Architectuurkader Informatiebeveiliging en Overdraagbaarheid

inclusief kaders voor toegang, beheer en continuïteit

Inhoud

Begrippen

SAML (Security Assertion Markup Language)	Een standaard voor het uitwisselen van authenticatie- en autorisatiegegevens tussen partijen (meestal voor Single Sign-On).
OIDC (OpenID Connect)	Een moderne identiteitslaag boven op het OAuth 2.0-protocol waarmee applicaties de identiteit van gebruikers kunnen verifiëren.
SCIM (System for Cross-domain Identity Management)	Een standaard voor het automatiseren van de uitwisseling van gebruikersidentiteitsgegevens tussen verschillende systemen (**provisioning**).
CEF (Common Event Format)	Een open logformaat ontwikkeld door HP ArcSight, specifiek ontworpen om de interoperabiliteit van beveiligingsgerelateerde data te verbeteren.

Hoofdstuk 1 - Inleiding, doel en gebruik

1.1 Organisatie en context

Organisatiestructuur. De organisatie bestaat uit twee samenwerkende entiteiten - Bibliotheek Zuid-Kennemerland (BZK) en Cpunt - onder één stichting, met circa 400 medewerkers verdeeld over 17 publiek toegankelijke locaties. BZK richt zich primair op bibliotheekdienstverlening. Cpunt combineert bibliotheekdienstverlening met een Kunstencentrum, Theater, Café en Poppodium, wat resulteert in een breed scala aan apparatuur en applicaties: van grafische designwerkplekken en 3D-printers tot kassasystemen en ticketing-infrastructuur. Bij beide entiteiten gebruiken publiek en frontoffice-medewerkers dezelfde fysieke ruimten. Kantoorpersoneel werkt hybride en mobiel tussen locaties; frontoffice-medewerkers werken op gedeelde balie-PC's; publiek gebruikt dedicated apparatuur waarvan het beheer bij andere/derde leveranciers ligt.
ICT-landschap. De omgeving is hybride: centraal identity management, centraal platform, SaaS-applicaties en lokale infrastructuurcomponenten. Het applicatielandschap omvat cloud-native diensten en applicaties met lokale afhankelijkheden. Het beheer is verdeeld over meerdere domeinen: infrastructuur, werkplekbeheer en IAM worden uitgevoerd door een Managed Service Provider; operationele technologie (gebouwbeheer, toegangscontrole) door gespecialiseerde leveranciers; domeinspecifieke systemen (publieke apparatuur, uitleensystemen, kassasystemen, ticketing, creatieve productieapparatuur) door functionele leveranciers. Sommige systemen hebben hybride architecturen met zowel lokale componenten als cloudcomponenten bij de leverancier. Leveranciers hebben remote en/of fysieke toegang nodig. De rolverdeling tussen "beheer uitvoeren" en "architectuur bepalen" is niet altijd vastgelegd; toegangsrechten zijn soms breder dan functioneel noodzakelijk.
Context en drivers. De kleinschaligheid van beide organisaties betekent dat de interne capaciteit voor IT-governance beperkt is. De architectuur moet daarom overdraagbaar zijn en niet afhankelijk van impliciete kennis. Er is bewust gekozen om governance en regie structureel op orde te brengen; verdere uniformering tussen de entiteiten wordt hiermee niet afgedwongen. NIS2-wetgeving en BIO (vrijwillig toegepast) vereisen aantoonbare grip op toegangsbeveiliging, logging en incident response. De verwerking van privacygevoelige gegevens - van klanten, leden, bezoekers, vrijwilligers en personeel - versterkt deze noodzaak. Geopolitieke ontwikkelingen maken exit-by-design relevant: afhankelijkheid van specifieke leveranciers mag geen blokkade vormen voor verandering.

1.2 Doel van dit architectuurkader

Het doel is het vastleggen van een consistent en overdraagbaar kader voor toegang, scheiding, communicatie, beheer en continuïteit. Het architectuurkader biedt richting voor interne besluitvorming, maakt keuzes en afhankelijkheden expliciet, ondersteunt bestuurbaarheid bij verandering en borgt overdraagbaarheid bij wisseling van mensen en partijen. Het richt zich op samenhang en randvoorwaarden, niet op concrete oplossingen of productspecificaties.
Doelbeeld. Een beheerbare en veilige keten waarin toegang wordt bepaald door identiteit, context en apparaatstatus - niet door netwerkpositie. Netwerk- en securitycomponenten begrenzen communicatiepaden en realiseren scheiding; applicaties en data zijn leidend voor autorisatie. De inrichting is overdraagbaar via koppelvlakeisen, logging, herstelbaarheid en een expliciet uitzonderingenproces.

1.3 Scope en afbakening

Dit architectuurkader beschrijft principes en kaders voor identiteit en toegang, device- en clienttypologie, netwerk, scheiding en communicatie, beheer, toezicht en overdraagbaarheid, en continuïteit, backup en herstel. Andere architectuurdomeinen - bedrijfsarchitectuur, informatie- en data-architectuur, applicatie-architectuur en integratie-architectuur - vallen buiten scope en worden waar nodig uitgewerkt in aanvullende documenten. Informatie-architectuur valt als discipline buiten scope; minimale data-eisen voor beveiliging, overdraagbaarheid en data-zeggenschap zijn wél in scope: exporteerbaarheid, audit-/reconstructiemogelijkheden en het vermijden van architectonische data-lock-in. Applicaties en ketens worden uitsluitend beoordeeld op beveiligings- en overdraagbaarheidsaspecten: interfaces, identiteit-integratie, logging/audit, export en herstelbaarheid.

