Appwinst

Normatieve specificatie: Klantportaal

Versie 1.8 van 26 oktober 2026

1. Status, reikwijdte en conventies

Deze specificatie beschrijft de apps van een bedrijf dat warmtepompen en ventilatie installeert en onderhoudt bij bedrijven en scholen in Twente. Dit document noemt dat bedrijf het installatiebedrijf (Begrippen). Zij is opgesteld bij de Bouwcheck en is een concept tot de Bouwbrief haar versie en digest vastlegt (BB-001). Zij beschrijft de Build die de Bouwcheck voorstelt; wat zij niet noemt, hoort niet bij de Build.

Reikwijdte. Twee apps die in de browser werken op desktop, tablet en telefoon (BC-011):

- het **Klantportaal**, voor de contactpersonen van de relaties van het installatiebedrijf, op `https://portaal.voorbeeld.example`;
- **Binnendienst**, voor de medewerkers van het installatiebedrijf, op `https://binnendienst.voorbeeld.example`.

Een klant logt in met een inloglink, ziet de orders van zijn relatie met hun status en geplande datum, opent een order met de werkbonnen, de factuur en de documenten, en stelt er een vraag over. Een binnendienstmedewerker logt in met een passkey, beantwoordt die vraag met de order erbij, en de klant krijgt een e-mail. De vragen en antwoorden zijn de Uitbreiding Berichten (A5). De app leest orders, stukken, relaties en contactpersonen uit Exact Online en schrijft er niets in. Teksten en beelden, Beheeromgeving en Organisatiebeheer zitten in de Build (ADD-006). Wat de Build niet doet, staat in de Niet-lijst.

Conventies.

- **ALG-001** De woorden MUST, MUST NOT, SHOULD, SHOULD NOT en MAY hebben de betekenis die BCP 14 (RFC 2119 en RFC 8174) ze geeft, als ze in hoofdletters staan.
- **ALG-002** Elke eis heeft een vaste code met een voorvoegsel per sectie. Een code wordt nooit opnieuw gebruikt of hernummerd; een ingetrokken eis houdt zijn code met de tekst "Ingetrokken in versie X.Y". Een wijziging na ondertekening is een nieuwe versie van dit document, genoemd in een Wijziging (BB-010).
- **ALG-003** Een code die dit document niet zelf vastlegt, zoals LEG-019, is een eis van de normatieve specificatie van Appwinst, in de versie die de Bouwbrief vastlegt (VER-001). Bij een verschil tussen dit document

en de Bouwbrief geldt de Bouwbrief voor prijs, datums en plichten, en dit document voor wat de app doet.

- **ALG-004** Elk begrip uit Begrippen betekent overal in dit document hetzelfde, en één idee heeft één woord.
- **ALG-005** Elke instelling van de app staat in Bijlage: configuratiewaarden, met de eis die haar vastlegt. Een andere instelling is een nieuwe versie van dit document (ALG-002). Wat de beheerder in de Beheeromgeving of in Teksten en beelden beheert, zoals de documenttypen per soort (GEG-006), zijn gegevens van de app en geen instelling: de beheerder wijzigt ze zonder nieuwe versie.

Onderzoeksbasis

De reizen en eisen in dit document steunen op deze bronnen, alle gelezen op 2026-10-26. Elke bron staat hier met uitgever, titel, site en datum; het volledige adres staat in het onderzoek dat de Bouwcheck bewaart. Het nummer tussen haken, zoals [20], is dat van dat onderzoek. Dit document haalt een bron aan met dat nummer, of met haar uitgever en titel zoals ze hier staan. Een bron die geen reis of eis gebruikt, staat hier niet, dus de nummers lopen niet door. De bronnen [41] en [42] noemen de eisen zelf.

- [1] Exact Online, REST API: SalesOrderSalesOrders, start.exactonline.nl, ongedateerd.
- [2] Exact Online, REST API: overzicht van de resources, start.exactonline.nl, ongedateerd.
- [3] Exact Online, REST API: WebhooksWebhookSubscriptions, start.exactonline.nl, ongedateerd.
- [4] Exact Online, REST API: DocumentsDocuments, start.exactonline.nl, ongedateerd.
- [5] Exact Online, REST API: CRMContacts, start.exactonline.nl, ongedateerd.
- [6] Apideck, Exact Online configuration, apideck.com, ongedateerd.
- [7] Exact Knowledge Base, App publication procedure, exactonline.com, ongedateerd (gelezen via een zoekresultaat).
- [8] Exact Knowledge Base, Step 3. Get/use access tokens, exactonline.com, ongedateerd (alleen het zoekfragment gelezen; de pagina laadde niet).
- [9] Nango, Exact Online, nango.dev, ongedateerd.
- [10] Hookdeck, Guide to Exact Online Webhooks, hookdeck.com, ongedateerd.
- [11] Clickker, Exact Online restricties boekingen en API-calls, clickker.nl, ongedateerd (ingangsdatum 1 januari 2025).
- [12] Barcode Scan, Exact Online API limits guide, barcodescan.nl, ongedateerd.
- [17] IPLO, Consumentendossier (opleverdossier) en Wkb, iplo.nl, ongedateerd.

– [18] VBK, Het opleverdossier van de Wkb met terugwerkende kracht in werking getreden, vbk.nl, 2024-03-07.
– [19] Kiwa, Wkb: consumentendossier alleen verplicht voor nieuwe werken, kiwa.com, ongedateerd.
– [20] Baymard, Accounts & Self-Service UX Research 2026, baymard.com, 2026-09-09.
– [21] Baymard, Order Tracking UX: 6 Key Details to Provide, baymard.com, ongedateerd.
– [22] Baymard, Order Tracking & Returns UX Benchmark 2024, baymard.com, maart 2024.
– [23] NN/g, Passwordless Accounts en A Checklist for Registration and Login Forms on Mobile, nngroup.com, ongedateerd.
– [24] NN/g, Visibility of System Status en Progress Indicators, nngroup.com, ongedateerd.
– [25] Buildertrend, Qobrix en Contractors Cloud, pagina's over klantportalen voor aannemers, ongedateerd.
– [26] OutSmart kennisbank, Klantportaal: werkboninstellingen, out-smart.com, ongedateerd.
– [27] Verordening (EU) 2016/679 (AVG), art. 5, 25, 28 en 32, 2016-04-27, van kracht.
– [28] Vlaamse Toezichtcommissie, Verwerkersovereenkomst, vlaanderen.be, ongedateerd; en Apideck, Exact Online overview, apideck.com, ongedateerd.
– [29] Taylor Wessing, European Accessibility Act: requirements for e-commerce services, taylorwessing.com, 2025-09-30.
– [34] Chift, How to integrate with Exact Online API, chift.eu, ongedateerd.
– [35] Microsoft Power Users, "Old refresh token used", microsoft.com, ongedateerd.
– [36] Exact Support, API rate limits, exactonline.com, ongedateerd (gelezen via een zoekresultaat).
– [38] Peliqan, Exact Online API, peliqan.io, ongedateerd.
– [39] Genkgo, Setup of the connection (Exact Online), genkgo.com, ongedateerd.
– [40] Cyclr, Exact Setup, cyclr.com, ongedateerd.
– [41] W3C, Web Content Accessibility Guidelines (WCAG) 2.2, W3C-aanbeveling, w3.org, 2023-10-05.
– [42] OWASP, Application Security Verification Standard 5.0.0, owasp.org, mei 2025.

