API Richtlijnen

Aanbestedingsversie – mei 2025

Dit document stelt eisen aan de API-koppelingen van systemen die worden aanbesteed of ingekocht. Het gaat over de technische inrichting van het koppelvlak zelf: het REST-contract, versie-levenscyclus, machine-to-machine authenticatie, scoped autorisatie per doelbinding, auditlogging van API-aanroepen en event-notificaties.

De eisen voor hosting, beveiliging van de omgeving, privacy, digitale soevereiniteit en exitrecht staan in het document “Richtlijnen Cloudapplicaties”. Beide documenten zijn complementair en dienen samen te worden gehanteerd bij aanbestedingen waarbij een extern systeem via een API gegevens uitwisselt met het integratieplatform van de Opdrachtgever.

Inhoudsopgave

1. Algemeen en toepassingsbereik

Tegenwoordig zijn er veel API-koppelingen tussen systemen. Naast de inhoud van een koppelvlak zijn er randvoorwaarden die het koppelvlak beheersbaar, veilig en duurzaam inzetbaar maken.

De eisen in dit document zijn van toepassing op alle systemen die via een API gegevens uitwisselen met de service bus of het integratieplatform van de Opdrachtgever. Dit omvat:

- SaaS-applicaties met een ingebouwd koppelvlak.
- Managed hosting-oplossingen waarbij de leverancier een API aanbiedt op een door hem beheerde omgeving.
- iPaaS-platforms waarbij de leverancier API-endpoints of connectoren levert als onderdeel van het integratieplatform.
- Maatwerkkoppelingen geleverd door een leverancier als dienst.

De eisen richten zich op het koppelvlak. Eisen aan de omgeving waarin het systeem draait — hosting, beveiliging, privacy, soevereiniteit, omgevingen en exit — staan in het document “Richtlijnen Cloudapplicaties”.

✦ Aanbestedingseis
De Inschrijver verklaart bij inschrijving dat het aangeboden koppelvlak voldoet aan alle eisen in dit document. Afwijkingen worden expliciet vermeld met een beschrijving van de alternatieve maatregel.

1.1 Toepasselijkheid bij SOAP-koppelvlakken

De eisen in dit document zijn primair geformuleerd voor REST-API's conform OpenAPI 3.x, omdat dit de voorkeurstandaard is van de Opdrachtgever voor nieuwe koppelingen. De Opdrachtgever erkent echter dat een deel van de markt momenteel uitsluitend een SOAP-koppelvlak aanbiedt.

Indien een Inschrijver op het moment van inschrijving geen REST-API ondersteunt maar wel een SOAP-koppelvlak, is inschrijving onverminderd mogelijk. In dat geval gelden alle bepalingen uit dit document naar analogie, voor zover technisch van toepassing op SOAP. Concreet betekent dit:

- **Versioning.** Versiebeheer via de WSDL-naamruimte of een vergelijkbaar mechanisme; het levenscyclusbeleid (12 maanden ondersteuning, 6 maanden vooraankondiging bij breaking changes) is onverkort van kracht.
- **Beveiliging.** Transport via HTTPS (TLS 1.2+), authenticatie via WS-Security tokens of een equivalent mechanisme; basic authenticatie is niet toegestaan. Scoped autorisatie per doelbinding wordt gerealiseerd via een API-gateway of vergelijkbare proxy die voor het SOAP-endpoint staat.
- **M2M toegang.** Service-accounts met kortlevende tokens of certificaten; key-rotatie zonder downtime; scheiding van credentials per afnemend systeem.
- **Documentatie.** De actuele WSDL en het bijbehorende XSD-schema worden bij contractsluiting overgedragen aan de Opdrachtgever. Een changelog van schema-wijzigingen is verplicht.
- **Auditlog.** Logging van SOAP-aanroepen door externe systemen conform de eisen in sectie 6, inclusief client-identificatie, endpoint, tijdstip en statuscode.
- **Event-notificaties.** Indien beschikbaar via WS-Eventing, polling-endpoint of vergelijkbaar mechanisme; de wens in sectie 7 geldt naar analogie.