1.4 Gebruik, normatieve status en proportionaliteit

Dit architectuurkader wordt binnen de organisatie gebruikt als referentiekader om samenhang tussen keuzes te bewaken, afwijkingen vast te leggen, risico's en afhankelijkheden inzichtelijk te maken en besluitvorming overdraagbaar te houden. De architectuurprincipes en definities zijn hierbij leidend.
Het kader schrijft geen specifieke oplossingen, producten of configuraties voor, verplicht niet tot onmiddellijke aanpassing van bestaande inrichtingen en fungeert niet als uitvoerings- of projectplan. Afwijkingen zijn toegestaan, mits vooraf door beide partijen vastgelegd (zie paragraaf 9.2).
Proportionaliteit. De organisatie is kleinschalig in governance-capaciteit. Dit kader wordt toegepast volgens het principe "zo licht als kan, zo zwaar als nodig": alleen kritieke ketens, rollen en flows worden volledig uitgewerkt; de rest volgt via een standaard set koppelvlakeisen en een uitzonderingenregister met herijkmoment. Dit voorkomt over-structurering, maar maakt afwijkingen wel bestuurbaar en overdraagbaar.

1.5 Levensduur en herijking

Het architectuurkader is ontworpen voor een meerjarige levensduur van 7+ jaar. Herijking vindt plaats wanneer structurele afwijkingen ontstaan, risico's wijzigen of de context wezenlijk verandert. Herijking betreft het expliciteren of aanpassen van principes en randvoorwaarden, niet het automatisch herontwerpen van de architectuur.

1.6 Samenhang van het architectuurkader

Toegangsmodel in hoofdlijnen. Toegang ontstaat in samenhang met identiteit, context en posture - niet op basis van netwerkpositie. Toegang geldt voor een concrete applicatie of functionaliteit, ongeacht of die on-premise, hybride of SaaS is.
Device-typologie als randvoorwaarde. Devices worden getypeerd naar geschiktheid voor handelingen (Hoofdstuk 5). De categorie bepaalt randvoorwaarden en beperkingen, niet autorisatie. De combinatie van identiteit, context én posture bepaalt welke toegang verantwoord is.
Netwerk als middel voor impactbeperking. Het netwerk is ontworpen om gevolgen van fouten lokaal te houden. Segmentatie begrenst communicatiepaden en minimaliseert laterale beïnvloeding en fungeert niet als autorisatiemodel. Uitgaande communicatie wordt bewust ontworpen om afhankelijkheden zichtbaar en beheersbaar te maken.
SaaS en verschuivende handhaving. Bij SaaS-diensten verschuift handhaving deels naar leveranciers, maar de verantwoordelijkheid voor toegang, toezicht en herstelbaarheid blijft bij de organisatie. Koppelvlakspecificaties zijn daarom randvoorwaardelijk: eisen aan identiteit-integratie, logging/audit, exportmogelijkheden en herstelprocedures worden contractueel geborgd.
Beheer, toezicht en overdraagbaarheid. Beheerhandelingen worden ingericht via beheerpaden met geschikte context, minimale privileges en traceerbaarheid. Zonder inzicht in wijzigingen, gebeurtenissen en afwijkingen is de omgeving niet bestuurbaar. Overdraagbaarheid vereist dat keuzes, uitzonderingen en afhankelijkheden zodanig zijn vastgelegd dat nieuwe partijen de samenhang kunnen begrijpen en voortzetten. Dit is een randvoorwaarde voor exit by design.

Hoofdstuk 2 - Begrippen en definities

2.1 Doel en gebruik

Dit hoofdstuk legt vast wat kernbegrippen binnen dit architectuurkader betekenen. De definities zijn normerend voor ontwerp, beoordeling en beheer. Waar termen in de praktijk of markt meerdere betekenissen hebben, geldt binnen deze context uitsluitend de hier vastgelegde betekenis. Ze ondersteunen consistente besluitvorming, explicitering van afwijkingen en overdraagbaarheid bij wisseling van rollen, personen of leveranciers.
De begrippen zijn onderverdeeld in vier thematische groepen die de structuur van het architectuurkader weerspiegelen.

2.2 Vertrouwen, toegang en identiteit

Vertrouwen: Tijdelijke toestemming om een specifieke handeling uit te voeren onder specifieke omstandigheden. Vertrouwen is geen permanente status en geen eigenschap van locatie of netwerk.
Toegang: Het expliciet toestaan van een concrete interactie met een applicatie, dienst of functionaliteit. Toegang is begrensd in scope en tijd.
Autorisatie: Het bepalen van wat binnen de toegestane interactie is toegestaan. Autorisatie ligt primair bij de applicatie of dienst; het netwerk is ondersteunend en begrenzend, niet leidend.
Identiteit: Het vastgestelde subject - menselijk of niet-menselijk - dat een handeling initieert. Identiteit is startpunt van een toegangsafweging, niet het volledige besluit.
Context: De omstandigheden waaronder toegang wordt gevraagd, zoals type device, beheerstatus, locatie, tijdstip, risicoprofiel en gevoeligheid van de handeling.
Posture: De vastgestelde staat van een device op het moment van toegang: beheerd of niet-beheerd, basisveiligheid, compliance-status. Posture is een signaal voor geschiktheid, geen garantie.
Lifecycle-geschiktheid: De mate waarin een component gedurende de levensduur ondersteund, beheerbaar en veilig te houden is. Hoe lager de lifecycle-geschiktheid (bijv. beperkt patchbaar of end-of-support), hoe strikter de toegangsvoorwaarden, hoe smaller de toegestane communicatiepaden en hoe zwaarder het toezicht.
Autorisatiematrix: Vastlegging van rollen/identiteiten naar functionaliteiten: wie mag wat in applicaties.