Versies

Versie	Datum	Wat veranderde
1.0–1.3	tot en met 2026-10-19	Opgesteld bij een eerdere Bouwcheck,

		voor een andere Aanvraag. Vervangen door 1.4.
1.4	2026-10-26	Geheel nieuw opgesteld voor de Aanvraag van Bouwcheckronde 1, voor de Build die de Bouwcheck voorstelt: het Klantportaal en Binnendienst met vragen over een order (A5), zeven schermen, drie rollen, één leeskoppeling met Exact Online. Contactpersonen komen via de koppeling, niet uit een importbestand (BUITEN-002). Onderhoud plannen is geen deel van de Build (BUITEN-003). Geen telefoonnummers (BUITEN-008). Een code uit 1.0–1.3 heeft in 1.4 alleen de betekenis die 1.4 haar geeft.
1.5	2026-10-26	De items van de Niet-lijst heten BUITEN-001 tot en met BUITEN-013; in 1.4 heetten ze UIT-, met dezelfde nummers en woorden, en elke verwijzing volgt. Waar een bron buiten de Onderzoeksbasis met haar datum werd aangehaald, staat nu haar nummer uit het onderzoek, zoals [27]. Wat de app doet, verandert niet.
1.6	2026-10-26	De eisen van het Domeinmodel heten

		GEG-001 tot en met GEG-015; in 1.5 heetten ze DOM-, met dezelfde nummers en woorden. Ze kregen een ander voorvoegsel omdat de specificatie van Appwinst zelf DOM- gebruikt. Elke verwijzing volgt. Wat de app doet, verandert niet.
1.7	2026-10-26	De namen van de gebeurtenissen voor geopende stukken in REIS-003 staan zonder tweede liggend streepje. Wat de app telt en doet, verandert niet.
1.8	2026-11-02	Het platform heet nu Appwinst, en zo staat het overal in dit document. Wat de app doet, verandert niet.

2. Begrippen

Deze begrippen zijn normatief. Elk idee heeft één woord; dat woord betekent overal in dit document precies dit. De code is de naam in de broncode. In lopende tekst staan de begrippen in kleine letters; alleen de namen Klantportaal, Binnendienst en Exact Online hebben een hoofdletter. De begrippen staan in de volgorde waarin een klant ze tegenkomt.

Begrip	Code	Betekenis
Installatiebedrijf	`InstallationCompany`	De opdrachtgever: het bedrijf dat de app laat bouwen en gebruikt. Het installeert en onderhoudt warmtepompen en ventilatie bij bedrijven en scholen.
Klantportaal	`CustomerPortal`	De app voor klanten, op het adres hieronder.
Binnendienst	`Office`	De app voor medewerkers, op het

		adres hieronder. Alleen de app heet zo (zie hieronder).
Relatie	`Relation`	Een bedrijf of school waarvoor het installatiebedrijf werkt: een account in Exact Online, met relatiecode, met ten minste één verkooporder. Een leverancier is geen relatie.
Contactpersoon	`Contact`	Een persoon bij een relatie in Exact Online, met naam en e-mailadres.
Klant	`Customer`	Rol: wie met een e-mailadres inlogt in het Klantportaal. Eén klant is één e-mailadres, dat bij een of meer contactpersonen staat (GEG-003).
Medewerker	`Employee`	Een persoon van het installatiebedrijf met toegang tot Binnendienst, met de rol binnendienstmedewerker of beheerder.
Binnendienstmedewerker	`OfficeEmployee`	Rol: een medewerker die vragen beantwoordt.
Beheerder	`Administrator`	Rol: de medewerker die medewerkers uitnodigt in Organisatiebeheer, en de toegang van klanten blokkeert en terugzet.
Inloglink	`SignInLink`	Een link per e-mail waarmee een klant inlogt, zonder wachtwoord, in de browser die hem aanvroeg (BEV-002).

Inlogcode	`SignInCode`	De code in dezelfde e-mail als de inloglink, om in te vullen in de browser die de link aanvroeg (BEV-002).
Passkey	`Passkey`	Waarmee een medewerker inlogt en een handeling van de beheerder bevestigt (BEV-006, ROL-010).
Synchronisatie	`Sync`	Het lezen van de wijzigingen uit Exact Online (KOP-004).
Order	`Order`	Een verkooporder van een relatie in Exact Online, met zijn ordernummer en omschrijving.
Status	`OrderStatus`	De ene tekst die zegt hoe een order ervoor staat, volgens STAT-001. Een order heeft er altijd precies één.
Geplande datum	`PlannedDate`	De leverdatum van een order in Exact Online (`DeliveryDate`), getoond zoals STAT-002 zegt.
Statuswijziging	`StatusChange`	Een wijziging van `Status` of `DeliveryDate` van een order in Exact Online, zoals de app haar bij een synchronisatie zag (VAST-002).
Stuk	`OrderFile`	Een document bij een order in Exact Online: een werkbon, een factuur of een ander document, met een of meer bestanden.
Documenttype	`DocumentType`	Het type van een document in Exact Online.

Soort	`FileKind`	Wat een stuk is: werkbon, factuur of document. De soort volgt uit het documenttype (GEG-006).
Werkbon	`WorkOrder`	Een stuk met het verslag van werk aan een order.
Factuur	`Invoice`	Een stuk met de rekening voor een order.
Document	`OtherDocument`	Elk ander stuk bij een order, zoals een opleverrapport of certificaat.
Bestand	`Attachment`	Een bestand van een stuk, zoals een pdf, dat opent.
Gesprek	`Conversation`	De vragen en antwoorden bij één order.
Vraag	`Question`	Een bericht in tekst van een klant over één order.
Antwoord	`Answer`	Een bericht in tekst van een binnendienstmedewerker in het gesprek van één order.
Open vraag	`OpenQuestion`	Een vraag waarna in het gesprek nog geen antwoord kwam en die niet is afgesloten.
Afsluiten	`Close`	Een open vraag afhandelen zonder antwoord. De vraag is dan afgesloten, en de klant krijgt geen e-mail.
Toegang	`Access`	Of een klant bij een relatie kan inloggen: Kan inloggen of Geblokkeerd.
Blokkeren	`Block`	De toegang van een e-mailadres bij één relatie beëindigen. Het resultaat

		is een blokkade (GEG-010).
Toegang terugzetten	`RestoreAccess`	Een blokkade opheffen, zodat de klant bij die relatie weer kan inloggen.
Gebeurtenis	`Event`	Iets wat de app per dag telt voor een maat van Kernproces (MEET-001).
Stap	`Step`	Eén tik of klik waarmee de gebruiker verder gaat. Typen in een veld en scrollen zijn geen stap.

Binnendienst is alleen de naam van de app. De mensen die er vragen beantwoorden, zijn binnendienstmedewerkers.

De adressen van de twee apps:

- Klantportaal: `https://portaal.voorbeeld.example`
- Binnendienst: `https://binnendienst.voorbeeld.example`

De woorden Teksten en beelden, Beheeromgeving, Organisatiebeheer, Preview, Mobiel, Tablet en Desktop betekenen wat de Appwinst-specificatie zegt (ADD-006, PRV-007).

