanwege de vergaande eigenschappen van de functies voor integratieservices en het afbreukrisico voor de organisatie voor illegaal gebruik daarvan, zijn speciale toegangsrechten en toegangscontroles op afname van berichtendiensten en beheerhandelingen essentieel. Als berichten gedeeld worden met applicaties van andere organisaties moet toegangscontrole tot de integratiefuncties 2-zijdig worden ingericht. Beide organisaties zijn in dat scenario verantwoordelijk voor de afname van hun deel van de integratieservices en het veilig uitvoeren van beheerhandelingen op de functies.

Doelstelling	Het voorkomen van onbevoegde toegang tot middlewarefuncties en beheerinterfaces.	
Risico	Als de toegangscontrole tot middlewarefunctionaliteit en bijbehorende beheerinterfaces onvoldoende is ingericht of gehandhaafd, bestaat het risico dat onbevoegden of te ruim geautoriseerde functies toegang krijgen tot integratie- en beheerfuncties, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van opgeslagen en verwerkte data mogelijk worden aangetast.	
Control	Het toewijzen en gebruik van speciale **toegangsrechten** tot de middlewarefunctionaliteiten en speciale systeemhulpmiddelen behoren te worden **beperkt** en **beheerst**.	BIO2: 8.2 BIO2: 8.18
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Toegangs-rechten	1.	Middlewarefunctionaliteiten, zoals databases, opslagbeheer en integratiefuncties mogen niet buiten reguliere paden om door gebruikers te benaderen zijn.	ISO 27040 2016: 6.4.2
	2.	Gebruikers verkrijgen toegang tot de middlewarefunctionaliteiten volgens de gedefinieerde reguliere paden en met goedkeurde additionele hulpmiddelen: • Beheerders identificeren zich op basis van (versterkte) authenticatie en via Privileged Access Management (PAM). • Gebruikers (systemen) identificeren zich met bijzondere middelen (PKIo e.d.). • API-sleutels moeten regelmatig gevalideerd worden, als verantwoordelijkheid van de eigen organisatie.	ISO 27040 2016: 6.4.2
	3.	Gegevens binnen middlewarecomponenten (of die door middlewarefunctionaliteiten worden geboden) mogen niet ongeautoriseerd worden gewijzigd.	ISO 27040 2016: 6.4.2
Beperkt	4.	Alleen bevoegd personeel heeft op die momenten dat toegang strikt noodzakelijk is toegang tot systeemhulpmiddelen.	BIO2: 8.18.01
	5.	Middleware biedt mechanismen, waarmee systeembeheerders, overeenkomstig hun verleende rechten en rollen, uitsluitend die handelingen kunnen uitvoeren die ze nodig hebben voor de uitoefening van hun taak.	BIO2: 8.02
Beheerst	6.	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	BIO2: 8.18.02
	7.	De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.	BIO2: 8.02.01

4.3.4 *U.04 Hardening middlewarecomponenten*

Objectdefinitie

Het uitschakelen van niet noodzakelijke functionaliteit.

Objecttoelichting

De standaardconfiguratie van de meeste middlewarecomponenten, zoals messaging middleware en databasemanagementservers is niet ontworpen met informatiebeveiliging als de primaire focus. De standaardinstellingen van deze producten zijn vooral gericht op bruikbaarheid, communicatie en functionaliteit. Hardening is het proces van het uitschakelen of verwijderen van overbodige en/of niet gebruikte functies, services en accounts, waarmee tevens de beveiliging wordt verbeterd. Ook middlewarecomponenten behoren te worden gehardend.

Dit uitschakelen van functies is voor middleware als Enterprise Service Bussen (ESB) lastig, vooral als een ESB een centrale rol speelt in de infrastructuur. Vooraf is niet te bepalen wanneer een bepaalde functie nodig is.

Doelstelling	Het verlagen van de kans op misbruik van standaard functionaliteiten.

Risico	Als middlewarecomponenten niet of onvoldoende worden gehardend, bestaat het risico dat overbodige of standaardfunctionaliteiten onnodig beschikbaar blijven, waardoor de kans op misbruik toeneemt en de beschikbaarheid, integriteit en vertrouwelijkheid van data mogelijk worden aangetast.		
Control	Voor het beveiligen van middlewarecomponenten behoren overbodige **functies** en ongeoorloofde **toegang** te worden uitgeschakeld.		ISO 27040 2016: 6.4.5
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Functies	1.	Alvorens hardening toe te passen, dienen organisaties te bepalen: • Bestaat er voor elke configuratie actuele documentatie en implementatiehandleidingen? • Hoe wordt aangetoond dat systemen voldoen aan de juiste configuratiestandaard? • Voor de systemen die niet kunnen worden gehardend, hoe worden deze gerechtvaardigd, gedocumenteerd en beheerd?	PCI-DSS v3 2013: 9.2
	2.	Middlewarecomponenten zijn zodanig geconfigureerd dat niet-essentiële en overbodige systeemtechnische services zijn uitgeschakeld.	ISO 27040 2016: 6.4.5
	3.	Middlewarecomponenten zijn zodanig geconfigureerd dat gebruik van onderstaande functies wordt beperkt: • Communicatiediensten die inherent vatbaar zijn voor misbruik • Communicatieprotocollen die gevoelig zijn voor misbruik	CIP-netwerk
Toegang	4.	Middlewarecomponenten zijn beschermd tegen ongeoorloofde toegang doordat: • onnodige of onveilige gebruikersaccounts zijn verwijderd; • belangrijke beveiliging-gerelateerde parameters juist zijn ingesteld.	ISO 27040 2016: 6.4.5

4.3.5 *U.05 Configuratie middlewarecomponenten*

Objectdefinitie

Het voor de gewenste eigenschappen instellen van systeemfuncties.

Objecttoelichting

De leverancier is op basis van een overeenkomst en het middlewarebeleid verantwoordelijk voor het configureren van middlewarecomponenten, bedoeld voor storage, archivering, back-up, herstel en integratieservices. Leveranciers zullen op dit gebied ook de noodzakelijke trainingen moeten verzorgen.

Doelstelling	Het zorgen voor voorspelbaar, gedocumenteerd gedrag van middlewarefuncties.	
Risico	Als middlewarecomponenten niet juist of niet consistent worden geconfigureerd, bestaat het risico dat het gedrag van middlewarefuncties onvoorspelbaar is, waardoor verstoringen in de dienstverlening kunnen optreden en de kans op datalekken of andere informatiebeveiligingsincidenten toeneemt.	
Control	De leverancier heeft volgens de **richtlijnen en procedures** de middlewarecomponenten geconfigureerd.	SoGP 2018: SY2
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Richtlijnen en procedures	1.	De richtlijnen en procedures voor het configureren van middlewarecomponenten hebben onder andere betrekking op: • het borgen van data-integriteit, replicatie, performance en servicelevels; • de klantvereisten voor de uitvoering van back-up en herstel; • het levenscyclusmanagementproces voor archivering en back-up en herstel; • de archivering en het back-up-proces; • het uitvoeringsproces van archivering en back-up- en herstelverzoek; • het testproces van archivering en back-up- en herstelprocedures; • trainingsfaciliteiten.	CIP-netwerk

4.3.6 *U.06 Logging en monitoring middleware*

Objectdefinitie

Vastlegging en monitoring van gebeurtenissen binnen het werkgebied van middleware.

Objecttoelichting

Vanwege de specifieke eigenschappen van middleware en in het bijzonder integratieservices, is het afbreukrisico voor de organisatie groot bij (on)bedoeld onjuist gebruik van deze functies. Het vastleggen van gebeurtenissen en beheerhandelingen (loggen) en de continue bewaking (monitoring) van geoorloofde afname van berichten via IT-diensten is daarom essentieel. Logging, monitoring en capaciteitsbeheer zullen in de operatie een onderdeel zijn van het systeembeheerproces voor middleware.

Doelstelling	Het verzamelen van bewijs over gebeurtenissen, waaronder de detectie van ongeoorloofd gebruik, en de continue bewaking van het nakomen van beleidsuitgangspunten.		
Risico	Ontbrekende of onvoldoende logging en monitoring van middlewareactiviteiten kan ertoe leiden dat afwijkingen van normaal gebruik, misconfiguraties of ongeoorloofde handelingen niet tijdig worden onderkend, waardoor incidenten zich onopgemerkt kunnen ontwikkelen en de impact op beschikbaarheid, integriteit of vertrouwelijkheid van gegevens toeneemt.		
Control	Middleware biedt continue signaleringsfuncties voor **registratie en detectie,** die **beveiligd** zijn ingericht.		SSD 2020: SSD-30
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Registratie en detectie	1.	In de middlewarearchitectuur zijn detectiemechanismen actief voor het vastleggen en detecteren van aanvallen (mechanismen leveren input aan een SIEM-systeem of gelijkwaardig).	SSD 2020: SSD-30/01.03 ISO 27040 2016: 6.4.4
	2.	De te registreren acties worden centraal opgeslagen (in een SIEM-systeem of gelijkwaardig).	SSD 2020: SSD-30/01.01 ISO 27040 2016: 6.4.4
	3.	Er is vooraf bepaald wat te doen bij het uitvallen van loggingsmechanismen (alternatieve paden).	SSD 2020: SSD-30/03.01
Beveiligd	4.	De (online of offline) bewaartermijn voor logging is vastgesteld en komt tot uitdrukking in de configuratie-instellingen van binnen het softwarepakket.	SSD 2020: SSD-30/03.02 ISO 27040 2016: 6.4.4

4.3.7 *U.07 Ontwerpdocumentatie*

Objectdefinitie

Specificaties van de technische samenhang van middlewarecomponenten.