2.3 Devices en communicatie

Device categorie: Een architectonische typering van devices met een eigen risicoprofiel en geschiktheid voor handelingen. De categorie bepaalt randvoorwaarden en beperkingen, niet autorisatie.
Publieke client: Een device in een openbare ruimte of buiten beheer dat blootstaat aan fysiek en logisch misbruik. Publieke clients zijn per definitie niet vertrouwd en krijgen uitsluitend strikt noodzakelijke, functiegerichte toegang.
Gedeeld apparaat: Een device dat door meerdere gebruikers - intern en/of extern - wordt gebruikt en waarvoor authenticatie en gebruiksdoel wisselen. Dit is een eigen categorie met begrensde toegang.
OT/IoT-systeem: Een apparaat of systeem dat grotendeels autonoom handelt, primair via communicatiepaden met diensten of applicaties, vaak met beperkte beheermogelijkheden. Update- en patchbaarheid is een expliciet ontwerpcriterium: per type device wordt vastgelegd hoe firmware/software-updates plaatsvinden, wie eigenaar is, hoe kwetsbaarheden worden opgevolgd en wat het compensatiemodel is als patching niet tijdig kan.
Leverancierssysteem: Een device of voorziening van een externe partij dat fysiek of logisch in de omgeving aanwezig is of ermee koppelt. Leverancierssystemen blijven buiten het interne vertrouwensdomein; paden zijn vastgelegd en begrensd.
Scheiding / segmentatie: Logische afbakening van systemen en domeinen om impact te beperken. Segmentatie is geen autorisatiemodel, maar een middel om fouten lokaal te houden en laterale beïnvloeding te voorkomen.
Laterale beïnvloeding: Ongewenste verspreiding van fouten of misbruik van het ene systeem naar andere systemen. In deze architectuur wordt dit beschouwd als een ontwerpfout, niet als een incident dat men achteraf oplost.
Communicatiepad: Een ontworpen, vastgelegd en toegestane route waarlangs systemen met elkaar communiceren. Elk pad is herleidbaar tot een functionele noodzaak.

Traffic matrix (communicatiematrix): Vastlegging van bron (domein/systeem) naar doel (dienst) met protocol/poort, logging-eis en eigenaar: welke paden bestaan en waarom.
Uitgaande communicatie: Communicatie van systemen naar externe diensten of domeinen. Uitgaande communicatie is ontworpen en begrensd om afhankelijkheden zichtbaar en beheersbaar te maken.

2.4 Beheer, toezicht en overdraagbaarheid

Toezicht: Het structureel kunnen verkrijgen van inzicht in relevante gebeurtenissen, wijzigingen en afwijkingen (logging/audit), inclusief bewaarperiode en beschikbaarheid voor audit, zodat beheer en risico's bestuurbaar zijn - ook bij uitbesteding en SaaS.
Beheerpad: Het expliciet ingerichte en afgedwongen pad waarlangs beheerhandelingen plaatsvinden, onder geschikte context, met traceerbaarheid en minimale privileges.
Koppelvlakspecificaties: Een vastgelegde ontwerpafspraak over hoe componenten samenwerken, onafhankelijk van leverancier of implementatie. Omvat minimaal: identiteit/claims, interfaces, logging/audit, data-export en configuratie-overdraagbaarheid.
Exit by design: Het architectuurprincipe dat vervanging van componenten of leveranciers mogelijk moet zijn zonder fundamenteel herontwerp van het toegangs- en scheidingsmodel.

2.5 Gegevens, portabiliteit en compliance

Gegevensgevoelige dienst: Een cloud- of SaaS-dienst waarop de architectuurprincipes 9 en 10 van toepassing zijn op basis van de verwerkte data - waaronder persoonsgegevens en logs - ongeacht de hoofdfunctie van de dienst.
Data-eigenaarschap: Het recht om te bepalen wat er met data gebeurt (toegang, verwijdering, export, locatie) en de zekerheid dat data bij contractbeëindiging volledig en in bruikbaar formaat wordt overgedragen. Data-eigenaarschap is een architectuurcriterium bij leverancierselectie.
Architectonische data-lock-in: Technische staat van data of configuraties met proprietary formaten, interfaces of diensten die een overstap (principe 10) belemmert zonder fundamenteel herontwerp.
Jurisdictierisico: Het risico dat een buitenlandse overheid toegang kan afdwingen tot data, authenticatie-informatie, logs of audit-trails op basis van eigen wetgeving - ongeacht fysieke opslaglocatie, contractuele afspraken of primaire functie van de dienst. Jurisdictierisico wordt bepaald door de rechtsvorm en vestigingsplaats van de leverancier en diens sub-verwerkers.

Hoofdstuk 3 - Architectuurprincipes

De twaalf principes zijn gegroepeerd in vier thema's die de samenhang van het model weerspiegelen.

Thema	Principes
Toegang en vertrouwen	1 t/m 5
Beperking van impact	6 t/m 8
Afhankelijkheden en verandering	9 en 10
Bestuurbaarheid en overdraagbaarheid	11 en 12