3. Invarianten

- **INVAR-001** Een klant MUST alleen orders, stukken en vragen van zijn eigen relatie kunnen zien of openen. De server MUST dit bij elk verzoek toetsen, ook bij het openen van een bestand; een verzoek om iets van een andere relatie krijgt hetzelfde antwoord als een verzoek om iets wat niet bestaat (ROL-009, SCH-005).
- **INVAR-002** De app MUST NOT iets schrijven in Exact Online: de code die Exact Online aanroept, kan alleen GET-verzoeken maken (KOP-001), ook als de registratie van de app in Exact Online schrijfrechten geeft.
- **INVAR-003** Een klant MUST alleen kunnen inloggen en ingelogd blijven zolang hij toegang heeft (GEG-003). De server MUST dit bij elk verzoek toetsen, zodat het einde van de toegang (ROL-007) ook een sessie beëindigt die al openstond.
- **INVAR-004** Elke order MUST precies één status hebben, die STAT-001 geeft. Een status MUST NOT leeg zijn, en een order MUST NOT twee statussen tegelijk tonen (STAT-003).
- **INVAR-005** Wat een scherm uit Exact Online toont, MUST ten hoogste één synchronisatie (KOP-004) achterlopen op Exact Online. Kan de app dat niet waarmaken, dan MUST het scherm de laatst bekende gegevens tonen met de tijd waarop ze zijn bijgewerkt (SCH-004, KOP-009), en

MUST NOT het een lege lijst tonen in plaats van gegevens die de app niet kon lezen.

- **INVAR-006** Een vraag MUST bij precies één order horen, en bij de klant die hem stelde zolang die klant bestaat (GEG-011). Een vraag MUST NOT naar een andere order verhuizen.
- **INVAR-007** Bij elk antwoord MUST elke klant die MEL-005 noemt precies één e-mail krijgen, ook als het versturen opnieuw wordt geprobeerd (GEG-012).

4. Rollen en rechten

De app kent drie rollen over twee portalen: de klant op het Klantportaal, de binnendienstmedewerker en de beheerder op Binnendienst. Wat ROL-004 niet toestaat, weigert de app.

- **ROL-001 Standaard geweigerd.** De app MUST elke handeling en elke vraag naar gegevens weigeren die ROL-004 niet aan de rol van de ingelogde persoon geeft. Identiteit, rol en relatie MUST uit de sessie op de server komen, bij elk verzoek, en nooit uit wat de browser meestuurt.
- **ROL-002 Klant.** Een klant is een contactpersoon in Exact Online met een e-mailadres, bij een relatie die in de gekoppelde administratie minstens één verkooporder heeft (VKL-003, GEG-002). Hij logt alleen in op het Klantportaal, en heeft toegang tot zo'n relatie zolang de beheerder hem daar niet blokkeert (GEG-003). Er is geen uitnodiging en geen account om aan te maken: de toegang volgt Exact Online. Een contactpersoon van een account zonder verkooporder, zoals een leverancier, is geen klant.
- **ROL-003 Binnendienstmedewerker en beheerder.** Een binnendienstmedewerker logt alleen in op Binnendienst, na een uitnodiging van de beheerder via Organisatiebeheer (ADD-006, I3). De beheerder heeft elk recht van de binnendienstmedewerker, en daarnaast de rechten die ROL-004 alleen hem geeft.
- **ROL-004 Rechten per rol.** Elke rol heeft precies de rechten hieronder, en geen andere.

Klant. Mag: orders en een order zien, met de status en de geplande datum, van zijn eigen relatie (ROL-005); een stuk bij een order openen (een werkbon, factuur of document) van zijn eigen relatie, alleen zichtbare stukken (ROL-006); een vraag stellen over een order van zijn eigen relatie; vragen en antwoorden lezen bij een order van zijn eigen relatie. Mag niet: een vraag beantwoorden of een open vraag afsluiten; Klanten zien; de toegang van een klant blokkeren of terugzetten; medewerkers uitnodigen, hun rol geven of verwijderen; Teksten en beelden of de instellingen in de Beheeromgeving wijzigen; iets schrijven in Exact Online (BUITEN-001).

Binnendienstmedewerker. Mag: alleen de order bij een vraag zien, met de status en de geplande datum; een stuk openen bij een order met een vraag, alleen zichtbare stukken (ROL-006); de vragen en antwoorden bij elke order lezen; elke vraag beantwoorden en elke open vraag afsluiten; Klanten zien: contactpersoon, relatie en toegang. Mag niet: een vraag stellen; de toegang van een klant blokkeren of terugzetten; medewerkers uitnodigen, hun rol geven of verwijderen; Teksten en beelden of de instellingen in de Beheeromgeving wijzigen; iets schrijven in Exact Online (BUITEN-001).

Beheerder. Mag: alles wat de binnendienstmedewerker mag; daarnaast de toegang van een klant bij een relatie blokkeren en terugzetten; medewerkers uitnodigen, hun rol geven en verwijderen (Organisatiebeheer); Teksten en beelden wijzigen, en de instellingen in de Beheeromgeving, waaronder de documenttypen per soort (ROL-006) en de koppeling met Exact Online (KOP-009). Mag niet: een vraag stellen; iets schrijven in Exact Online (BUITEN-001).

- **ROL-005 Eigen relatie.** De relatie van een klant is de relatie in Exact Online waarbij zijn contactpersoon staat. Een order hoort bij precies één relatie, gelezen uit één veld van de verkooporder in Exact Online (**VRAAG-ROL-1**: telt de besteller, het afleveradres of het factuuradres?). Dat veld bepaalt wie welke orders ziet; het installatiebedrijf beantwoordt de vraag daarom vóór ondertekening (BB-006), en het antwoord komt in deze eis. Op Dag 0 toetst de Bouwer alleen dat het gekozen veld in de testadministratie gevuld is (BOUW-002). Een order MUST NOT via een tweede veld zichtbaar worden. Staat één e-mailadres bij contactpersonen van meer dan één relatie, dan is die persoon klant van elk van die relaties; elk verzoek om gegevens geldt dan voor één van die relaties tegelijk, en nooit voor een relatie waarvan hij geen contactpersoon is (SCH-023).
- **ROL-006 Zichtbare stukken.** Een stuk is alleen zichtbaar, voor klanten en medewerkers, als de tabel Documenttypen per soort (GEG-006) zijn documenttype in Exact Online een soort geeft (werkbon, factuur of document), en als de relatie die Exact Online bij het document noemt, waar die er staat, dezelfde is als de relatie van de order. Een documenttype dat de tabel niet noemt of niet zichtbaar geeft, toont de app niemand: Exact Online kan bij een order ook interne stukken bewaren. De tabel is leeg tot het installatiebedrijf haar vóór Start met de Bouwer vaststelt (**VRAAG-ROL-2**: welke documenttypen in Exact Online zijn de werkbon, de factuur en de documenten die klanten mogen zien?; BOUW-002); de beheerder wijzigt haar daarna in de Beheeromgeving.
- **ROL-007 Einde van de toegang.** De toegang van een klant tot een relatie MUST eindigen, ook in een sessie die al openstaat: bij zijn

eerstvolgende verzoek nadat de beheerder hem bij die relatie blokkeert; en bij de eerstvolgende synchronisatie (KOP-004) waarin geen contactpersoon van die relatie zijn e-mailadres meer heeft, of waarin de relatie niet meer in de administratie staat of geen verkooporder meer heeft. Een blokkade rust op het genormaliseerde e-mailadres bij één relatie (GEG-010). Zij MUST blijven gelden als dat adres uit Exact Online verdwijnt en later terugkomt, en eindigt alleen als de beheerder de toegang terugzet of de relatie verdwijnt. Een blokkade bij de ene relatie raakt de toegang tot een andere relatie niet. Een medewerker die de beheerder in Organisatiebeheer verwijdert, verliest de toegang bij zijn eerstvolgende verzoek.