Objecttoelichting

In de middlewarearchitectuur zijn de functionele relaties vastgelegd tussen middlewarecomponenten onderling en met andere componenten in de informatieketen. De ontwerpdocumentatie beschrijft op basis daarvan de ontworpen (ingestelde) technische relaties tussen de middlewarecomponenten en hoe configuraties wordt ingericht.

Doelstelling	Het zorgen voor inzicht en overzicht van functionele en technische relaties tussen middlewarecomponenten en hun actuele configuraties.		
Risico	Onvoldoende of niet-actuele ontwerpdocumentatie kan ertoe leiden dat configuratiewijzigingen niet goed worden overzien, waardoor het risico ontstaat op onvoorspelbaar gedrag van middlewarecomponenten, met mogelijke gevolgen voor beschikbaarheid en een verhoogde kans op informatiebeveiligingsincidenten, waaronder datalekken.		
Control	Het (her)ontwerp van middleware behoort te zijn **gedocumenteerd**.		SoGP 2018: SY1.1.1
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gedocumen-teerd	1.	Het ontwerp van middleware van informatiesystemen is gedocumenteerd, waarbij onder andere beschreven is: • de functies die door elke component worden geleverd; • de geactiveerde interactie met andere systemen; • op welke wijze configuratie en deployment mogelijk is.	SoGP 2018: SY1.1.1
	2.	Documentatie van een (her)ontwerp is bij voorkeur in een repository opgeslagen, om op eenvoudige wijze de impact van een aanpassing te kunnen bepalen.	CIP-netwerk

4.3.8 *U.08 Vertrouwelijkheid en integriteit data*

Objectdefinitie

Mate van vertrouwelijkheid en integriteit van de verwerkte en opgeslagen data.

Objecttoelichting

De vertrouwelijkheid van data die is opgeslagen binnen opslagsystemen (data in rust) en de vertrouwelijkheid tijdens transport van en naar de opslagsystemen, wordt meestal gehandhaafd met maskeringstechnieken zoals versleuteling, pseudonimisatie en anonimisatie. Raadpleeg voor versleuteling ISO/IEC 18033 2021 Information Security – Encryption algorithms, NIST FIPS 197 2001 Advanced Encryption Standard (AES), de IEEE 1619.2 2010 Standard for Wide-Block Encryption for Shared Storage Media en het Forum Standaardisatie.

Hoewel versleuteling noodzakelijk kan zijn, introduceert het ook beschikbaarheidsrisico's als in ketens fouten ontstaan vanuit de versleutelingstechnologie of fouten bij de uitgifte en het beheer van cryptosleutels. Betrouwbare technologie en adequaat beheer van cryptosleutels is daarom essentieel.

Zie voor sleutelbeheer ISO/IEC 11770 Standard for Key Management Techniques, NIST Special Publication 800-57Recommendation for Key Management en BIO 2019: 10.1.2. Als versleuteling wordt toegepast in combinatie met elektronische handtekeningen, kan daarmee behalve de vertrouwelijkheid tevens de authenticiteit en integriteit van de opgeslagen gegevens worden geverifieerd.

Doelstelling	Het beschermen van data tegen ongeoorloofd lezen, wijzigen of vernietigen door een correct en doeltreffend gebruik van maskeringstechnieken.		
Risico	Onvoldoende of onjuist toegepaste maskeringstechnieken en tekortschietend beheer van cryptografische sleutels kunnen ertoe leiden dat data niet afdoende wordt beschermd tegen ongeoorloofd lezen, wijzigen of vernietigen, waardoor de kans toeneemt op datalekken en aantasting van beschikbaarheid, vertrouwelijkheid en integriteit van gegevens.		
Control	Gevoelige data behoort volgens het overeengekomen beleid over maskerings- of crypto-maatregelen, tijdens opslag voor onbevoegden te zijn **gemaskeerd of versleuteld**.		ISO 27040 2016: 6.8.2 ISO 27040 2016: 7.5 BIO2: 8.24
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Gemaskeerd of versleuteld	1.	Voor dataopslag dienen uitsluitend adequate encryptiealgoritmen en -methoden van maskering te worden toegepast.	ISO 27040 2016: 6.8.2.3
	2.	Waar mogelijk dient een centraal toepasbaar sleutelbeheersysteem te worden toegepast voor de generatie en archivering van cryptosleutels.	ISO 27040 2016: 6.8.2.3
	3.	De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van de AIVD.	BIO2: 8.24.04
	4.	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit de risicoafweging blijkt dat deze noodzakelijk zijn als onderdeel van gereedheid voor bedrijfscontinuiteit.	BIO2: 8.24.05

4.3.9 *U.09 Betrouwbare dataopslag*

Objectdefinitie

Mate waarin de data ononderbroken beschikbaar is voor eindgebruikers.

Objecttoelichting

De technische betrouwbaarheid van opslagsystemen bepaalt in hoge mate de beschikbaarheid van de opgeslagen data. Technische betrouwbaarheid is gespecificeerd als: MTBF (Mean Time Between Failures), MTTR (Mean Time To Repair) en MTTF (Mean Time To Failure).

De effectieve beschikbaarheid van opslag bepaalt de toegankelijkheid van data, die kan worden uitgedrukt in de verhouding van de tijd waarin de data beschikbaar is ten opzichte van de niet beschikbare tijd. Voor een zeer hoge beschikbaarheid, bijvoorbeeld 7x24 uur en 99,999% dient kostbare hardware en softwarematige redundantie te worden toegepast. Aanvullend is het belangrijk eisen te stellen aan het maximum aantal onderbrekingen per uur, dag of jaar.

Lange bewaartijd van opslag impliceert veel zorg voor data-integriteit, authenticiteit en privacy-aspecten. Dit is minder van toepassing op systemen met een beperkte bewaartijd.

Doelstelling	Het implementeren van maatregelen die naar de behoefte van de klant zorgen voor een ononderbroken toegang tot de data. Het kunnen vertrouwen op de beschikbaarheid en integriteit van de data.		
Risico	Onvoldoende betrouwbaarheid of beschikbaarheid van dataopslag kan ertoe leiden dat gegevens tijdelijk of structureel niet toegankelijk zijn of beschadigd raken, waardoor de continuïteit van de bedrijfsvoering onder druk komt te staan en herstelmaatregelen noodzakelijk worden.		
Control	Opslagfaciliteiten behoren met voldoende **redundantie** te worden geïmplementeerd om aan **beschikbaarheidseisen** te voldoen.		BIO2: 8.14
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Redundantie	1.	De beveiliging van opslagfaciliteiten bevat verschillende lagen van redundancy, waarmee 'single points of failure' worden voorkomen en de overeengekomen beschikbaarheid van data kan worden gegarandeerd.	ISO 27040 2016: 7.2.3
	2.	Redundancy moet zoveel mogelijk worden benut.	ISO 27040 2016: 7.3.5
Beschikbaar-heidseisen	3.	De technische betrouwbaarheid van opslagsystemen mag de effectiviteit van beveiligingsfuncties niet kunnen beïnvloeden.	ISO 27040 2016: 7.3.1
	4.	Kwetsbaarheden van opslagsystemen dienen proactief te worden verholpen om hun impact op de betrouwbaarheid te beperken.	ISO 27040 2016: 7.3.1

4.3.10 *U.10 Dataherstel*

Objectdefinitie

Herstel van data na een technische uitval of de vernietiging van opslagsystemen.

Objecttoelichting

Tijdens de normale bedrijfsvoering kunnen (opslag)systemen uitvallen en kan de opgeslagen data verminkt worden door een defect of door andere oorzaken. Een betrouwbare storage-architectuur moet in deze situaties inherente mogelijkheden te bieden voor herstel van de data.

Een traditionele methode is back-up en herstel. Bij grote informatiesystemen is de back-up en herstelprocedure vaak niet meer toepasbaar en wordt de data van uitgevallen elementen hersteld, gebruikmakend van andere methoden zoals mirroring, Redundant Array of Independent Disks (RAID), Journaling-technologie of combinaties daarvan.

Wanneer opslagsystemen uitvallen als gevolg van calamiteiten, waarbij de normale bedrijfsvoering van de leverancier niet meer mogelijk is, zijn zogenaamde Disaster Recovery (DR) methodieken nodig en andere maatregelen, bestuurd vanuit bedrijfscontinuïteitsmanagement. Ook uitwijkscenario's zijn toegepaste oplossingen voor herstel van data en bedrijfsprocessen nadat een calamiteit is opgetreden.