3.1 Toegang en vertrouwen (principes 1–5)

Principe 1: ***Toegang is gebaseerd op vooraf vastgestelde voorwaarden, niet op netwerkpositie***
Historisch werd "binnen het netwerk" gebruikt als proxy voor vertrouwen. In het doelbeeld mag netwerkpositie nooit zelfstandig leiden tot extra rechten of bredere toegang. Het netwerk is een transport- en scheidingslaag, geen autorisatielaag.
Principe 2: ***Toegang is gericht op functionaliteit, niet op infrastructuur***
Toegang wordt verleend tot een concrete functionaliteit - applicatie, dienst of handeling - en nooit als generieke netwerktoegang "voor de zekerheid". Rechten zijn herleidbaar tot een functionele noodzaak.
Principe 3: ***Vertrouwen is tijdelijk en contextafhankelijk***
Toegang wordt beoordeeld in samenhang met identiteit, context en device-kenmerken. Vertrouwen is geen permanente status maar een tijdelijke toestemming die kan worden beperkt of ingetrokken als omstandigheden wijzigen.
Principe 4: ***Publieke en onbeheerde systemen krijgen beperkte privileges***
Publiek toegankelijke systemen en onbeheerde clients krijgen geen impliciete rechten; zij krijgen uitsluitend strikt noodzakelijke, functiegerichte toegang en blijven logisch gescheiden van kernprocessen. "Onbeheerd" omvat bijvoorbeeld ook activiteitenlaptops of tijdelijke devices die niet volledig aan beheer- en patch-eisen voldoen: zij worden behandeld als risicodomein. Waar toch functionaliteit nodig is, worden expliciete beperkingen toegepast - zoals alleen browser-toegang, alleen specifieke SaaS-applicaties, geen laterale paden, kortlopende sessies of een beheerde tussenlaag zoals VDI/RDP.
Principe 5: ***Device-posture is beoordelingscriterium, geen beslissingsbasis***
Device-kenmerken (beheerstatus, compliance, patching) zijn relevante signalen bij toegangsbeoordeling, maar vervangen identiteitsverificatie en autorisatie niet. Een "vertrouwd device" is een randvoorwaarde voor bepaalde handelingen, geen toegangsbewijs. Device-posture wordt beoordeeld samen met identiteit en context; de combinatie bepaalt welke handelingen verantwoord zijn.

3.2 Beperking van impact (principes 6–8)

Principe 6: ***Impactbeperking is leidend: fouten moeten lokaal blijven***
De architectuur is primair ontworpen om gevolgen van fouten, misbruik of verstoringen te begrenzen. Scheiding, minimale communicatiepaden en het voorkomen van ongewenste laterale beïnvloeding zijn ontwerpeisen, geen incidentmaatregelen.
Principe 7: ***Communicatie tussen domeinen is expliciet en herleidbaar***
Systemen communiceren alleen via expliciet ontworpen paden die herleidbaar zijn tot een functionele noodzaak. Het ontwerpuitgangspunt is default-deny tussen domeinen, met een allowlist van communicatiepaden. Per pad worden vastgelegd: bron, doel, protocol/poort, functionele reden, eigenaar en logging-eis. Als een pad niet is ontworpen, bestaat het niet. "Het werkte al zo" of "dit is handig" is geen functionele noodzaak.

Principe 8: ***Uitgaande communicatie is net zo belangrijk als inkomende***

Niet alleen inkomend, maar ook uitgaand verkeer wordt bewust ontworpen. Uitgaand verkeer omvat ook update- en beheerkanalen (firmware/agent-updates, tijdsynchronisatie, certificaatcontroles, remote beheer). Per domein en device categorie wordt vastgelegd welke bestemmingen en protocollen noodzakelijk zijn, met logging en eigenaarschap. Dit voorkomt dat "updates moeten kunnen" leidt tot generieke internettoegang. Wanneer updatekanalen niet beheersbaar zijn, wordt dit behandeld als lagere posture en volgen compenserende maatregelen via strengere scheiding, minimale paden en verhoogd toezicht. Het ontwerp van uitgaande communicatie dient drie doelen: afhankelijkheden zichtbaar maken, misbruik en datalekken beperken, en afwijkingen detecteerbaar maken.

3.3 Afhankelijkheden en verandering (principes 9–10)

Principe 9: ***Leveranciersafhankelijkheden zijn expliciet, omkeerbaar en juridisch beoordeeld***
Afhankelijkheid van leveranciers en SaaS-diensten is toegestaan, mits expliciet geborgd. Dit principe is van toepassing op elke gegevensgevoelige dienst - zoals SSO, e-mail, bestandsopslag, samenwerkingstooling en backupdiensten. De aard van de verwerkte data is leidend, niet het type product.
Documentatie en koppelvlakspecificaties. Voor elke gegevensgevoelige dienst worden vastgelegd: de functie, het risico, de dataclassificatie en beschikbare alternatieven. De koppelvlakspecificaties omvatten minimaal: wie toegang heeft tot de data (inclusief de leverancier zelf en sub-processors); welke audit trails van datatoegang beschikbaar zijn, inclusief bewaarperiode en exporteerbaarheid; welke exportformaten, procedures en tijdlijnen gelden bij exit; en wie eigenaar is van backups en hoe restore-procedures zijn ingericht.
Jurisdictierisico. Per gegevensgevoelige dienst wordt beoordeeld in welke mate buitenlandse wetgeving toegang tot data kan afdwingen via de (sub)leverancier. De beoordeling wordt getoetst aan AVG artikel 44–49 en NIS2, gericht op de rechtsvorm van de leverancier. Bij gelijkwaardige alternatieven geniet een leverancier onder Europese jurisdictie met data-opslag in Nederland of de EU de voorkeur.
Voorkomen van architectonische data-lock-in. Voor kritieke functies (identity management, data-opslag, audit-logging) is een exit-strategie vereist. Concreet betekent dit: gebruik van open standaarden voor authenticatie (SAML, OIDC) en provisioning (SCIM); standaard exportformaten voor data-opslag; exporteerbare logs in gangbare formaten (Syslog, CEF); en overdraagbare toegangsregels en policies. Een migratie naar een alternatief moet uitvoerbaar zijn zonder fundamenteel herontwerp van de toegangsarchitectuur of dataverlies.
Principe 10: ***Exit by Design: vervanging zonder fundamenteel herontwerp***
De architectuur maakt vervanging van componenten en leveranciers mogelijk zonder dat het onderliggende toegangs- en scheidingsmodel opnieuw moet worden ontworpen. Dit vereist dat architectonische data-lock-in tot een minimum wordt beperkt door data-eigenaarschap in de ontwerpfase te borgen. Het resultaat is een overdraagbaar stelsel van identiteiten, interfaces, logging/audit, data-export en configuraties, waardoor een migratie naar een alternatieve leverancier technisch en juridisch uitvoerbaar blijft.