- **ROL-008 Gescheiden portalen.** Een sessie van het Klantportaal MUST NOT gelden op Binnendienst, en omgekeerd. Een klant kan niet inloggen op Binnendienst.
- **ROL-009 Niet gevonden is niet gevonden.** Een verzoek om een order, stuk of vraag buiten de rechten van ROL-004 MUST hetzelfde antwoord krijgen als een verzoek om iets dat niet bestaat (SCH-005). Een adres in de app SHOULD een eigen willekeurige sleutel dragen, niet het ordernummer uit Exact Online.
- **ROL-010 Bevestigen met een passkey.** Blokkeren, toegang terugzetten, een medewerker uitnodigen, opnieuw uitnodigen (BEV-006), zijn rol wijzigen of hem verwijderen, de documenttypen per soort wijzigen en de koppeling met Exact Online opnieuw maken MUST een bevestiging met de passkey van de beheerder vragen binnen de laatste 10 minuten.

5. Domeinmodel

Exact Online is de bron van relaties, contactpersonen, orders en stukken. De app houdt daarvan een kopie die alleen de koppeling schrijft (BUITEN-001), zodat een lijst niet bij elke weergave Exact Online hoeft te vragen en de app ziet wanneer een status verandert. Wat gebruikers zelf invoeren (vragen, antwoorden, afsluitingen, blokkades, de documenttypen) is van de app. Elke waarde staat op één van de twee draden van het framework: YSQL (relationeel, met transacties, sleutels en constraints) of YCQL (op één sleutel, met verlooptijd en tellers).

Entiteiten

De naam van elke entiteit is de naam in het model; waar Begrippen het woord ook vastlegt, betekent het hetzelfde. Per entiteit: identificatie, waar zij bij hoort, velden, bron, en de draad met de reden.

- **Relatie.** Identificatie: het account-ID van Exact Online (GUID); de relatiecode (`Code`) is uniek. Hoort bij: heeft contactpersonen en orders. Velden: relatiecode, naam. Bron: de koppeling (`crm/Accounts`). Draad: YSQL: elke toegangscontrole loopt via de relatie; de relatiecode is uniek door een index.

- **Contactpersoon.** Identificatie: het contact-ID van Exact Online (GUID). Hoort bij: precies één relatie; precies één klant, via het e-mailadres. Velden: naam (`FullName`), e-mailadres (het veld van IMP-003). Bron: de koppeling (`crm/Contacts`). Draad: YSQL: sleutel naar relatie en klant; gelijst per relatie en gezocht in Klanten.
- **Klant.** Identificatie: een UUIDv5 van het genormaliseerde e-mailadres; het adres is uniek. Hoort bij: één of meer contactpersonen. Velden: e-mailadres. Bron: afgeleid uit de contactpersonen. Draad: YSQL: inloggen zoekt op het adres; een vraag draagt zijn identificatie.
- **Blokkade.** Identificatie: het genormaliseerde e-mailadres en de relatie samen. Hoort bij: één e-mailadres, één relatie. Velden: geblokkeerd door (medewerker), geblokkeerd op. Bron: wat de beheerder invoert (Klanten). Draad: YSQL: een blokkade geldt direct; de toegangscontrole leest haar in dezelfde transactie; zij verwijst niet naar de klant, zodat zij blijft als de klant verdwijnt.
- **Order.** Identificatie: het order-ID van Exact Online (GUID); het ordernummer is uniek. Hoort bij: precies één relatie; heeft stukken, statuswijzigingen en één gesprek. Velden: ordernummer, omschrijving, orderdatum (`OrderDate`), geplande datum (`DeliveryDate`), `Status`. Bron: de koppeling (`SalesOrders`). Draad: YSQL: gelijst per relatie op status en datum; sleutel voor stukken, statuswijzigingen en het gesprek.
- **Documenttype.** Identificatie: het documenttype van Exact Online. Hoort bij: niets. Velden: naam in Exact Online, soort (werkbon, factuur, document) of niet zichtbaar. Bron: vóór de Start vastgesteld (BOUW-002), daarna de beheerder (Beheeromgeving). Draad: YSQL: elke stuk-regel van de koppeling leest het; een wijziging start een nieuwe lezing van de documenten.
- **Stuk.** Identificatie: het document-ID van Exact Online (GUID). Hoort bij: precies één order; precies één documenttype; heeft bestanden. Velden: onderwerp, datum. Bron: de koppeling (`Documents`). Draad: YSQL: gelijst per order; de toegang volgt de relatie van de order.
- **Bestand.** Identificatie: het bijlage-ID van Exact Online (GUID). Hoort bij: precies één stuk. Velden: bestandsnaam, bestandstype, grootte. Bron: de koppeling (`DocumentAttachments`). Draad: YSQL: alleen de verwijzing; de inhoud bewaart de app niet (GEG-007).
- **Statuswijziging.** Identificatie: order, moment gezien en veld samen. Hoort bij: precies één order. Velden: veld (`Status` of `DeliveryDate`), oude waarde, nieuwe waarde, gezien op, gewijzigd in Exact (`Modified`). Bron: de koppeling, bij elke synchronisatie. Draad: YSQL: geschreven in dezelfde transactie als de order die haar toont, en verwijderd met de order.
- **Vraag, Antwoord.** Identificatie: het bericht-ID van de threads-kit van Berichten (A5). Hoort bij: het gesprek van precies één order; een vraag van een klant, een antwoord van een binnendienstmedewerker. Velden:

tekst, geschreven op, geschreven door; bij een antwoord ook gezien op. Bron: wat gebruikers invoeren (Order, Vraag). Draad: YSQL: de lijst open vragen filtert over alle orders, en de e-mail gaat via de outbox in dezelfde transactie.

- **Afsluiting.** Identificatie: het gesprek en het moment samen. Hoort bij: het gesprek van precies één order. Velden: afgesloten door (medewerker), afgesloten op. Bron: wat een binnendienstmedewerker invoert (Vraag). Draad: YSQL: sluit de open vragen van dat gesprek in dezelfde transactie.
- **Inloglink.** Identificatie: de klant-identificatie: per klant ten hoogste één geldige link. Hoort bij: precies één klant. Velden: hash van het token, hash van de inlogcode, binding aan de browser die hem vroeg, foute pogingen, gebruikt. Bron: de app, bij een aanvraag (Klantportaal: Inloggen). Draad: YCQL: verloopt op de klok (een verlooptijd bij het schrijven, BEV-002), gelezen op één sleutel; gebruiken en foute pogingen zijn voorwaardelijke schrijfacties op die sleutel; een nieuwe aanvraag overschrijft de vorige link.
- **Telling.** Identificatie: gebeurtenis en dag samen. Hoort bij: niets: geen persoon, geen relatie, geen order. Velden: aantal. Bron: de app, bij elke gebeurtenis van Kernproces (MEET-001). Draad: YCQL: een teller, alleen opgeteld en per gebeurtenis over dagen gelezen.
- **Synchronisatie.** Identificatie: de bron in Exact Online (relaties, contactpersonen, orders, documenten). Hoort bij: niets. Velden: cursor, laatst gelukt op, laatste fout. Bron: de koppeling. Draad: YSQL: de cursor schuift in dezelfde transactie als de gegevens die hij las; Orders, Order, Klanten en de Beheeromgeving lezen er de tijd van de stand uit (KOP-009).
- **Koppelingsslot.** Identificatie: de administratie van Exact Online. Hoort bij: niets. Velden: versie van het geheim in de geheimenopslag, access token verloopt op. Bron: de koppeling. Draad: YSQL: één rij, vergrendeld met `SELECT ... FOR UPDATE` bij elke vernieuwing, zodat er nooit twee tegelijk lopen (KOP-006). Geen token: dat staat in de geheimenopslag en het geheugen (BEV-009).