Bij de uitwijk-oplossing worden systemen en hun dataopslag tijdelijk op een alternatieve fysieke locatie voortgezet totdat de bronsystemen hersteld zijn. Voor bedrijfscontinuïteit hanteren we in de BIO-thema-uitwerkingen de eisen en begrippen zoals die genormeerd zijn in ISO 22301 2019 Security and resilience.

Doelstelling	Het kunnen herstellen van data na storingen, diefstal, systeemuitval of calamiteiten. Het beschermen tegen het verlies van gegevens.		
Risico	Wanneer voorzieningen voor dataherstel onvoldoende zijn ingericht of niet betrouwbaar functioneren, bestaat het risico dat gegevens na storingen, systeemuitval of calamiteiten niet (tijdig) kunnen worden hersteld, waardoor de continuïteit van de bedrijfsvoering in gevaar komt.		
Control	Regelmatig behoren **back-upkopieën** van informatie te worden gemaakt en **getest** in overeenstemming met een overeengekomen back-upbeleid.		BIO2: 8.13
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Back-upkopieën	1.	Back-upinformatie is beschermd tegen ongeautoriseerde toegang, bijvoorbeeld met encryptie.	ISO 27040 2016: 7.3.3
	2.	Uitsluitend geautoriseerde personen hebben toegang tot back-upmedia.	ISO 27040 2016: 7.3.3
	3.	Kopieën voor bedrijfs-kritische informatie worden met passende zorg voor betrouwbaarheid, fout-tolerantie en performance gemaakt en beheerd.	ISO 27040 2016: 7.3.3
	4.	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	BIO2.0-opmaat: 8.13.2 BIO 2019: 12.3.1.2
Getest	6.	Periodiek (minimaal jaarlijks en na een grote wijziging) wordt getest of herstel van back-updata werkt en of disaster recovery van opslagsystemen functioneert.	ISO 27040 2016: 7.3.4 BIO2: 8.13.04

4.3.11 *U.11 Schonen data en media*

Objectdefinitie

Onherstelbaar vernietigen van de data op ontkoppelde opslagmedia.

Objecttoelichting

De inhoud van opslagmedia moet onherstelbaar vernietigd worden, wanneer media niet langer nodig zijn of worden verwijderd of vervangen. Sanitization verwijst naar het proces van het zodanig vernietigen van eerder geschreven gegevens, dat de gewiste gegevens niet meer kunnen worden gelezen of gereconstrueerd.

Als media-schoning een onderdeel vormt van naleving, moeten de eigenschappen van de media worden beoordeeld om te bepalen welke overschrijftechnieken verplicht dienen te worden gebruikt.

Doelstelling	Het voorkomen van, die op (niet meer gebruikte) media is opgeslagen, als deze media in andere systemen wordt hergebruikt of in handen van onbevoegden terechtkomen.
Risico	Wanneer data en opslagmedia niet zorgvuldig en onherstelbaar worden geschoond bij buitengebruikstelling of hergebruik, bestaat het risico dat achtergebleven gegevens kunnen worden teruggelezen of misbruikt, wat kan leiden tot onbevoegde openbaarmaking van informatie en mogelijke schade voor de organisatie.

Control	Media behoren op een veilige en **beveiligde** manier te worden **verwijderd** als ze niet langer nodig zijn, overeenkomstig formele procedures.		BIO2: 7.10
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Beveiligd verwijderd	1.	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten, de bedrijfsgevoellige inhoud onherstelbaar verwijderd is.	BIO2: 7.10.01
	2.	• Er wordt gecontroleerd of alle data onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt; • Er wordt gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) een positief inzetadvies afgegeven heeft.	BIO2: 7.10.02

4.3.12 *U.12 Beveiliging berichtenverkeer*

Objectdefinitie

Beveiliging van het berichtenverkeer met gebruikers en tussen systeemcomponenten onderling.

Objecttoelichting

De beveiliging van het berichtenverkeer omvat beveiligingsmechanismen die bescherming bieden tegen Cross-Site Scripting (XSS), SQL Injections en andere bedreigingen voor het berichtenverkeer.

Om de vertrouwelijkheid, integriteit en authenticiteit van berichten in gedistribueerde omgevingen zeker te stellen, wordt op de middleware-laag vaak gebruik gemaakt van Message-level security. Deze set van maatregelen regelt onder meer hoe berichten tussen een client-applicatie en een webservice moeten worden versleuteld en/of digitaal ondertekend.

Doelstelling	Het handhaven van de beveiliging van uitgewisselde informatie binnen het ICT-landschap van een organisatie en met externe entiteiten.		
Risico	Wanneer het berichtenverkeer tussen systemen en gebruikers onvoldoende is beveiligd, bestaat het risico dat berichten worden onderschept, gemanipuleerd of misbruikt, waardoor de vertrouwelijkheid, integriteit en beschikbaarheid van uitgewisselde gegevens kunnen worden aangetast.		
Control	Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van **onvolledige overdracht**, foutieve routering, **onbevoegd wijzigen** van berichten, **onbevoegd openbaar** maken, onbevoegd vermenigvuldigen of afspelen.		CIP-netwerk
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Onbevoegd	1.	Er kunnen uitsluitend berichten van en met geauthentiseerde gebruikers en systemen worden uitgewisseld.	CIP-netwerk
	2.	De applicaties en systemen die berichten uitwisselen zijn bekend.	CIP-netwerk
Onvolledige overdracht	3.	Fout of onvolledig uitgewisselde data wordt herkend en hersteld.	CIP-netwerk

Onbevoegd wijzigen	4.	Het dataverkeer van of naar de vertrouwde omgeving, wordt bewaakt/geanalyseerd op verdacht verkeer met detectievoorzieningen.	BIO2: 8.21.02
	5.	Geavanceerde en/of gekwalificeerde elektronische handtekeningen moeten voldoen aan de Advanced Electronic Signatures (AdES Baseline Profiles), zoals opgenomen in de Lijst open standaarden van Forum Standaardisatie.	BIO2: 5.14.3
Onbevoegd openbaar	6.	Maak bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated-certificaten. Maak bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten kunnen voortvloeien uit een risicoanalyse, aansluitvoorwaarden of wetgeving.	BIO2: 5.14.02
	7.	Internetfacing-informatiesystemen en e-mail- berichtenverkeer moeten blijvend voldoen aan de verplichte standaarden, zie hiervoor de website van het Forum Standaardisatie. Hierop wordt gestuurd met de metingen van internet.nl. Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.	BIO2: 5.14.01

4.3.13 *U.13 Capaciteitsbeheer*

Objectdefinitie

Bewaking van de belasting van het back-end-systeem, proactieve signalering van ontwikkelingen daarin en tijdige advisering over toekomstige capaciteitsbehoefte.

Objecttoelichting

Met het oog op de continuïteit van bedrijfsvoering en dienstverlening is het van belang dat servers steeds voldoende capaciteit behouden voor het waarmaken van het afgesproken serviceniveau. Monitoring van vraag en aanbod vanuit client-systemen en tijdige aanpassing van de capaciteit als deze groeien, is daarom nodig.

Denial of Service (DoS)- of Distributed Denial of Service (DDoS)-situaties kunnen de continuïteit in hoge mate verstoren. Belangrijk is na te gaan welke maatregelen zijn genomen om deze aanvallen vroegtijdig te signaleren en waar mogelijk af te slaan.

Doelstelling	Het voorkomen van overbelasting van de keten. Het bieden van een ‘eerlijke’ verdeling van de beschikbare capaciteit over de afnemers van de services.	
Risico	Wanneer capaciteitsbeheer van middleware en achterliggende systemen onvoldoende is ingericht of gemonitord, bestaat het risico dat piekbelasting of aanvallen (zoals DoS/DDoS) leiden tot overbelasting van de keten, waardoor de continuïteit van het berichtenverkeer en de dienstverlening voor afnemers onder druk komt te staan.	
Control	Het gebruik van middelen behoort te worden **gemonitord** en **beoordeeld**, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	BIO2: 8.06

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Gemonitord	1.	De doorvoercapaciteit van de integratievoorziening wordt bewaakt op: • behalen van gestelde capaciteitsdoelen; • voorkomende piek- en dal-perioden; • voorkomende bottlenecks zoals overbelasting inclusief te lange netwerk queues, latency en netwerk jitter.	SoGP 2018: SY2.2.1
	2.	Netwerken waar integratievoorzieningen gebruik van maken, worden bewaakt op DoS- en DDoS-aanvallen.	CIP-netwerk
Beoordeeld	3.	De resultaten van monitoractiviteiten worden gereviewd en gepresenteerd aan de eigenaren van de bedrijfsprocessen. (De aanbieder wordt daarbij geacht een plan B te hebben als de limieten van de dienstverlening structureel behaald/overschreden worden.)	SoGP 2018: SY2.2.5

5 Control-domein

5.1 Doelstelling

De doelstelling van het control-domein voor middleware is te zorgen en/of vast te stellen dat:

- de middlewarefunctionaliteiten afdoende zijn ingericht voor het leveren van het gewenste niveau van de middlewarediensten;
- het juiste beveiligingsniveau wordt gegarandeerd.
- Dit houdt onder meer in dat binnen de organisatie een adequate beheersingsorganisatie moet zijn ingericht waarin beheerprocessen zijn vormgegeven.