3.4 Bestuurbaarheid en overdraagbaarheid (principes 11–12)

Principe 11: ***Beheer is een apart architectuurdomein met eigen paden en toezicht***
Beheerhandelingen worden bewust ingericht, afgebakend en controleerbaar gemaakt. Beheer vindt plaats via herkenbare paden onder geschikte context, met traceerbaarheid en minimale privileges. Uitbesteding verandert niets aan deze eis.
Principe 12: ***Overdraagbaarheid: samenhang moet blijven bestaan bij wisseling van mens en leverancier***
Architectuurkeuzes, definities, uitzonderingen en afhankelijkheden worden zodanig vastgelegd dat een volgende beheerpartij of architect de samenhang kan begrijpen en voortzetten. Dit principe ondersteunt continuïteit en is een randvoorwaarde voor exit by design.

Hoofdstuk 4 - Identiteit en toegang

4.1 Rol van identiteit

Identiteit is het startpunt van elke toegangsafweging. Het stelt vast wie of wat een handeling initieert, onafhankelijk van netwerkpositie (principe 1). Identiteit is noodzakelijk, maar nooit voldoende.

4.2 Context en posture

Toegang wordt toegekend op basis van identiteit in samenhang met context en posture (principe 3). Hierdoor kan toegang proportioneel worden toegekend en kunnen risicovolle handelingen worden beperkt tot geschikte situaties.
Meervoudige verificatie. Identiteitsvaststelling voor handelingen met verhoogde impact vereist meervoudige verificatie: minimaal twee onafhankelijke factoren, waarvan ten minste één gebaseerd is op bezit of inherentie. Deze eis geldt ongeacht de locatie van de gebruiker of het gebruikte device, en is van toepassing op alle menselijke identiteiten. Welke handelingen als 'verhoogde impact' worden aangemerkt, wordt bepaald in de autorisatiematrix; beheerhandelingen, toegang tot gegevensgevoelige diensten en wijzigingen in toegangsbeleid vallen hier in elk geval onder.

4.3 Toegang eindigt bij applicaties en functionaliteit

Toegang wordt altijd verleend tot een applicatie of concrete functionaliteit, nooit tot infrastructuur of generieke netwerksegmenten. Applicaties bepalen autorisatie; het netwerk begrenst paden; identiteit en context bepalen of toegang überhaupt mogelijk is.

4.4 Menselijke en niet-menselijke identiteiten

De architectuur onderscheidt menselijke identiteiten (medewerkers, beheerders) en niet-menselijke identiteiten (services, devices, integraties). Niet-menselijke identiteiten krijgen uitsluitend de minimaal noodzakelijke rechten en worden ontworpen rond vastgelegde communicatiepaden. Service-identiteiten (certificaten, API-clients, integratieaccounts) zijn traceerbaar, minimaal geprivilegieerd en vallen onder dezelfde log- en beheerafspraken.

4.5 Versleuteling van communicatie

Communicatie over niet-vertrouwde netwerken - waaronder internet, publieke wifi en externe koppelingen met leveranciers - is versleuteld. De versleuteling voldoet aantoonbaar aan actuele normen zoals vastgesteld door een erkend nationaal of Europees referentiekader. Verouderde of kwetsbaar bevonden mechanismen zijn niet toegestaan; wat als kwetsbaar geldt, volgt uit het geldende referentiekader op het moment van beoordeling - niet uit deze tekst. Zo blijft de eis functioneel geldig ongeacht toekomstige technologische ontwikkelingen. Koppelvlakspecificaties bevatten een expliciete verwijzing naar het gehanteerde referentiekader en het moment van beoordeling.

Hoofdstuk 5 - Device- en clienttypologie

5.1 Doel

Device-typologie maakt zichtbaar welke categorieën devices bestaan, welke geschiktheid zij hebben voor handelingen en welke beperkingen gelden. De typologie voorkomt impliciet vertrouwen en zorgt dat het toegangsmodel consequent toepasbaar is. Grijze gevallen - devices die kenmerken van meerdere categorieën combineren - worden expliciet geprofileerd en niet weggedefinieerd.

5.2 Categorieën

Dit kader hanteert minimaal de volgende categorieën: beheerde werkplek, publieke internet-client, gedeeld apparaat, OT/IoT-systeem en leverancierssysteem. Sommige devices hebben meerdere kenmerken: internet- en catalogusdevices zijn voor publiek toegankelijk maar technisch beheerd en logisch geïsoleerd van interne systemen; er zijn geen laterale paden naar andere domeinen; lokale sessiedata wordt periodiek automatisch gewist en kan door de gebruiker zelf worden gereset; multifunctionalprinters kunnen bij de ene entiteit gedeeld zijn tussen medewerkers en publiek, terwijl ze bij de andere entiteit per groep dedicated zijn. Deze nuances worden per categorie geprofileerd in paragraaf 5.3.

5.3 Architectuureisen per categorie

Per categorie wordt beschreven welke geschiktheid geldt, welke toegang verantwoord is en welke beperkingen noodzakelijk zijn. De eisen gelden onafhankelijk van specifieke producten of leveranciers. Afwijkingen worden vastgelegd conform paragraaf 9.2.