Medewerkers (binnendienstmedewerkers en de beheerder), hun e-mailadres, hun rol en hun passkeys zijn van Organisatiebeheer (ADD-006, BEV-006); dit model verwijst naar hen met hun identificatie. De grenzen van BEV-004 per IP-adres, per e-mailadres en voor geopende stukken telt de server in zijn geheugen (AVG-003); vragen per klant per dag telt hij uit de vragen zelf.

Eisen

- **GEG-001 Exact Online is de bron.** Relatie, contactpersoon, order, stuk en bestand MUST alleen door de koppeling worden geschreven. Geen scherm wijzigt een waarde die uit Exact Online komt; een wijziging

gebeurt in Exact Online en komt bij de volgende synchronisatie in de app (VKL-002). De koppeling leest alleen de velden van de entiteiten hierboven, met de sleutels en wijzigingsmomenten die de synchronisatie nodig heeft, en het veld van ROL-005 (KOP-002, KOP-004).

- **GEG-002 Alleen wat een stap nodig heeft.** De app MUST een relatie alleen houden als Exact Online minstens één verkooporder van die relatie heeft (VKL-003), en een contactpersoon alleen als hij een e-mailadres heeft en bij een gehouden relatie hoort (AVG-004). Van een contactpersoon MUST de app alleen naam en e-mailadres lezen; het telefoonnummer, de functie en elk ander veld MUST NOT worden gelezen of bewaard (BUITEN-008). Van een order MUST NOT de naam van wie hem in Exact Online wijzigde (`ModifierFullName`) worden gelezen, en ook `DeliveryStatus` en `InvoiceStatus` niet zolang STAT-001 ze niet gebruikt (OPEN-001); zet OPEN-001 ze in STAT-001, dan komen ze bij de velden van Order.
- **GEG-003 Een klant is één e-mailadres.** De app MUST één klant houden per e-mailadres, genormaliseerd zonder spaties en in kleine letters, zolang minstens één contactpersoon dat adres heeft. Staan twee contactpersonen met hetzelfde adres in Exact Online (een gedeelde mailbox, of dezelfde persoon bij twee relaties), dan is dat één klant met elk van die relaties (SCH-023). Een klant heeft toegang tot een relatie als een contactpersoon van die relatie zijn adres heeft en er geen blokkade van dat adres bij die relatie is; Rollen en rechten zegt wat die toegang toestaat.
- **GEG-004 Identificaties die convergeren.** Relatie, contactpersoon, order, stuk en bestand MUST de identificatie van Exact Online als sleutel hebben, en een klant de UUIDv5 van zijn adres, zodat hetzelfde adres altijd dezelfde klant-identificatie geeft. Elke schrijfactie van de koppeling MUST een upsert op die sleutel zijn, zodat een synchronisatie die opnieuw loopt of een pagina opnieuw leest hetzelfde resultaat geeft. Elke identificatie is een eigen type, nooit een kale tekst of UUID.
- **GEG-005 Order, relatie en stukken.** Een order MUST bij de relatie horen in het veld dat ROL-005 noemt; dit model kiest dat veld niet. Een document in Exact Online is een stuk van een order als het diens ordernummer draagt (`SalesOrderNumber`) of aan de order zelf is gekoppeld (`SalesOrders.Document`); een document dat op beide manieren bij dezelfde order hoort, MUST één stuk zijn. Noemt Exact Online bij het document een relatie (`Account`) die niet die van de order is, dan MUST de app het niet houden (ROL-006).
- **GEG-006 Het documenttype bepaalt de soort.** De app MUST een document alleen als stuk houden als zijn documenttype een soort heeft:

werkbon, factuur of document. Een documenttype dat de app niet kent, of dat niet zichtbaar is, MUST NOT worden gehouden, ook niet voor Binnendienst (ROL-006): Exact Online bewaart bij een order ook interne stukken. Tot de Bouwer en het installatiebedrijf de soort van elk documenttype vaststellen (BOUW-002, VRAAG-ROL-2), heeft geen documenttype een soort. Daarna wijzigt de beheerder ze in de Beheeromgeving (ROL-004, ROL-010). Na een wijziging leest de koppeling de documenten opnieuw, zodat wat zichtbaar wordt verschijnt en wat niet meer zichtbaar is verdwijnt. Of de factuur bij een order als document in Exact Online staat, is VRAAG-KOP-2.

- **GEG-007 Bestanden worden doorgegeven, niet bewaard.** De app MUST NOT de inhoud van een bestand bewaren. Opent een klant of medewerker een bestand, dan haalt de koppeling het op bij Exact Online en geeft het door (KOP-005). Werkbonnen en documenten bevatten namen en adressen; zo staat die inhoud op één plek, en is er geen tweede kopie die met Exact Online gelijk moet blijven. Van het bestand houdt de app alleen naam, type en grootte, voor SCH-031 en de grens van KOP-005.
- **GEG-008 De status wordt afgeleid, niet bewaard.** De app MUST `Status` en `DeliveryDate` bewaren zoals Exact Online ze geeft, en de status bij elke weergave daaruit afleiden (STAT-001). De afgeleide status MUST NOT worden opgeslagen: een wijziging van STAT-001 geldt dan meteen voor elke order.
- **GEG-009 Vragen, antwoorden en afsluiten.** Elke order heeft ten hoogste één gesprek. Een vraag schrijft een klant met toegang tot de relatie van de order, een antwoord een binnendienstmedewerker; de tekst is gewone tekst (BUITEN-007, BEV-007), niet leeg en niet langer dan BEV-004 toestaat. Een verstuurde vraag of een verstuurd antwoord MUST NOT worden gewijzigd of verwijderd door een gebruiker (VRG-004). Een vraag is open tot er in hetzelfde gesprek een antwoord na komt of een binnendienstmedewerker het gesprek afsluit (VRG-002). Een antwoord is gezien op het moment dat een klant van die relatie de order voor het eerst opent nadat het er kwam (SCH-021); wie dat was, legt de app niet vast. Het gesprek heeft een volgnummer dat bij elk bericht en elke afsluiting stijgt; een antwoord of afsluiting noemt het volgnummer dat de medewerker zag, en is er intussen iets bij gekomen, dan MUST de app het weigeren en tonen wat er bijkwam (SCH-064).
- **GEG-010 Een blokkade blijft tot de toegang wordt teruggezet.** Een blokkade MUST gelden voor één genormaliseerd e-mailadres bij één relatie, en MUST NOT veranderen door een synchronisatie. Verdwijnt het adres uit Exact Online en komt het later terug bij een contactpersoon van die relatie, dan geldt de blokkade weer (ROL-007).

Zij eindigt alleen door toegang terugzetten, of als haar relatie uit de app verdwijnt.