5.2 Risico's

Als de noodzakelijke maatregelen voor beheersing binnen de organisatie ontbreken, dan is het risico dat de middlewareomgeving niet aan de beoogde organisatorische en beveiligingsvoorwaarden voldoet. Ook kan niet worden vastgesteld dat de gewenste maatregelen daadwerkelijk worden nageleefd.

5.3 Objecten, controls en maatregelen

Tabel 3 toont de objecten die specifiek voor dit domein een rol spelen. Elk blauw gemarkeerd object komt voor in de BIO. De wit gemarkeerde objecten zijn betrokken uit andere best practices. De objecten zijn ingedeeld naar de invalshoeken: intentie, functie, gedrag of structuur. De overeenkomstige basiselementen staan tussen haken genoteerd.

Intentie	Functie	Gedrag	Structuur
C.01 Evaluatie-richtlijnen (Assessment)	C.04 Rapporteren middlewarefunctionaliteiten (Proces)	C.05 Monitoren gebruikers- en beheerdersactiviteiten (Event/historie)	/
C.02 Evaluatie naleving beleid (Assessment)	/	/	/
C.03 Beoordeling middlewarefunctionaliteit (Assessment)	/	/	/

Tabel 3: Control-objecten met basiselementen voor middleware per invalshoek

5.3.1 *C.01 Evaluatierichtlijnen*

Objectdefinitie

Vooraf vastgestelde regels voor het evalueren/controleren van middlewarefunctionaliteiten.

Objecttoelichting

Richtlijnen voor evaluatie zijn noodzakelijk om te zorgen dat evaluatieactiviteiten betrouwbaar worden uitgevoerd en dat op de resultaten van de controles kan worden gebouwd.

Doelstelling	Een betrouwbaar controleproces en het betrouwbaar kunnen rapporteren van tekortkomingen aan het management.	
Risico	Wanneer evaluatierichtlijnen ontbreken of onvoldoende zijn uitgewerkt, bestaat het risico dat controle-activiteiten niet gestructureerd of consistent worden uitgevoerd, waardoor het voor het management lastig wordt om vast te stellen of middlewarefunctionaliteiten periodiek en toereikend worden beoordeeld.	
Control	**Evaluatie-richtlijnen** behoren te zijn vastgesteld om de implementatie en beveiliging van middlewarefunctionaliteiten te controleren, waarbij tekortkomingen tijdig aan het management worden gerapporteerd.	CIP-netwerk

Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Evaluatie-richtlijnen	1.	De leverancier beschikt over richtlijnen voor het beoordelen van de technische omgeving van middlewarefunctionaliteiten (onder andere geleverd door middlewareproducten en de database).	CIP-netwerk
	2.	De leverancier beschikt over geautomatiseerde middelen voor een effectieve ondersteuning van de controle-activiteiten.	CIP-netwerk
	3.	De leverancier beschikt over richtlijnen voor het uitvoeren van registratie, statusmeting, analyse, rapportage en evaluatie.	CIP-netwerk
	4.	De leverancier heeft de taken, verantwoordelijkheden en bevoegdheden van controlefunctionarissen vastgelegd.	CIP-netwerk

5.3.2 *C.02 Evaluatie naleving beleid*

Objectdefinitie

Periodieke evaluatie van de naleving van het beleid voor bewaken en herstellen van middlewarefunctionaliteiten.

Objecttoelichting

In het belang van de continuïteit is het noodzakelijk om het beleid voor 'Bewaken en herstellen' (back-up, herstel, uitwijkvoorziening en dergelijke) en de overeenkomsten hieromtrent, regelmatig te beoordelen op naleving. Welke oplossing de leverancier voor data- of functioneel herstel toepast, is een verantwoordelijkheid van de leverancier, al dan niet vastgelegd in een overeenkomst. De leverancier beoordeelt periodiek zowel de organisatorische als de technische aspecten van het overeengekomen beleid.

Doelstelling	Het vaststellen of de middlewarefunctionaliteiten 'Bewaken en herstellen' volgens het overeengekomen beleid worden geboden.	
Risico	Wanneer de naleving van het beleid voor bewaken en herstellen niet periodiek wordt geëvalueerd, bestaat het risico dat onvoldoende inzicht ontstaat in de mate waarin middlewarefunctionaliteiten conform afspraken worden geleverd, waardoor afwijkingen of tekortkomingen niet tijdig worden onderkend.	
Control	De leverancier behoort regelmatig de naleving van richtlijnen en procedures voor de uitvoering van middlewarefunctionaliteiten 'Bewaken en herstellen' te **beoordelen** aan de hand van de desbetreffende beleidsregels.	BIO2: 5.36

Conformiteitsindicator, nummer en maatregel			Afgeleid/afkomstig van
Beoordelen	1.	De toegekende autorisaties aan gebruikers en de daarbij behorende rechten zijn afgestemd met de klant en de wijze waarop dit wordt gelogd, is gedefinieerd. Voor beheerders wordt bij voorkeur PAM toegepast.	CIP-netwerk
	2.	De naleving van het beleid voor Bewaken en Herstellen wordt door de leverancier periodiek getoetst en geëvalueerd, waarbij tenminste wordt bepaald: • welke afwijkingen er zijn tussen beleid en uitvoering; • welke maatregelen worden getroffen om de uitvoering (weer) te laten voldoen aan het beleid.	CIP-netwerk

5.3.3 *C.03 Beoordeling middlewarefunctionaliteit*

Objectdefinitie

Periodieke beoordeling van middlewarefunctionaliteiten, gericht op de organisatorische en technische aspecten van deze omgevingen.

Objecttoelichting

Om de betrouwbaarheid en veiligheid van middlewarefunctionaliteit doeltreffend te kunnen beheersen, dienen periodiek zowel de organisatorische als technische aspecten van deze omgevingen beoordeeld te worden. Voorbeelden van deze aspecten zijn: de toepassing van het geformuleerd inrichtingsbeleid voor servers, serverplatformarchitectuur, rollen en verantwoordelijkheden, gebruik van technische middelen, controle-aanpak en inschakelen van externe specialisten. Als resultaat van de beoordeling dient een rapportage van bevindingen aan het management te worden uitgebracht.

In de situatie dat de dienst in de vorm van SaaS of PaaS wordt geleverd, zijn de hiervoor genoemde beoordeling en rapportage een verantwoordelijkheid van de aanbieder en moet dit als eis worden meegenomen als onderdeel van de aanbesteding.

Doelstelling	Het tijdig traceren van tekortkomingen in middlewarefunctionaliteiten en of het beheer daarvan alsmede het nemen van adequate maatregelen.	
Risico	Wanneer middlewarefunctionaliteiten en het bijbehorende beheer niet periodiek worden beoordeeld, bestaat het risico dat organisatorische en technische tekortkomingen niet tijdig worden gesignaleerd, waardoor corrigerende maatregelen uitblijven en de betrouwbaarheid en veiligheid van de dienstverlening onder druk komen te staan.	
Control	Middlewarefunctionaliteiten en technische omgevingen waarin ze actief zijn, behoren regelmatig op **naleving** van de **richtlijnen** ten aanzien van **toegang** te worden beoordeeld en **gerapporteerd**.	BIO2: 5.35
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Naleving	1.	• Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's van de feitelijke veiligheid. Dit kan door middel van (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten. • Internetfacing-informatiesystemen worden bij voorkeur continue getest op zwakheden en kwetsbaarheden.	BIO2: 8.08.04
	2.	De periodieke beoordelingen worden uitgevoerd door personen met een onafhankelijke positie, zoals een interne of externe auditor. De personen die deze beoordelingen uitvoeren, beschikken over de passende competentie.	ISO 27002:2022: 5.35
	3.	De resultaten van de onafhankelijke beoordelingen worden geregistreerd en gerapporteerd aan het management dat de beoordelingen heeft geïnitieerd. Indien nodig initieert het management corrigerende maatregelen.	ISO 27002:2022: 5.35
Richtlijnen	4.	De leverancier voert periodiek controles uit op de toegekende autorisaties voor middlewarefunctionaliteiten.	CIP-netwerk
	5.	De leverancier beschikt over richtlijnen voor het beoordelen van de technische omgeving van middlewarefunctionaliteiten.	CIP-netwerk
Toegang	6.	De toegekende autorisaties aan gebruikers en de daarbij behorende rechten zijn afgestemd met de klant en de wijze waarop dit wordt gelogd is gedefinieerd. Voor beheerders wordt bij voorkeur PAM toegepast.	CIP-netwerk
Gerapporteerd	7.	De leverancier rapporteert de afwijkingen op de toegang tot middleware, inclusief de reden hiervan.	CIP-netwerk

5.3.4 *C.04 Rapporteren middlewarefunctionaliteiten*

Objectdefinitie

Evalueren van de implementatie van middlewarefunctionaliteiten en het rapporteren van de resultaten hiervan aan het management van de klant.