De Inschrijver geeft in de inschrijving expliciet aan welke bepalingen bij een SOAP-koppelvlak niet of slechts gedeeltelijk van toepassing zijn, en beschrijft per afwijking de alternatieve maatregel. Een roadmap met een concrete planning voor migratie naar REST is een pre bij de kwalitatieve beoordeling.

✦ Aanbestedingseis
Een Inschrijver met uitsluitend een SOAP-koppelvlak is ontvankelijk, mits de inschrijving per sectie toelicht hoe aan de strekking van elke eis wordt voldaan binnen de SOAP-architectuur. *Wens:* de Inschrijver levert een concrete roadmap voor migratie naar een REST API.

---

2. API URL en versioning

- **Vaste URL.** De API heeft een vaste URL die is opgenomen in het DNS van de leverancier. Naast een productie-URL is er altijd minimaal een acceptatie- of stagingversie beschikbaar op een ander (sub)domein, met een ander IP-adres en zonder verbinding naar de live dataset.

Voorbeeld:
Productie: `https://api.voorbeeldplatform.nl` *of* `https://voorbeeldplatform/api`

Acceptatie: `https://acc.api.voorbeeldplatform.nl` *of* `https://acc.voorbeeldplatform.nl/api`

- **Versiebeheer in de URL (eis).** Het major versienummer vormt onderdeel van de URL. Een breaking change in het schema leidt altijd tot een nieuw major versienummer, zodat meerdere versies parallel actief kunnen zijn tijdens migraties.

Voorbeeld: `https://api.voorbeeldplatform.nl/v1/`

- **Levenscyclusbeleid (eis).** De leverancier handhaaft elke major API-versie minimaal 12 maanden na publicatie van een opvolgende versie. Breaking changes worden minimaal 6 maanden van tevoren schriftelijk gecommuniceerd aan de Opdrachtgever, inclusief een migratieprocedure en tijdspad.
- **Eigendom API-specificatie (eis).** De OpenAPI 3.x specificatie van alle aangeboden koppelvlakken wordt bij contractsluiting overgedragen aan de Opdrachtgever in machineleesbaar formaat (YAML of JSON). De leverancier mag de specificatie niet incompatibel wijzigen zonder voorafgaande schriftelijke instemming van de Opdrachtgever.
- **Parameters.** Parameters worden toegevoegd als querystringparameters, niet als URL-fragmenten.

Voorbeeld: `https://api.voorbeeldplatform.nl?parameter1=waarde&parameter2=waarde2`

✦ Aanbestedingseis
Eis: de Inschrijver levert bij inschrijving een versioned REST API (OpenAPI 3.x) en beschrijft het versie-levenscyclusbeleid: minimale ondersteuningsperiode en communicatieprocedure bij wijzigingen.

---

3. Beveiliging van het koppelvlak

De eisen in deze sectie richten zich op de beveiliging van het API-koppelvlak zelf. Eisen aan de onderliggende hostingomgeving staan in “Richtlijnen Cloudapplicaties”, sectie 2 en 3.

- **Authenticatie (eis).** De API is voorzien van authenticatie voor alle niet-openbare informatie. Gebruik hierbij OAuth 2.0 Bearer token of JWT. Basic authenticatie is niet toegestaan. API-keys worden uitsluitend geplaatst in de Authorization-header, nooit in de querystring.
- **Transport (eis).** De API is uitsluitend bereikbaar via HTTPS op poort 443, met minimaal TLS 1.2. De leverancier gebruikt certificaten van een officiële Certificate Authority. Self-signed certificaten zijn niet toegestaan.
- **IP-locking.** IP-locking is alleen toegestaan tussen services (server-to-server), nooit naar eindgebruikers en nooit als vervanging van authenticatie of SSL.
- **Scoped autorisatie per doelbinding (eis).** De API ondersteunt OAuth 2.0 scopes of een vergelijkbaar mechanisme waarmee per integrerende partij exact wordt bepaald welke velden, resources en endpoints toegankelijk zijn. Dit is direct herleidbaar tot een verwerkingsdoelbinding conform de AVG, zodat elk afnemend systeem (IAM, telefoonboek, toegangspas, etc.) uitsluitend de gegevens ontvangt die passen bij zijn doelbinding.
- **SLA voor de API-laag (eis).** De leverancier garandeert voor de API-laag afzonderlijk: minimaal 99,9% beschikbaarheid per kalendermaand, maximale responstijd van 2 seconden (p95), gepubliceerde rate limits (minimaal X aanroepen per minuut per tenant), en een statuspage met meldplicht bij incidenten binnen 15 minuten.