- **GEG-011 Wat uit Exact Online verdwijnt, verdwijnt uit de app.** Verdwijnt een relatie, contactpersoon, order, stuk of bestand uit Exact Online, dan MUST de app het verwijderen bij de synchronisatie die dat ziet, uiterlijk bij de volledige lezing van de nacht (KOP-004). Heeft geen contactpersoon het adres van een klant meer, dan verwijdert de app die klant met zijn inloglink; zijn vragen blijven bij hun order, met verwijderde contactpersoon als afzender, en de blokkades van zijn adres blijven (GEG-010). Met een order verdwijnen zijn stukken, bestanden, statuswijzigingen en gesprek; met een relatie haar blokkades.
- **GEG-012 Schrijven in één transactie.** Elke schrijfactie die meer dan één rij raakt, MUST in één serializable transactie gebeuren: een pagina van de koppeling met zijn statuswijzigingen en de cursor van Synchronisatie; een vraag of antwoord met zijn e-mail in de outbox (INVAR-007); een afsluiting met het einde van de open vragen; een blokkade of het terugzetten van de toegang met de vastlegging; een wijziging van een documenttype met de vastlegging. Een e-mail gaat pas weg nadat de transactie is vastgelegd. Een transactie die op een conflict stuit, loopt opnieuw en geeft hetzelfde resultaat.
- **GEG-013 De leespaden.** Elke tabel dient minstens één van deze leespaden, en elk leespad heeft zijn index:

Leespad	Wie	Sleutel en volgorde
Een klant bij zijn adres	Klantportaal: Inloggen	uniek op het e-mailadres
De relaties van een klant, zonder geblokkeerde	elk verzoek van een klant (INVAR-003)	contactpersonen per klant, blokkades per e-mailadres en relatie
De orders van een relatie, lopend op geplande datum en eerder nieuwste eerst, per pagina	Klantportaal: Orders	per relatie, op `Status`, geplande datum en orderdatum
Een order op ordernummer of omschrijving, binnen één relatie	Klantportaal: Orders (zoeken)	binnen de orders van die relatie
Orders met een antwoord dat nog niet gezien is	Klantportaal: Orders (Nieuw antwoord)	antwoorden per order zonder gezien op
Eén order met zijn stukken en bestanden	Klantportaal: Order, Binnendienst: Vraag	stukken per order, bestanden per stuk
De statuswijzigingen van een order, nieuwste eerst	Binnendienst: Vraag (SCH-061)	per order, op moment gezien aflopend

Het gesprek van een order	Klantportaal: Order, Binnendienst: Vraag	per order, in volgorde van schrijven
De open vragen, oudste eerst, en hun aantal	Binnendienst: Vragen	op het moment van de oudste open vraag
Beantwoorde en afgesloten vragen, nieuwste eerst	Binnendienst: Vragen	op het moment van het laatste antwoord of de afsluiting
Relaties met hun contactpersonen en blokkades, en zoeken op naam, relatie of e-mailadres	Binnendienst: Klanten	relaties op naam, contactpersonen per relatie; zoeken leest de contactpersonen, een paar duizend rijen (GEG-014)
Een order bij zijn ordernummer	de koppeling, voor GEG-005	uniek op het ordernummer
De documenttypen	de koppeling, de Beheeromgeving	op documenttype
De inloglink van een klant	Klantportaal: Inloggen	de klant-identificatie
De tellingen van een gebeurtenis over een reeks dagen	de maten van Kernproces	per gebeurtenis, op dag aflopend

- **GEG-014 De schaal.** Het model houdt ongeveer 1.200 klanten, 5 binnendienstmedewerkers en 1 beheerder, samen 1.206 personen (AAN-011, de Aanvraag). Het aantal relaties is ten hoogste het aantal contactpersonen. Hoeveel orders een relatie heeft en hoeveel stukken een order, noemt de Aanvraag niet: dat is een open punt voor Dag 0, dat een telling in de administratie van het installatiebedrijf beantwoordt (BOUW-002). Het model hangt er niet van af: elk leespad van GEG-013 is één geïndexeerde leesactie per sleutel, per pagina, behalve het zoeken in Klanten, dat bij deze omvang alle contactpersonen leest; en geen sleutel begint met een oplopende waarde, zodat de kopie zonder ander ontwerp meegroeit met Exact Online.
- **GEG-015 Test data in de Preview, productie vanaf Live.** De Preview MUST alleen de testadministratie van het installatiebedrijf lezen (PRIV-005, INV-008, KOP-011). Bij Live bouwt de koppeling de kopie op uit de administratie in productie; niets uit de Preview gaat mee, ook de documenttypen niet: die stelt de beheerder vast voor de productieadministratie, met de tabel uit de testadministratie als voorstel. De eerste stand die de app van een order ziet, is geen statuswijziging (BUITEN-004).

6. Kernproces

Het kernproces is: **een klant ziet zelf hoe zijn order ervoor staat, met de werkbonnen, de factuur en de documenten erbij.** De vragen over een order en hun antwoorden zijn de Uitbreiding Berichten in deze Build.

De stappen

De stappen zijn die van de Aanvraag, in deze volgorde en met deze nummers, in de woorden van Begrippen.

- **PROC-001** De klant logt in. Scherm: Klantportaal: Inloggen. Reis: REIS-001.
- **PROC-002** Hij ziet de orders van zijn relatie met hun status. Scherm: Klantportaal: Orders. Reis: REIS-002.
- **PROC-003** Hij opent een order, met de werkbonnen, de factuur en de documenten erbij. Scherm: Klantportaal: Order. Reis: REIS-003.
- **PROC-004** Hij stelt een vraag over de order. Scherm: Klantportaal: Order. Reis: REIS-004.
- **PROC-005** Een binnendienstmedewerker antwoordt en de klant krijgt een e-mail. Schermen: Binnendienst: Vragen en Binnendienst: Vraag. Reis: REIS-005. Melding: MEL-005.
- **PROC-006** De klant kiest een moment voor het jaarlijkse onderhoud. Deze stap zit niet in deze Build (BUITEN-003).

De order

- **STAT-001** De app MUST elke order precies één status geven, uit deze tabel. Een waarde die niet in de tabel staat, geeft In behandeling; de app MUST die waarde dan vastleggen voor Beheer.

Status	Code	Uit Exact Online (`SalesOrders`)
Gepland	`Planned`	`Status` 12 (Open) met een `DeliveryDate` van vandaag of later
In behandeling	`InProgress`	`Status` 12 (Open) in elk ander geval: zonder `DeliveryDate`, of met een `DeliveryDate` vóór vandaag; en elke waarde die niet in deze tabel staat
Deels geleverd	`PartlyDelivered`	`Status` 20 (Gedeeltelijk)
Afgerond	`Done`	`Status` 21 (Compleet)
Geannuleerd	`Cancelled`	`Status` 45 (Geannuleerd)

- **STAT-002** De app MUST de geplande datum tonen bij de status Gepland en bij Deels geleverd met een `DeliveryDate` van vandaag of later, en nergens anders. Een datum die voorbij is, belooft niets meer.

- **STAT-003** De app MUST NOT een tweede status naast de ene tonen, en MUST NOT een lege status tonen zoals "status niet beschikbaar" ([22], [21]).
- **STAT-004** Lopend zijn de orders met In behandeling, Gepland of Deels geleverd; Eerder zijn de orders met Afgerond of Geannuleerd.
- **OPEN-001** Vraag aan het installatiebedrijf, vóór ondertekening. Welke waarden `DeliveryStatus` en `InvoiceStatus` hebben, staat niet in de onderzoeksbasis. STAT-001 gebruikt ze daarom niet. Moet een waarde ervan de status veranderen, bijvoorbeeld naar een status voor een geleverde of gefactureerde order, dan wordt dat in STAT-001 geschreven vóór ondertekening.