Objecttoelichting

Om de gebruikersorganisatie in staat te stellen het beleid omtrent middlewarefunctionaliteiten te kunnen bijstellen, dan wel daarover aanvullende afspraken te kunnen maken, is het noodzakelijk dat de leverancier rapportages uitbrengt met specifieke informatie over de implementatie en de beschikbaarheid.

Doelstelling	Het bieden van tijdig inzicht in implementatieactiviteiten en beschikbaarheid van middlewarefunctionaliteiten.
Risico	Wanneer niet of onvoldoende wordt gerapporteerd over de implementatie en beschikbaarheid van middlewarefunctionaliteiten, bestaat het risico dat het management onvoldoende inzicht heeft om tijdig bij te sturen op informatiebeveiliging en gemaakte afspraken.

Control	De leverancier behoort periodiek te **rapporteren** over de implementatie, performance en beschikbaarheid van middlewarefunctionaliteiten en review-activiteiten.		ISO 27002:2022: 5.22
Conformiteitsindicator, nummer en maatregel			**Afgeleid/afkomstig van**
Rapporteren	1.	In de rapportages wordt, onder andere, aandacht besteed aan: • implementatieactiviteiten van middlewarefunctionaliteiten en getroffen maatregelen/voorzieningen hieromtrent; • de performance van de services; • incidenten over middlewarefunctionaliteiten die mogelijk invloed hebben gehad op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie-verwerkende systemen; • analyse van incidenten en mogelijke verbeteringsvoorstellen.	CIP-netwerk

5.3.5 *C.05 Monitoren gebruikers- en beheerdersactiviteiten*

Objectdefinitie

Continue bewaking van beveiligingsgebeurtenissen en rapportage van verdachte activiteiten.

Objecttoelichting

Het vanuit een auditrol monitoren van gebruikers- en beheerdersactiviteiten heeft tot doel ongeautoriseerde toegangspogingen tot middlewarefunctionaliteiten (zoals databases) tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringsfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris. Monitoring zoals hier bedoeld, is gericht op vastgelegde gebruikers- en beheerdershandelingen. De geregistreerde gegevens dienen te worden geanalyseerd en gerapporteerd (alerting). Alerting kan geautomatiseerd plaats vinden na overschrijding van vastgestelde drempelwaarden.

Doelstelling	Het tijdig vaststellen van onjuist gebruik en verdachte activiteiten aan middlewarefunctionaliteiten. Het tijdig rapporteren van bevindingen.	
Risico	Wanneer gebruikers- en beheerdersactiviteiten onvoldoende worden gemonitord en geanalyseerd, bestaat het risico dat ongeautoriseerde of onjuiste handelingen niet tijdig worden vastgesteld en dat achteraf niet kan worden vastgesteld wie welke acties heeft uitgevoerd, waardoor opvolging en verantwoording worden bemoeilijkt.	
Control	De organisatie **reviewt** en **analyseert** regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten aan middlewarefunctionaliteiten vast te stellen en bevindingen aan het management te **rapporteren**.	ISO 27002 2017: 12.4.1
Conformiteitsindicator, nummer en maatregel		**Afgeleid/afkomstig van**

Reviewt	1.	De verantwoordelijke functionaris analyseert periodiek: • de gelogde gebruikers-en activiteitengegevens betreffende middlewarefunctionaliteiten; • het optreden van verdachte gebeurtenissen[1] en mogelijke schendingen van de beveiligingseisen; • eventuele ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden van middlewarefunctionaliteiten.	ISO 27002:2022: 8.16
Analyseert	2.	De verzamelde loginformatie van middlewarefunctionaliteiten wordt in samenhang geanalyseerd.	ISO 27002:2022: 8.16
	3.	Periodiek worden de geanalyseerde en beoordeelde gelogde (gesignaleerde) gegevens aan de eigenaren van middlewarefunctionaliteit aan het management gerapporteerd.	ISO 27002:2022: 8.16
	4.	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen adequaat en tijdig behandeld.	BIO2: 8.16.03
	5.	De rapportages uit de beheerdisciplines compliancy-management, vulnerability-assessment, penetratietest en logging en monitoring worden geanalyseerd en geëvalueerd op aanwezigheid van structurele risico's.	ISO 27002:2022: 8.16
Rapporteren	6.	De analyse bevat informatie over kwetsbaarheden, zwakheden en misbruik en wordt gecommuniceerd met het verantwoordelijk management.	ISO 27002:2022: 8.16
	7.	De eindrapportage bevat, op basis van analyses, verbeteringsvoorstellen voor beleid en uitvoering.	ISO 27002:2022: 8.16

[1] Verdachte gebeurtenissen zijn afwijkend en opmerkelijk gedrag van gangbare patronen en geldende (beleids)regels.

Bijlage 1: Use case Interne applicatie-integratie

Integratieservices

In deze implementatie worden twee bijna gelijkwaardige applicatie-eindpunten binnen een rekencentrum met elkaar verbonden voor berichtenverkeer. Dit kunnen overigens ook volstrekt verschillende informatiesystemen zijn die verschillende formaten van data gebruiken. Het linker bedrijfsproces (rood) kan daarmee communiceren met het rechter bedrijfsproces (blauw), zie applicatie A. In afbeelding 5 zijn de integratiefuncties (blauw) geschetst in een communicatieketen van applicatie A naar B met daaronder in rode blokken de beveiligingsobjecten.

Oplossing

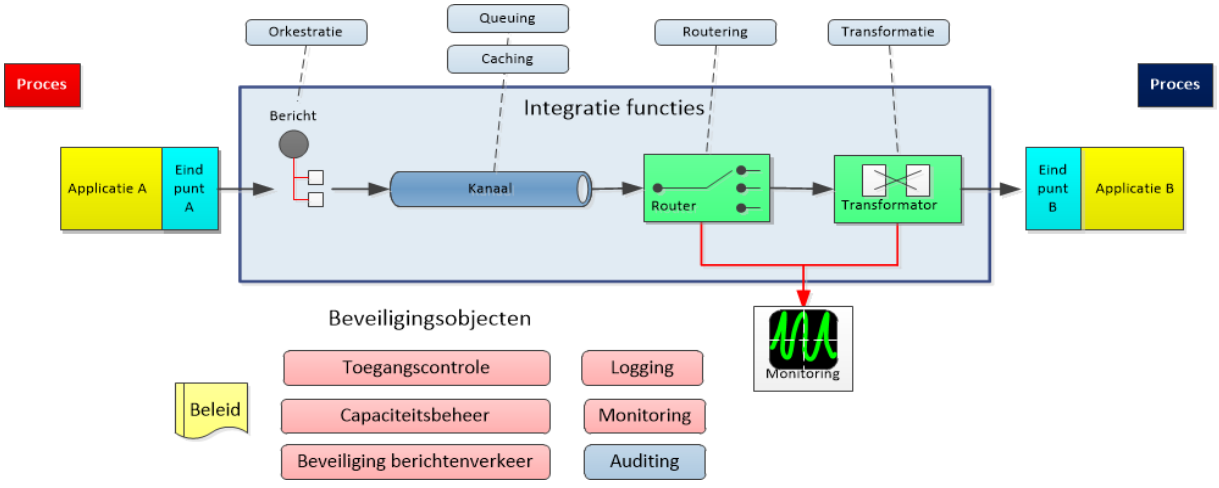
Applicatie A stelt een bericht samen en zet die via zijn eindpunt op de lijn. De orkestratiefunctie hakt het bericht in geschikte stukjes en stuurt die in porties achtereenvolgens via het communicatiekanaal naar de router. NB: Orkestratie omvat in de praktijk een vorm van workflow. In onderstaand voorbeeld, met eenvoudige berichtuitwisseling is het voor de volledigheid erbij gezet.

De router zorgt ervoor dat het bericht van A altijd bij de juiste eindpunt terechtkomt. Er kunnen namelijk meerdere systemen achter hangen, zoals onder andere geschetst is in bijlage 4 Use Case End-to-end applicatie-integratie.

De transformator zet het bericht vervolgens om in het gewenste formaat wat het doeleindpunt kan lezen. Daarna wordt het bericht doorgegeven aan applicatie B voor het bedrijfsproces.

De queuing- en caching-functies dienen voor tijdelijke buffering zodat alle elementen in de keten optimaal benut kunnen worden voor een optimale performance en een minimale doorlooptijd. Caching is een taak van het integratieplatform. Queuing kan ook onderdeel zijn van applicatie A of B.