Lifecycle als posture-factor

Naast beheerstatus (managed/unmanaged) krijgt elke device categorie een lifecycle-profiel: goed patchbaar / beperkt patchbaar / niet patchbaar (inclusief end-of-support). Dit profiel bepaalt niet óf toegang mogelijk is, maar onder welke voorwaarden. Beperkt of niet patchbaar leidt standaard tot strengere scheiding, minimale communicatie via een allowlist, geen laterale paden, beperking van beheerrechten en verhoogd toezicht op afwijkend gedrag. Lifecycle-geschiktheid is daarmee een ontwerpcriterium binnen toegang en beveiliging, geen puur beheeronderwerp.

Beheerde werkplekken (kantoorpersoneel)

Beheerde laptops van kantoorpersoneel hebben de hoogste geschiktheid voor handelingen met verhoogde impact. Ze bieden toegang tot de volledige bedrijfsapplicaties en ondersteunen hybride werk. Architectuureis: device-posture op compliance, patching en encryptie.

Gedeelde apparatuur - multifunctionalprinters

Bij de ene entiteit gedeeld tussen medewerkers en publiek, bij de andere dedicated per groep. Toegang is beperkt tot printfunctionaliteit met gebruikersauthenticatie. Architectuureis: herleidbaarheid per print-job naar gebruiker of account, met segmentatie naar alleen printservices en geen andere interne systemen.

Gedeelde apparatuur - balie-PC's (frontoffice)

Gedeeld tussen frontoffice-medewerkers. Toegang is beperkt tot functie specifieke applicaties (frontoffice); toegang tot HR-, financiële of beheersystemen is uitgesloten. Architectuureis: herleidbaarheid van handelingen naar persoon en geen laterale beweging naar andere domeinen. Waar volledige herleidbaarheid technisch of organisatorisch niet haalbaar is, worden compenserende maatregelen getroffen (zie paragraaf 8.3 en 9.2).

Beheerde devices voor publieke internet (bijvoorbeeld internet-catalogus PC's)

Devices in deze categorie zijn publiek toegankelijk maar technisch beheerd. De gebruikersomgeving is begrensd tot de beoogde functie (internettoegang, catalogus); er zijn geen laterale paden naar interne systemen buiten de publiekszone. Lokale sessiedata -waaronder browsergeschiedenis, cookies en cachebestanden -wordt na een configureerbare periode van inactiviteit automatisch gewist; de gebruiker kan dit ook zelf initiëren. Hoe sessie-isolatie en het wissen technisch worden gerealiseerd is een implementatiekeuze, mits aantoonbaar gerealiseerd. Koppelvlakspecificaties zijn verplicht, inclusief logging van beheerhandelingen, de gehanteerde isolatiemaatregel en de lifecycle-status van het gekozen model.

Publiek beheerde devices - uitleenapparatuur

Beheerd door leveranciers, met toegang uitsluitend tot de uitleenapplicatie. Koppelvlakspecificaties zijn verplicht inclusief logging van beheerhandelingen. Segmentatie in een apart domein.

OT/IoT - **gebouwbeheer, toegangscontrole, narrowcasting**

Architecturen variëren van volledig on-premise tot hybride (lokaal plus cloud bij leverancier) tot volledig cloud. Update- en patchbaarheid is een expliciet ontwerpcriterium (zie definitie paragraaf 3.2). Beheer door externe leveranciers vindt plaats in een apart domein per dienst met logging. Er zijn geen ongecontroleerde internetpaden; hybride systemen communiceren uitsluitend naar het eigen cloud-component. Geen laterale beweging naar andere domeinen.

Leverancierstoegang - **MSP en OT-leveranciers**

Leveranciers blijven buiten het interne vertrouwensdomein en hebben toegang uitsluitend via PAM en een gesegmenteerd beheerpad (principe 11). Koppelvlakspecificaties met exit-afspraken zijn verplicht.

Hoofdstuk 6 - Netwerk, scheiding en communicatie

6.1 Rol van netwerk

Het netwerk realiseert bereikbaarheid, scheiding en beheersbaarheid (principe 6). Het is nadrukkelijk geen mechanisme om vertrouwen toe te kennen (principe 1). Netwerkpositie heeft geen zelfstandige betekenis voor autorisatie.

6.2 Scheiding en segmentatie

Scheiding wordt toegepast op basis van domeinen met verschillende risicoprofielen en verantwoordelijkheden: beheerde werkplekken, publieke clients, OT/IoT, leveranciersvoorzieningen en beheer-/managementpaden. Segmentatie voorkomt dat het compromis van één domein automatisch leidt tot toegang tot andere domeinen.

Verplichte zones

De volgende zones zijn verplicht aanwezig en mogen niet worden samengevoegd: (1) Beheerde werkplekzone - kantoorpersoneel, beheerde laptops en hybride werkplekken; (2) Publiekszone - publiek toegankelijke clients, internet-PC's, catalogus-PC's en publieke wifi; (3) OT/IoT-zone - gebouwbeheer, toegangscontrole, narrowcasting en overige operationele technologie; (4) Leveranciers- en beheerzone - PAM-toegang en uitbestede beheerhandelingen, strikt gescheiden van productiezones; (5) Server- en applicatiezone - interne systemen, identity-platform en applicatieservers. Per zone wordt een uitgaand communicatieprofiel vastgelegd (zie §6.4).

Harde scheidingen

De volgende scheidingen zijn hard (default-deny; elk pad vereist expliciete vastlegging):

a) Publiekszone → beheerde werkplekzone: geen laterale beweging mogelijk; publieke clients hebben geen toegang tot interne systemen of identiteiten.
b) OT/IoT-zone → alle andere zones: OT/IoT communiceert uitsluitend naar het eigen cloud-component of een expliciet vastgelegd endpoint; geen laterale paden naar werkplek- of applicatiezones.
c) Leveranciers- en beheerzone → productiezone: leverancierstoegang verloopt uitsluitend via PAM; directe toegang tot productiesystemen zonder gecontroleerd beheerpad is niet toegestaan.