De vraag

- **VRG-001** Het gesprek van een order staat bij die order, in de volgorde waarin de berichten zijn verstuurd, elk met tijd. Bij een vraag staat de naam van de klant; in het Klantportaal staat bij een antwoord de naam van het installatiebedrijf.
- **VRG-002** Een vraag is open tot een binnendienstmedewerker antwoordt of hem afsluit. Een nieuwe vraag bij die order is weer een open vraag. Bij elke vraag ziet de klant of hij open, beantwoord of afgesloten is.
- **VRG-003** Elke klant van de relatie ziet het gesprek bij de orders van die relatie. Een klant van een andere relatie ziet het nooit.
- **VRG-004** Een vraag of antwoord is na versturen niet te wijzigen of te verwijderen. Een correctie is een nieuw bericht.

Reizen, uitkomsten en maten

Elke reis verdient een uitkomst voor het installatiebedrijf. De app meet wat in de app gebeurt, met de gebeurtenis bij elke maat. Het aantal telefoontjes meet het installatiebedrijf zelf. De nummers tussen haken zijn die van de Onderzoeksbasis.

REIS-001 Inloggen

- App en rol: Klantportaal, klant.
- Uitkomst: binnen zonder wachtwoord.
- Maat en gebeurtenis: het aandeel verstuurde inloglinks dat tot een sessie leidt: `inloglink_verstuurd`, `inloglink_gebruikt`.
- Patroon en bron: inloggen zonder wachtwoord met een link per e-mail, voor accounts die zelden worden gebruikt; één veld, één knop ([23], [20]).
- Klaar-pad: KLAAR-001.

REIS-002 Waar staat mijn order?

- App en rol: Klantportaal, klant.
- Uitkomst: de stand gevonden zonder te bellen.

- Maat en gebeurtenis: het aandeel sessies dat een order opent: `sessie_gestart`, `order_bekeken`. Buiten de app: telefoontjes per dag, tegen de 40 van de Aanvraag.
- Patroon en bron: één status per order met de geplande datum, lopende orders bovenaan ([24], [20], [22]).
- Klaar-pad: KLAAR-006.

REIS-003 Werkbon of factuur nodig

- App en rol: Klantportaal, klant.
- Uitkomst: het stuk zelf geopend, niet opnieuw gevraagd.
- Maat en gebeurtenis: geopende bestanden per soort: `werkbon_geopend`, `factuur_geopend`, `document_geopend`.
- Patroon en bron: de stukken bij de order zelf, niet in aparte lijsten ([26]; [25], marketing en daarom licht gewogen).
- Klaar-pad: KLAAR-010.

REIS-004 Een vraag over een order

- App en rol: Klantportaal, klant.
- Uitkomst: de vraag schriftelijk bij de order, geen telefoontje.
- Maat en gebeurtenis: vragen per bekeken order: `vraag_gesteld`, `order_bekeken`; gelezen antwoorden: `antwoord_gelezen`.
- Patroon en bron: een contactkanaal in het overzicht per opdracht, zoals de peers het tonen ([25]); onduidelijkheid over een order drijft naar contact ([20], [22]). Het bewijs voor deze vorm is dun.
- Klaar-pad: KLAAR-015.

REIS-005 Een vraag beantwoorden

- App en rol: Binnendienst, binnendienstmedewerker.
- Uitkomst: één antwoord met de order ernaast, en de klant krijgt bericht.
- Maat en gebeurtenis: de tijd tot het eerste antwoord (mediaan) en de open vragen aan het eind van de dag, gelezen uit de vragen en antwoorden zelf (VAST-001); `vraag_beantwoord`, `vraag_afgesloten`.
- Patroon en bron: één werklijst met de oudste open vraag bovenaan; e-mail alleen bij een nieuw antwoord, met een directe link (het onderzoek bij de Bouwcheck, §3 patroon 5, bewijs dun; de volgorde is een ontwerpkeuze om de wachttijd te beperken, zonder bron).
- Klaar-pad: KLAAR-023.

REIS-006 Toegang beheren

- App en rol: Binnendienst, beheerder.
- Uitkomst: alleen de juiste mensen kunnen erin.
- Maat en gebeurtenis: geen commerciële maat: `toegang_geblokkeerd`, `toegang_teruggezet`.
- Patroon en bron: toegang volgt de contactpersonen in Exact Online (VKL-003); blokkeren vraagt een bevestiging met de passkey (ROL-010). Geen bron in de onderzoeksbasis.

– Klaar-pad: KLAAR-029.

De zes stappen van de Aanvraag zijn de stappen van PROC-001 tot PROC-006, geen zes fasen van een order: de order toont één status uit Exact Online (STAT-001), geen tijdlijn.

Meten

– **MEET-001** De app MUST elke gebeurtenis van de reizen tellen per dag, zonder persoon, relatie of order, zoals VAST-003 zegt; de soort van een stuk zit alleen in de naam van de gebeurtenis. Een gebeurtenis die per sessie telt (`sessie_gestart`, `order_bekeken`), telt zoals VAST-003 dat voor een sessie regelt.
– **MEET-002** De app MUST NOT analytics van derden of trackingcookies gebruiken. Het installatiebedrijf leest de maten uit de tellingen en uit de vragen en antwoorden, in de export van zijn gegevens (BEH-011).

7. Schermen

– **SCH-001** De Build heeft zeven schermen in twee portalen. Het Klantportaal heeft Inloggen, Orders en Order. Binnendienst heeft Inloggen, Vragen, Vraag en Klanten. Teksten en beelden, Beheeromgeving en Organisatiebeheer zitten in elke Build en tellen niet mee (ADD-006).
– **SCH-002** Het Klantportaal is ontworpen voor Mobiel eerst, Binnendienst voor Desktop eerst. Elk scherm werkt op Mobiel, Tablet en Desktop.
– **SCH-003** Elk scherm opent met een eigen kop, laat één hoofdactie zien en zegt waar de gebruiker daarna heen kan. Elke lege staat zegt wat er is, waar het gebied voor is, en biedt één actie.
– **SCH-004** Is Exact Online niet bereikbaar, of werkt de koppeling niet (KOP-009), dan MUST elk scherm met gegevens uit Exact Online de laatst bekende gegevens tonen, met de tijd waarop ze zijn bijgewerkt, en zeggen dat die niet actueel zijn. Het MUST NOT een lege lijst of alleen een foutmelding tonen alsof er niets is.
– **SCH-005** Een order, stuk of vraag die niet bestaat of niet bij de gebruiker hoort, geeft dezelfde pagina "niet gevonden". De pagina zegt niet welke van de twee het is (ROL-009).

Klantportaal: Inloggen

– **SCH-010** Toont één veld voor het e-mailadres en één knop om een inloglink te sturen. Het veld laat de browser het e-mailadres aanvullen.
– **SCH-011** Na versturen zegt het scherm, voor elk adres hetzelfde: als het adres toegang heeft, staat er een inloglink in de mailbox (BEV-003). Daaronder staat een veld voor de inlogcode uit die e-mail, voor wie de e-mail op een ander apparaat of in een andere browser opent.
– **SCH-012** Een inloglink of een juiste inlogcode opent Orders, of de pagina waarvoor de klant moest inloggen, zoals de order uit een e-mail.