✦ Aanbestedingseis

Eis: de Inschrijver beschrijft:
a) het authenticatiemechanisme (OAuth 2.0 / JWT);
b) de wijze waarop scoped autorisatie per doelbinding is ingericht;
c) de API-SLA (uptime, latency p95, rate limits, statuspage).

4. Machine-to-machine (M2M) toegang

De service bus van de Opdrachtgever communiceert met de API via een machine-to-machine verbinding — er is geen menselijke gebruiker betrokken. Hiervoor gelden aanvullende eisen naast de algemene beveiligingseisen in sectie 3.

- **OAuth 2.0 Client Credentials (eis).** M2M API-toegang verloopt via de OAuth 2.0 Client Credentials flow. Access tokens zijn kortlevend (maximale geldigheid: 1 uur) en worden automatisch vernieuwd door de integrerende partij.
- **Automatische key-rotatie (eis).** De leverancier ondersteunt het zonder onderbreking roteren van client secrets en/of certificaten. De procedure voor key-rotatie is gedocumenteerd en uitvoerbaar zonder downtime voor de koppeling.
- **Scheiding van service-accounts (eis).** Elke integrerende partij heeft een eigen client-ID met bijbehorende scopes. Gedeelde credentials tussen systemen zijn niet toegestaan.
- **Mutual TLS (wens).** De API ondersteunt optioneel mTLS als aanvullende verbindingsbeveiliging, zodat client en server wederzijds worden geauthenticeerd op certificaatniveau.
- **Geen MFA voor service-accounts.** Multi-factor authenticatie is niet van toepassing op M2M service-accounts; de Client Credentials flow met kortlevende tokens biedt een gelijkwaardig beveiligingsniveau.

✦ Aanbestedingseis
Eis: de Inschrijver beschrijft de M2M-authenticatiemethode (Client Credentials), de maximale token-levensduur en de procedure voor zero-downtime key-rotatie.
Wens: ondersteuning voor mTLS als aanvullende verbindingslaag.

5. Inhoudelijk en documentatie

5.1 Inhoudelijke eisen

- **REST en JSON (eis).** De API is een RESTful HTTP/HTTPS API conform OpenAPI 3.x, met JSON als primair dataformaat. SOAP-interfaces zijn toegestaan als aanvulling, maar niet als enige koppelvlak.
- Indien een object niet beschikbaar is maar verplicht teruggegeven moet worden, heeft het de waarde 'null'.
- Indien een lijst niet beschikbaar is maar verplicht teruggegeven moet worden, wordt een lege lijst verwacht ('[]').
- Datum- en tijdsnotatie volgen ISO 8601, inclusief tijdzone-indicatie.
- Gebruik camelCase voor attribuutnamen.
- Gebruik standaard HTTP-statuscodes voor succes- en foutresponses.
- Validatiefouten bevatten naast de HTTP-statuscode een duidelijke omschrijving in de response payload van welke validatie is mislukt en waarom.
- De API-definitie is bij voorkeur in het Engels.

5.2 Documentatie

- **OpenAPI-specificatie (eis).** De actuele documentatie is beschikbaar als OpenAPI 3.x definitie (voor REST-APIs) of XML-schema (voor SOAP-APIs). De specificatie wordt bij contractsluiting overgedragen in YAML of JSON.
- **Changelog (eis).** De leverancier houdt een changelog bij van alle API-versies: datum, aard van de wijziging (breaking / non-breaking) en migratiepad.
- **Sandbox-omgeving (wens).** De leverancier stelt een sandbox- of developer-omgeving beschikbaar waarmee nieuwe integraties kunnen worden ontwikkeld en getest zonder impact op productie of acceptatie.