De elementen van de integratieketen dienen te zijn opgebouwd onder een regime van een soft- of hardware-ontwikkelproces, waarin securitymaatregelen een integraal onderdeel vormen van de systeemarchitectuur en het ontwerp van A, B, van beide, of als afzonderlijke infrastructuur. Het systeembeheer van de integratiefuncties vereist bijzondere gebruikersrechten. In de volgende bijlagen zijn enkele implementaties van integratieservices geschetst.



Afbeelding 5: Integratiefuncties en beveiligingsobjecten

Bijlage 2: Use case Applicaties met integratiefuncties

In deze implementatie zijn alle applicaties van organisatie A voorzien van eigen integratiefuncties. De verschillende applicaties verzorgen vanuit de bedrijfsprocessen P, Q en R zelf het berichtenverkeer, zie afbeelding 6. Voordeel daarvan is de onafhankelijkheid van de platformen voor wat betreft performance en beschikbaarheid. Ook is er geen sprake van een 'single point of failure'-effect in een centraal platform. Nadelen zijn de dubbeling van het beheer, de beheersingskosten voor de instandhouding van meervoudige functies met hetzelfde doel en de extra kosten voor pentesten etc.

Een tweede belangrijk nadeel van deze opstelling is dat alles point-to-point met elkaar verbonden wordt. Als proces Q verhuist, dan moeten P en R meebewegen. Bij het gebruik van centraal opgestelde integratietechnologie hebben processen P en R geen notie van wat er met Q gebeurt.

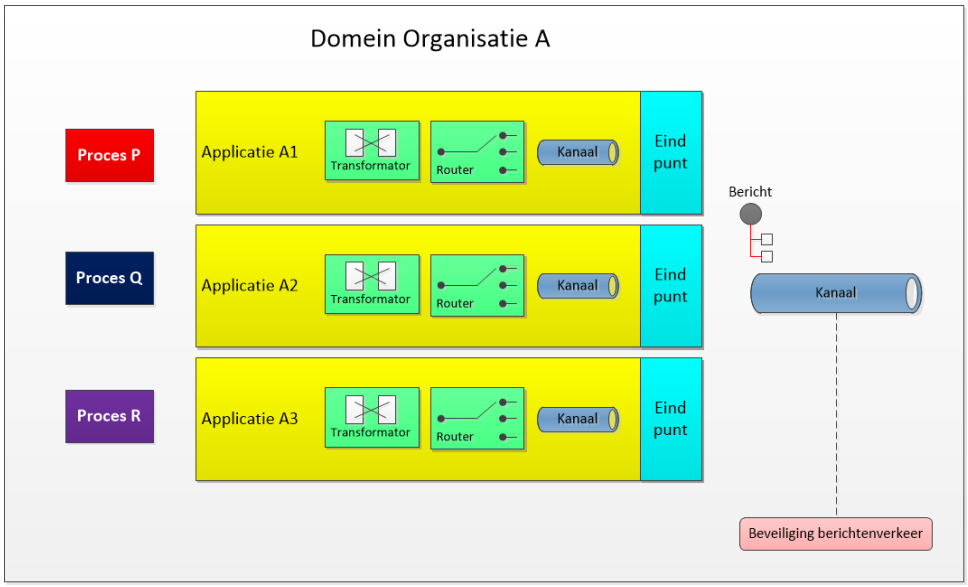
Kenmerken zijn:

- Koppeling met andere platformen is onderdeel van applicatieverantwoordelijkheid.
- Meervoudige toepassing van dezelfde functionaliteit.
- Geen specialisatievoordeel.

Beveiligingsobjecten

Omdat de integratiefuncties hier integraal onderdeel zijn van de applicatie zelf, blijven relevante beveiligingsobjecten voor deze implementatie beperkt tot de beveiliging van berichtenverkeer, wat afhankelijk van de classificatie van de data op verschillende manieren opgelost wordt; van een simpele SSL/TLS-koppeling tot een meer geavanceerde koppeling op basis van Message Level Security.

Applicatieontwikkelaars dienen over de benodigde specialistische kennis beschikken om deze maatregelen in te kunnen bouwen in hun applicaties.



Afbeelding 6: Applicaties met hun eigen integratiefuncties

Bijlage 3: Use case Gedelegeerde integratiefuncties

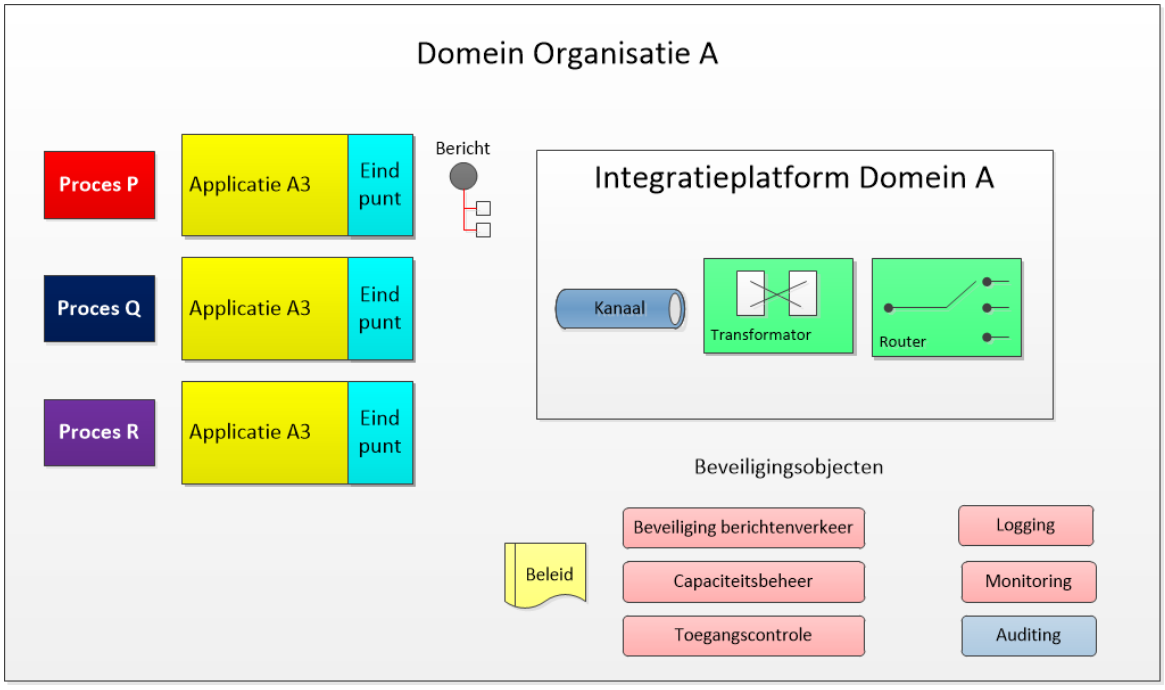
In deze implementatie 'delegeren' de applicaties van organisatie A de integratiefuncties aan een centraal integratieplatform. Het berichtenverkeer vanuit de bedrijfsprocessen P, Q en R wordt daarbij centraal door het integratieplatform domein A verzorgd, wat gespecialiseerde functies bevat waarmee een scala aan applicaties kunnen worden bediend.

Kenmerken zijn:

- Integratie is gedelegeerde applicatieverantwoordelijkheid.
- Meervoudig gebruik van enkelvoudige functionaliteit.
- Specialisatievoordeel.

Beveiligingsobjecten

Relevante objecten voor deze implementatie zijn dezelfde als die van use case 1, gericht op separate integratiefuncties van het integratieplatform. Ook de overige beveiligingsobjecten uit dit thema zijn van toepassing, maar zijn voor de omvang daarvan niet allemaal geschetst in afbeelding 7.



Afbeelding 7: Applicaties delegeren de integratiefunctie

Bijlage 4: Use case End-to-end applicatie-integratie

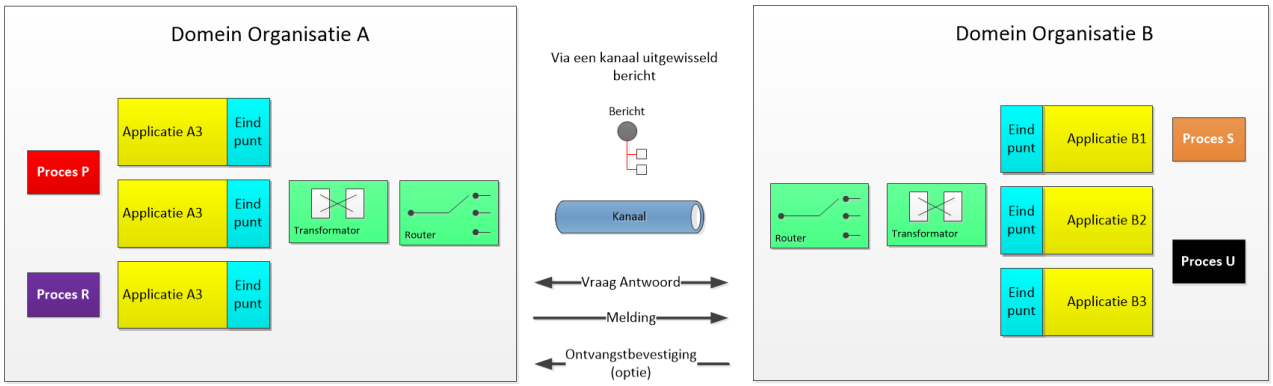
Deze implementatie is geschikt om een aantal bedrijfsprocessen van twee organisaties met elkaar te verbinden. Het betreft dezelfde opzet van de gedelegeerde integratiefuncties van use case 3, maar nu in de infrastructuur van beide organisaties uitgevoerd.