Afwijkingen van harde scheidingen worden behandeld als tijdelijke uitzondering conform §9.2, met verplichte compenserende maatregelen en einddatum.

6.3 Communicatiepaden en herleidbaarheid

Communicatie tussen domeinen vindt alleen plaats via ontworpen en vastgelegde paden die herleidbaar zijn tot een functionele noodzaak. Elk communicatiepad heeft een eigenaar (wie verantwoordt het), een doel (waarom bestaat het) en een afbakening (wat is expliciet uitgesloten). Herleidbaarheid maakt het mogelijk voorstellen en wijzigingen inzichtelijk te maken en veranderingen beheerst door te voeren.

6.4 Uitgaande communicatie en afhankelijkheden

Uitgaande communicatie wordt bewust ingericht, omdat afhankelijkheden naar externe diensten anders onzichtbaar ontstaan. Uitgaand verkeer omvat ook update- en beheerkanalen (firmware/agent-updates, tijdsynchronisatie, certificaatcontroles, remote beheer). Per domein en device categorie wordt vastgelegd welke bestemmingen en protocollen noodzakelijk zijn, met logging en eigenaarschap.

Uitgaande communicatieprofielen verschillen per domein. Publieke clients en leveranciersvoorzieningen krijgen geen generiek internetprofiel. OT/IoT krijgt uitsluitend de noodzakelijke endpoints. Beheerde werkplekken kunnen breder internetgebruik hebben, maar zonder laterale paden naar domeinen met hoger risico.

Hoofdstuk 7 - Continuïteit, backup en herstel

7.1 Herstelbaarheid als architectuurkwaliteit

Continuïteit is een ontwerpeigenschap: de organisatie moet verstoringen kunnen opvangen zonder verlies van regie. Verstoringen en incidenten zijn onvermijdelijk. Herstelbaarheid is daarom geen operationele bijzaak maar onderdeel van het ontwerp van de keten.
Backup en herstel omvatten meer dan data. Drie herstelobjecten zijn relevant: data (inhoud en transacties), configuratie en beleid (instellingen, policies, integraties), en samenhang (koppelingen, identiteit-integratie, noodzakelijke referenties en metadata). Een omgeving is pas functioneel hersteld wanneer de samenhang die toegang en communicatie mogelijk maakt, ook hersteld is. Een backupstrategie voor alleen data is onvoldoende.

7.2 SaaS, leveranciers en herstelverantwoordelijkheid

SaaS-diensten kennen vaak ingebouwde beschikbaarheid, maar dit vervangt geen vastgelegd herstelmodel (principe 9). Voor elke gegevensgevoelige dienst moet de technische en juridische herstelbaarheid zijn geborgd in koppelvlakspecificaties. Zonder expliciete afspraken verschuift de herstelbaarheid volledig naar de leverancier, terwijl de verantwoordelijkheid bestuurlijk bij de organisatie blijft.
Voor kritische functies wordt vastgelegd: data-export volledig in standaardformaten en geautomatiseerd testbaar; metadata voor herstelbaarheid van configuraties, koppelingen en integraties; bewaartermijnen afgestemd op AVG/BIO en reconstructiebehoefte; herstelfrequentie, escalatieprocedures en gedifferentieerde hersteldoelstellingen (RTO/RPO) op basis van het belang van de dienst; en beschikbaarheid van logging/audit voor incidentreconstructie.
Indeling naar bedrijfskritische waarde. Hersteldoelstellingen worden bepaald per dienst op basis van de impact van uitval op bedrijfsvoering en compliance. Als richtinggevend kader worden drie niveaus gehanteerd:

1) Kritiek - diensten waarvan uitval directe bedrijfsontwrichting of compliance schending veroorzaakt (bijv. identiteitsbeheer, authenticatie, primaire bedrijfsapplicaties); hersteldoelstellingen worden zo kort mogelijk gesteld en zijn onderdeel van de SLA;
2) Operationeel - diensten waarvan uitval de werkuitvoering belemmert maar geen directe schade veroorzaakt; herstel binnen een werkdag is het vertrekpunt;
3) Ondersteunend - overige diensten; herstel binnen een nader af te spreken termijn, vastgelegd in de koppelvlakspecificaties. De indeling per dienst wordt vastgelegd in de koppelvlakspecificaties en herijkt bij contractverlenging of wezenlijke wijziging van de dienst.

Kritisch voor exit-by-design. Nieuwe leveranciers moeten toegang krijgen tot data-backups zonder afhankelijkheid van proprietary tooling van de vertrekkende leverancier. Beleidsinstellingen (zoals Conditional Access of toegangsregels) zijn gedocumenteerd en exporteerbaar. Backups en audit-logs zijn zodanig toegankelijk dat het jurisdictierisico van de primaire leverancier geen blokkade vormt voor de eigen toegang tot herstelbronnen.

7.3 Backup van configuraties en ketens

Voor netwerk- en securitycomponenten geldt dat configuratie en beleidsinstellingen onderdeel zijn van de herstelbare staat. Dit geldt ook voor integraties: configuraties van koppelingen, toegangsclaims en autorisatiemapping zijn essentieel om ketens na herstel correct te laten functioneren.

Hoofdstuk 8 - Beheer, toezicht en overdraagbaarheid

8.1 Beheer als apart domein

Beheerhandelingen wijzigen configuraties, beleid, toegangslogica en communicatiepaden en hebben daarmee een grote impact op risico en continuïteit. Het architectuurkader behandelt beheer als een apart domein met eigen paden, randvoorwaarden en toezicht. Beheer vindt uitsluitend plaats onder geschikte context, met minimale privileges en met traceerbaarheid.