6. LOG en Audit van API-aanroepen

Naast de algemene logging van de applicatie (zie “Richtlijnen Cloudapplicaties”, sectie 6) gelden specifieke eisen voor de logging van API-aanroepen door externe systemen.

- **Auditlog van externe API-aanroepen (eis).** Alle API-aanroepen door externe systemen — inclusief de service bus van de Opdrachtgever — worden gelogd met minimaal: timestamp, client-ID (OAuth client), endpoint, HTTP-methode, HTTP-statuscode en — gepseudonimiseerd — een aanduiding van welke resources zijn bevraagd. Volledige persoonsgegevens worden niet gelogd.
- **Bewaartermijn auditlog (eis).** De auditlog van API-aanroepen is minimaal 12 maanden beschikbaar en op eerste verzoek opvraagbaar door de Opdrachtgever.
- **Geen persoonsgegevens in standaard logregels.** Bijzondere persoonsgegevens worden niet opgenomen in standaard loglevel-regels. Debug-modus op productie is uitsluitend tijdelijk en na expliciete goedkeuring van de Opdrachtgever toegestaan.
- **Maintenancelog.** Herconfiguratie van toegangsparameters voor een API-integratie (zoals wijziging van client-ID, scopes of endpoints) wordt bijgehouden in de maintenancelog. Zie “Richtlijnen Cloudapplicaties”, sectie 6.3.

✦ **Aanbestedingseis**
Eis: de Inschrijver beschrijft de logging van externe API-aanroepen: welke velden worden gelogd, hoe persoonsgegevens worden gepseudonimiseerd, en op welke wijze de Opdrachtgever inzage krijgt.

---

7. Event-notificaties (wens)

Deze sectie beschrijft een wens van de Opdrachtgever. Leveranciers die event-notificaties ondersteunen worden uitgenodigd dit te beschrijven in hun inschrijving.

Voor de koppeling met de service bus is polling inefficiënt en foutgevoelig. Mutaties moeten idealiter real-time of near-real-time worden doorgegeven.

- **Webhook-ondersteuning (wens).** Bij elke relevante mutatie stuurt het systeem een HTTP POST naar een configureerbaar endpoint van de Opdrachtgever. De payload bevat minimaal: event-type, timestamp en een verwijzing naar het gewijzigde object. Volledige gegevens payload worden niet in de notificatie opgenomen.
- **Betrouwbare aflevering (wens).** Webhooks worden bij faalscenario's (onbereikbaar endpoint) opnieuw aangeboden met exponentiële back-off. De leverancier biedt een mechanisme om gemiste events alsnog op te halen.
- **Eventcatalogus (wens).** De leverancier publiceert een catalogus van beschikbare events (typen, payload-schema's) als onderdeel van de OpenAPI-documentatie of als apart AsyncAPI-document.
- **Delta-endpoint als alternatief (wens).** Indien webhooks niet worden ondersteund, biedt de leverancier minimaal een delta-endpoint waarmee uitsluitend gewijzigde records kunnen worden opgehaald sinds een opgegeven tijdstip.

✦ **Aanbestedingseis**
Wens: de Inschrijver beschrijft of en hoe event-notificaties worden ondersteund (webhooks, event streams of delta-endpoints), inclusief betrouwbaarheidsgaranties en documentatie.

---

8. Omgevingen

De eisen voor de inrichting van test-, acceptatie- en productieomgevingen staan in het document "Richtlijnen Cloudapplicaties", sectie 7. Voor de API-koppeling geldt aanvullend het volgende.

- **Aparte API-endpoints per omgeving (eis).** Elke omgeving (test, acceptatie, productie) heeft een eigen, afzonderlijk API-endpoint. De acceptatie-API is nooit aangesloten op de live dataset en heeft een ander IP-adres dan productie.
- **Versienummer consistent per omgeving.** Het major versienummer van de API is gelijk aan of hoger dan dat van productie, zodat integraties getest kunnen worden op de toekomstige API-versie vóór go-live.
- **Acceptatie-omgeving beschikbaar voor ketentest.** De acceptatieomgeving is beschikbaar voor ketentest met de acceptatieversies van andere systemen in het systeemlandschap van de Opdrachtgever.

— Einde document —