Kenmerken zijn:

- tweeweg-communicatie met gelijkwaardige functies;
- integratie is gedelegeerde applicatieverantwoordelijkheid;
- meervoudig gebruik van enkelvoudige functionaliteit;
- specialisatievoordeel.

Beveiligingsobjecten

Relevante objecten voor deze implementatie zijn dezelfde als die van use case 1 en use case 3, gericht op separate integratiefuncties van het integratieplatform.



Afbeelding 8: End-to-end-integratie met gedelegeerde integratiefuncties

Bijlage 5: Use case Enterprise Service Bus (ESB)

De Enterprise Service Bus is een Service Oriënted Architecture (SOA)-oplossing, die ontworpen is voor een breed scala aan integratiefuncties. De ESB wordt onder andere gebruikt wordt voor routering, berichttransformatie en protocol-bridging. Dit zijn overigens vergelijkbare integratiefuncties als die besproken zijn in use cases 1 tot en met 4, alleen nu niet bedoeld voor interactie tussen bedrijfsapplicaties, maar voor de interactie tussen applicatieservices.

Services, als onderdeel van SOA, zijn gespecialiseerde softwarecomponenten, bedoeld voor uitvoering van enkele bedrijfsfuncties, zoals informatie verzamelen, uitvoeren van specifieke bewerkingen etc.

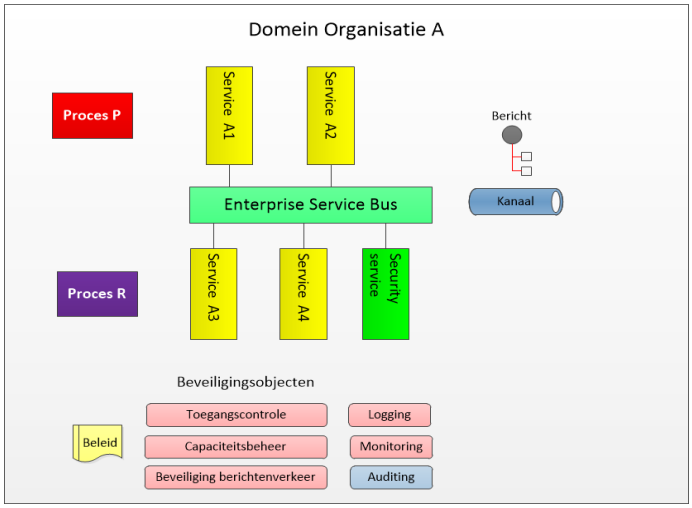
Een ESB is een middel voor service-to-service-communicatie. Met deze techniek hoeven services niet individueel gekoppeld te worden voor de communicatie, waardoor het aantal koppelingen drastisch wordt verminderd. De ESB biedt op basis van apart in te richten beveiligingsservices, tevens een aantal beveiligingsfuncties en protocollen voor berichtenverkeer, die gegarandeerd integere communicatie tussen de verschillende diensten mogelijk maken.

Kenmerken zijn:

- Tweewegcommunicatie met gelijkwaardige applicatie/servicefuncties.
- Applicatiefunctionaliteit is verdeeld over een aantal gespecialiseerde services.
- Integratie is gedelegeerde serviceverantwoordelijkheid van de bus.
- Meervoudig gebruik van enkelvoudige functionaliteit.
- Specialisatievoordeel.

Beveiligingsobjecten

SOA-services en een ESB bevatten zelf nauwelijks beveiligingsfuncties, hoewel de meeste ESB's wel TLS en MLS ondersteunen. De meeste beveiligingsfuncties worden door speciale securityservices geleverd. Voor de communicatie met grote informatiesystemen of partnerorganisaties worden integere berichtenprotocollen gebruikt. Voor de veilige communicatie met specifieke clients, zoals mobiele devices, desktop apparaten of webservices kunnen zogenaamde API-gateways op de bus worden aangesloten. De overige objecten uit dit thema zijn hier ook van toepassing.



Afbeelding 9: Enterprise Service Bus

Bijlage 6: Use case End-to-End integratie met API gateway

In de wereld, waarbij in toenemende mate functionaliteit wordt aangeboden via webservices voor allerlei verschillende clients (gebruikersapparaten) en de situatie, waarin delen van applicaties worden vervangen door zogenaamde microservices, spelen API's een steeds belangrijkere rol. De huidige uitwisseling van data via internet zou volgens het Akamai State of the Internet Security Report 2019, voor meer dan 80% via API's geregeld worden. De centrale vraag daarbij is: 'Hoe kunnen verschillende soorten clients toegang krijgen tot de functionaliteit die door de microservices (of applicaties) geleverd worden?'

Problematiek

De granulariteit van API's die door microservices geleverd wordt, wijkt vaak af van wat een bepaalde client nodig heeft. Microservices bieden doorgaans fijnmazige API's, wat betekent dat clients met meerdere services moeten communiceren. Als een lezer van een webpagina bijvoorbeeld de details van een product nodig heeft, dan deze moet zijn client-gegevens ophalen bij een reeks van services. Verder hebben verschillende clients voor dezelfde pagina verschillende gegevens nodig om pagina's goed weer te geven op een display. Een desktopversie van een productdetailpagina is bijvoorbeeld uitgebreider dan de mobiele versie. Verder verschillen de netwerkprestaties per client. Ook de netwerkprestaties kunnen per client sterk verschillen. Webapplicaties aan de serverzijde kunnen daardoor meer verzoeken doen aan backend-services zonder de gebruikerservaring te beïnvloeden dan een mobiele client.

Oplossing

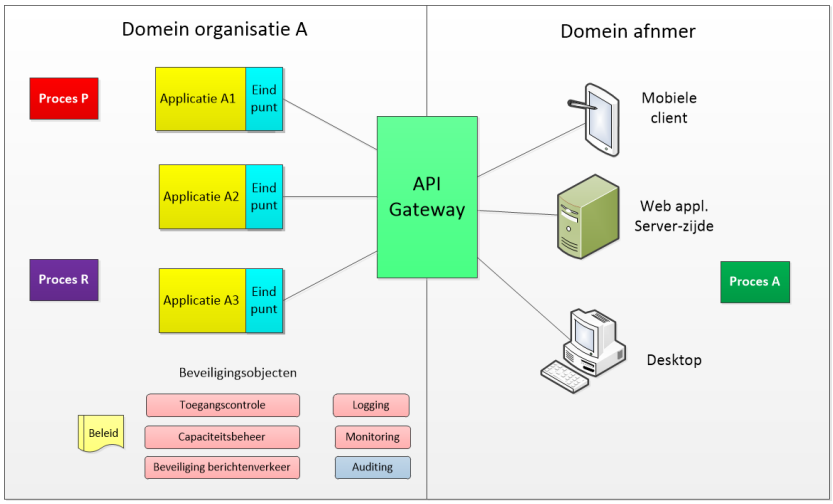
Implementeer een of meerdere API-gateway(s) die het enige toegangspunt vormen voor alle clients, zoals afbeelding 10 of één gateway per specifieke client. De API-gateway verwerkt verzoeken op twee manieren:

- Sommige verzoeken worden een-op-een gerouteerd naar de juiste service.
- De gateway behandelt andere verzoeken door deze uit te waaien naar meerdere achterliggende services.

Proces A maakt veilig gebruik van de geboden functionaliteit.

Kenmerken zijn:

- communicatie van gelijkwaardige functies in één richting: van applicatie/service naar de client;
- functionaliteit en performance van gateway afgestemd op de gemiddelde client.