8.2 Uitbesteding en regie

Uitbesteding van beheer is mogelijk en vaak wenselijk. Uitbesteding verandert echter niets aan de architectuureis dat beheer bestuurbaar en controleerbaar moet blijven (principe 11). Dit betekent een vastgelegde rolverdeling: wie stelt beleid vast, wie voert changes uit, wie autoriseert uitzonderingen en wie controleert. De organisatie behoudt minimaal expertise op architectuur-, toezicht- en auditniveau.

8.3 Toezicht: logging en audit als randvoorwaarde

Toezicht betekent dat relevante gebeurtenissen en wijzigingen zodanig worden vastgelegd dat reconstructie mogelijk is. Dit omvat minimaal: wijzigingen in configuratie en beleid, toekenning en gebruik van beheerrechten, relevante toegangs- en authenticatiegebeurtenissen, handelingen met compliancerelevantie en afwijkingen in communicatiepaden.
Toezicht strekt zich uit over eigen systemen én SaaS/leveranciersdiensten; toegang tot relevante logs en auditinformatie een verplicht onderdeel van de koppelvlakspecificaties.
Bij gedeelde resources (apparatuur, accounts, diensten) is herleidbaarheid per definitie lastiger. In die gevallen worden compenserende maatregelen getroffen: logging op applicatieniveau waar mogelijk, strikte functiebeperking, sessiemanagement en periodieke review. De mate van noodzakelijke herleidbaarheid wordt bepaald door de gevoeligheid van de handelingen en compliancevereisten.

8.4 Overdraagbaarheid en uitzonderingenbeheer

Overdraagbaarheid vereist dat architectuurkeuzes zijn vastgelegd (principe 12): definities en principes, uitzonderingen met reden, risico en einddatum, afhankelijkheden van externe diensten, en koppelvlakspecificaties die exit mogelijk maken. Het uitzonderingenregister wordt beheerd door de IT-manager en de Informatie-manager en jaarlijks herijkt.
Lifecycle als onderdeel van overdraagbaarheid. De overdrachtsmap bevat een lifecycle-overzicht: assetcategorie → ondersteuningsstatus → afhankelijkheden → compensatiemaatregelen.
Zo kan een nieuwe partij de architectuur voortzetten zonder verborgen EOL-risico's of stilvallende updates.

8.5 Koppelvlakken en portabiliteit

Afhankelijkheden op leverancier- of platformspecifieke functies worden geminimaliseerd door koppelvlakken te baseren op open standaarden en door mappings en configuraties overdraagbaar vast te leggen. Dit geldt voor alle ketens: applicaties, integraties, beheer en toegang.
Standaarden als uitgangspunt. Integraties gebruiken bij voorkeur algemeen geaccepteerde en goed gedocumenteerde standaarden - zoals SAML/OIDC/SCIM voor toegang en provisioning, gangbare web-API standaarden - tenzij dit aantoonbaar niet mogelijk of disproportioneel is. Afwijkingen worden onderbouwd ("pas toe of leg uit") inclusief de impact op overdraagbaarheid en benodigde compenserende maatregelen.
Functionele mapping. Autorisaties en koppelingen worden functioneel beschreven en beheerd, met een gecontroleerde mapping naar technische implementaties (groepen/claims/rollen, clientprofielen, policies). Waar processen leunen op platformdiensten (e-mail, files, identiteit, logging) worden exporteerbaarheid, bewaartermijnen en audit/reconstructie als contractuele eis vastgelegd.

Hoofdstuk 9 - Fasering en ontwikkeling

9.1 Doel van fasering

Fasering is het mechanisme om van een huidige situatie met gemengde patronen naar het doelbeeld te groeien zonder verlies van samenhang. Het is geen planningstechniek maar een architectuurmechanisme: het voorkomt dat onderdelen los van elkaar worden aangepast en daardoor nieuwe afhankelijkheden of uitzonderingen ontstaan.

9.2 Tijdelijke afwijkingen zijn expliciet

Het architectuurkader accepteert dat tijdelijke afwijkingen van het doelbeeld bestaan, bijvoorbeeld door afhankelijkheden, budget, contracten of technische beperkingen. Elke afwijking moet worden vastgelegd met: reden en scope, geïntroduceerd risico, mitigatie of compensatiemaatregel, eigenaar en beoogde einddatum of herijkmoment. Zonder deze explicitering is "een tijdelijke afwijking" feitelijk een permanente afwijking. Voorbeeldcategorieën van tijdelijke afwijkingen zijn: gedeelde apparatuur met beperkte herleidbaarheid (mitigatie: functiebeperking, applicatielogging, sessietimeouts, periodieke review); OT-systemen met beperkte segmentatie (mitigatie: compenserende netwerk-controls, extra monitoring, beperkte uitgaande communicatie); leverancierstoegang breder dan functioneel noodzakelijk (mitigatie: PAM, logging, tijdsbeperking, periodieke review); en on-premise componenten zonder volledige backup/hersteltest (mitigatie: alternatieve herstelroutes, documentatie afhankelijkheden).

9.3 Herijking en levensduur

Dit architectuurkader is ontworpen voor een levensduur van 7+ jaar, maar erkent dat technologie, dreigingen, wet- en regelgeving en leveranciersdiensten in de tijd veranderen. Voorgenomen wijzigingen - nieuwe diensten, vervanging van componenten, wijzigingen in beheervorm of leveranciers - worden beoordeeld tegen het doelbeeld en de vastgestelde definities. Afwijkingen en compenserende maatregelen worden vastgelegd in het uitzonderingenregister. Hiermee blijft de richting van het doelbeeld stabiel, terwijl de inrichting kan worden aangepast zonder verlies van overdraagbaarheid of aantoonbare beheersing.