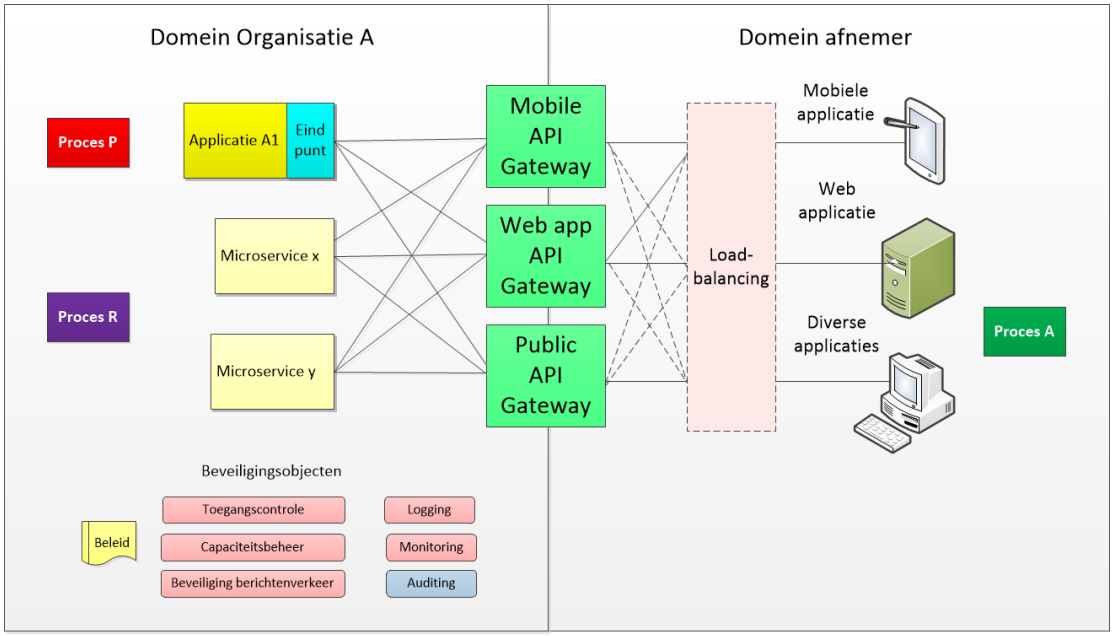


Afbeelding 5: Implementatie met één API gateway

Bijlage 7: Gespecialiseerde API gateway-toepassing

Om verschillende redenen kan het nodig zijn om meerdere API gateways in te zetten, bijvoorbeeld in verband met complexiteit, performance, latency of het single-point-of-failure-effect, waarbij één defecte gateway een heel bedrijfsproces plat kan leggen.

Afbeelding 11 geeft een voorbeeld van een implementatie, waarbij de API gateways zijn gespecialiseerd en geoptimaliseerd voor een bepaald type berichtenverkeer en voor een specifieke client. De gateways zijn in deze toepassing evenals in de enkelvoudige toepassing van afbeelding 11, op het grensvlak van intern naar extern van organisatie A gepositioneerd (in de DMZ). Om te voorkomen dat bij uitval een hele afnemerketen wordt uitgeschakeld, wordt load-balancing toegepast.



Afbeelding 11: Gespecialiseerde toepassing van API gateways met load-balancing

Beveiligingsobjecten

Relevante objecten voor de implementatie van API gateways, zowel voor de enkelvoudige als de gespecialiseerde toepassing, zijn globaal hetzelfde als de objecten gericht op separate integratiefuncties van het hiervoor besproken integratieplatform. Evenals het geval is voor een apart integratieplatform, kan een API-gateway zowel in soft- als in hardware of als clouddienst zijn uitgevoerd. Ook hierbij geldt dat dergelijke producten intrinsiek veilig moeten zijn ontworpen en in die hoedanigheid als module of als dienst worden geleverd aan organisaties.

NB: De in afbeelding 11 geschetste specialisatie is slechts een voorbeeld. In plaats van gespecialiseerde API-gateways kunnen gateways ook als cluster samenwerken om een hoge beschikbaarheid te garanderen. De overige objecten uit deze thema-uitwerking zijn ook in deze opstelling van toepassing.

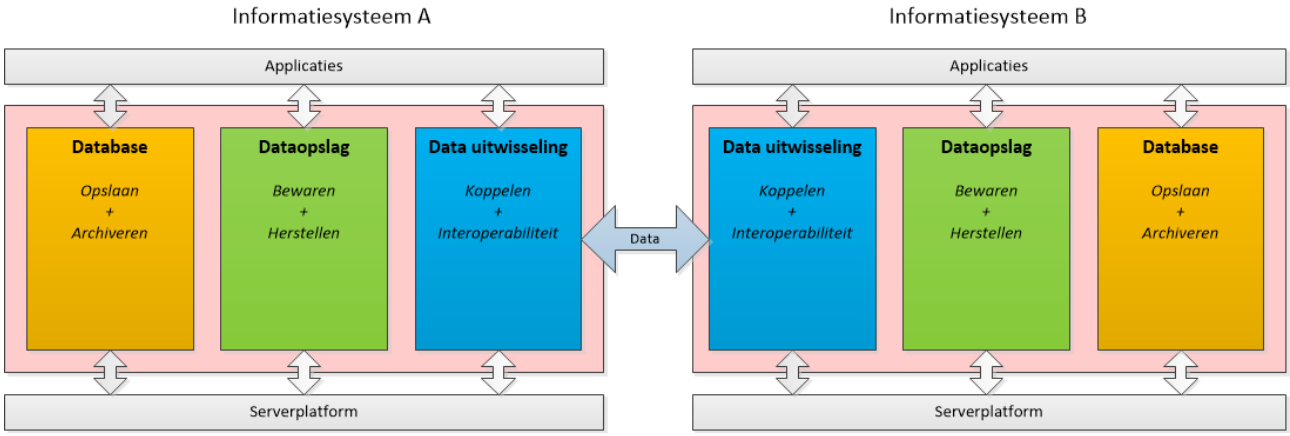
Kenmerken zijn:

- Communicatie van gelijkwaardige functies in één richting; van applicatie/service naar de client.
- Functionaliteit en performance afgestemd op het type client die de gateway bedient.

Bijlage 8: Context en systeemfuncties middleware

Context middleware

Elke organisatie heeft te maken met zijn eigen unieke omgeving (context). De ene organisatie werkt voornamelijk met uitbesteding van IT in clouddiensten, de andere heeft een eigen rekencentrum en ontwikkelt zelf de nodige maatregelen. Ondanks de verschillen in context blijven gebruikersorganisaties altijd eindverantwoordelijk voor wat er met hun data gebeurt en dus ook verantwoordelijk voor de eisen die gesteld worden aan de beveiliging van die data. In deze BIO Thema-uitwerking richten de eisen voor middleware (hierna controls genoemd) zich op een context, zoals die geschetst is in afbeelding 12.

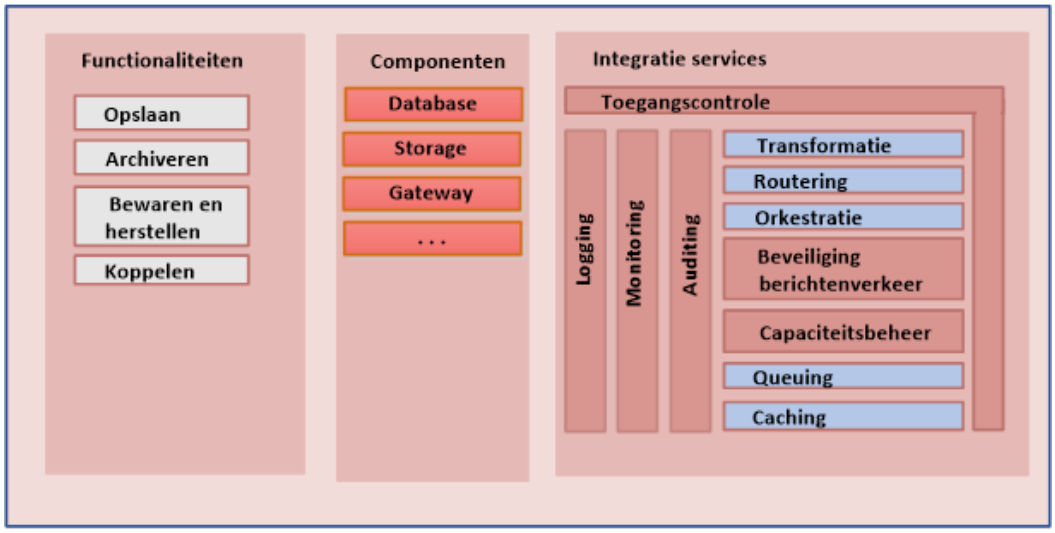


Afbeelding 12: Data-uitwisseling tussen informatiesystemen

Vanuit deze min of meer universele opzet voor middleware zijn relevante controls en maatregelen uit de BIO en andere best practices te duiden, zie hoofdstukken 3, 4 en 5 van dit document. In de geschetste opzet uit afbeelding 5 vindt naast een uitwisseling van data tussen applicaties en serverplatform, tevens uitwisseling van data plaats via berichtenverkeer tussen onderling gekoppelde informatiesystemen.

Systeemfuncties van middleware

Middleware bestaat grotendeels (en soms geheel) uit software. Voor de interne systeemfuncties van middleware, zoals aangegeven in de blauwe vlakken van afbeelding 13, gelden de beveiligingseisen die horen bij softwareontwikkelprocessen. Zie daarvoor de BIO Thema-uitwerking Applicatieontwikkeling en de OWASP-literatuur (Open Web Application Security Project) op internet. In deze BIO Thema-uitwerking zijn objecten uitgewerkt voor de functionaliteiten (links) en de integratieservices (rechts) uit afbeelding 13.



Afbeelding 13: Interne systeemfuncties van middleware