- **SCH-013** Staten: leeg veld of geen geldig e-mailadres (het scherm zegt wat er mist en houdt de invoer); link verstuurd, met het veld voor de inlogcode; inlogcode onjuist (het scherm zegt dat, en houdt de invoer); te vaak een onjuiste inlogcode, of te veel aanvragen (het scherm zegt dat een nieuwe link nodig is, en wanneer dat weer kan, BEV-002, BEV-004); link gebruikt of verlopen (een pagina die dat zegt, met één knop voor een nieuwe link); sessie verlopen (dit scherm, met de pagina waar de klant was als bestemming).
- **SCH-014** Opent een klant de inloglink in een andere browser dan die hem aanvroeg, dan zegt een pagina dat de link alleen werkt in de browser waarin hij hem aanvroeg, en dat hij daar de inlogcode uit de e-mail kan invullen. Die pagina MUST NOT de inlogcode tonen.

Bron: de contactpersonen met hun e-mailadres uit de koppeling met Exact Online, en de blokkades die de beheerder invoert.

Klantportaal: Orders

- **SCH-020** Toont de orders van de relatie van de klant, eerst Lopend, dan Eerder (STAT-004). Lopende orders staan op geplande datum, de eerste bovenaan, en orders zonder getoonde datum daarna; eerdere orders staan nieuwste eerst. Een relatie heeft altijd minstens één order, want anders is zij geen relatie en kan niemand bij haar inloggen (ROL-002, ROL-007).
- **SCH-021** Elke order toont ordernummer, omschrijving, status (STAT-001) en de geplande datum waar STAT-002 die toont. Een order met een antwoord dat nog geen klant van de relatie opende, draagt het label Nieuw antwoord (GEG-009).
- **SCH-022** Een zoekveld vindt een order op ordernummer of omschrijving.
- **SCH-023** Staat de klant met zijn e-mailadres bij meer dan één relatie, dan kiest hij boven de lijst de relatie, en toont de lijst alleen haar orders. Bij één relatie is er geen keuze.
- **SCH-024** Staten: laden; geen lopende orders (op de plek van Lopend zegt het scherm dat er nu geen lopende order is, een nieuwe order hier verschijnt zodra hij in Exact Online staat, en hoe de klant het installatiebedrijf bereikt, uit Teksten en beelden; de eerdere orders staan eronder); geen zoekresultaat (met een knop om het zoeken te wissen); Exact Online niet bereikbaar (SCH-004).

Bron: de koppeling met Exact Online (orders, status, geplande datum); de antwoorden die binnendienstmedewerkers invoeren (het label Nieuw antwoord).

Klantportaal: Order

- **SCH-030** Toont bovenaan ordernummer, omschrijving, status en geplande datum (STAT-001, STAT-002), daaronder de orderdatum en,

bij meer dan één relatie, de naam van de relatie. Op Mobiel staat onder de status een link naar het veld voor een vraag.
- **SCH-031** Toont de stukken bij de order in drie groepen, in deze volgorde: werkbonnen, factuur, documenten. Elke groep staat er altijd; een groep zonder stukken zegt dat er nog geen staat. Elk stuk toont onderwerp en datum, en elk bestand van het stuk staat op een eigen regel met zijn bestandstype en grootte; elk bestand opent met één stap. Alleen stukken waarvan het documenttype een soort heeft, staan erin (GEG-006, ROL-006).
- **SCH-032** Toont het gesprek van de order (VRG-001, VRG-002), met daaronder een veld voor een vraag en één knop om hem te versturen. Na versturen staat de vraag direct onderaan, met tijd, en zegt het scherm dat de klant een e-mail krijgt als er een antwoord is.
- **SCH-033** Staten: laden; een order zonder stukken (elke groep zegt dat er nog niets staat, en het veld voor een vraag staat eronder); een bestand dat nu niet te openen is, ook als het te groot is of het dagbudget op is (dat zegt het scherm, bij dat bestand, en de rest blijft bruikbaar, KOP-005, KOP-007); leeg vraagveld (de knop verstuurt niets en het scherm zegt wat er mist); een te lange vraag (het scherm zegt hoeveel tekens mogen, en de tekst blijft staan, GEG-009); te veel vragen op een dag (het scherm zegt dat, en de tekst blijft staan, BEV-004); versturen mislukt (de tekst blijft staan, met een knop om opnieuw te versturen); Exact Online niet bereikbaar (SCH-004); niet gevonden (SCH-005).

Welke documenttypen een werkbon, een factuur of een document zijn, regelen GEG-006 en ROL-006 (VRAAG-ROL-2).

Bron: de koppeling met Exact Online (de order, zijn status en zijn stukken met hun bestanden); de vragen die klanten invoeren en de antwoorden die binnendienstmedewerkers invoeren.

Binnendienst: Inloggen

- **SCH-040** Toont één knop om in te loggen met een passkey (BEV-006). Er is geen veld voor een wachtwoord of een e-mailadres, en Binnendienst stuurt geen inloglink. Onder de knop staat voor wie op dit apparaat geen passkey heeft: een passkey die het eigen wachtwoordbeheer synchroniseert, werkt op elk apparaat; anders vraagt hij de beheerder om een nieuwe uitnodiging in Organisatiebeheer.
- **SCH-041** Alleen een medewerker kan hier inloggen. Een klant kan hier niet inloggen (ROL-008).
- **SCH-042** Na het inloggen opent Vragen, of de pagina waarvoor de medewerker moest inloggen, zoals de vraag uit een e-mail (BEV-014).
- **SCH-043** Staten: inloggen afgebroken of geweigerd (het scherm zegt dat, met de knop om het opnieuw te proberen en de uitleg van

SCH-040 voor wie geen passkey heeft); de eerste inlog van de beheerder met één passkey (het scherm vraagt een tweede passkey op een ander apparaat, en hij gaat pas verder als die er is, BEV-006); sessie verlopen (dit scherm, met de pagina waar de medewerker was als bestemming).

Bron: de medewerkers die de beheerder uitnodigt in Organisatiebeheer, met hun passkey.

Binnendienst: Vragen

- **SCH-050** Toont de orders met een open vraag, de oudste open vraag bovenaan. Elke regel toont relatie, ordernummer, naam van de klant, het begin van de vraag en sinds wanneer hij open staat.
- **SCH-051** Een keuze boven de lijst toont in plaats daarvan de beantwoorde en afgesloten vragen, nieuwste eerst, met wie antwoordde of afsloot.
- **SCH-052** De navigatie van Binnendienst toont het aantal open vragen naast Vragen.
- **SCH-053** Staten: laden; geen open vragen (dat zegt het scherm, met de keuze voor beantwoorde en afgesloten vragen).

Bron: de vragen die klanten invoeren en de antwoorden die binnendienstmedewerkers invoeren; relatie en ordernummer uit de koppeling met Exact Online.

Binnendienst: Vraag

- **SCH-060** Toont het gesprek van één order (VRG-001), met de naam van de binnendienstmedewerker bij elk antwoord, en daaronder een veld voor een antwoord en één knop om het te versturen.
- **SCH-061** Toont de order zoals de klant hem ziet: status, geplande datum en stukken (SCH-030, SCH-031). Daaronder de statuswijzigingen van de order (VAST-002), nieuwste eerst, elk met de datum waarop de app haar zag, het veld en de oude en de nieuwe waarde. Op Desktop staan order en gesprek naast elkaar; op Tablet en Mobiel staat het gesprek eerst.
- **SCH-062** Een tweede knop sluit de open vraag af zonder antwoord (Afsluiten), na een bevestiging.
- **SCH-063** Na versturen of afsluiten zegt het scherm wat er gebeurde en biedt het één knop naar de volgende open vraag, of naar Vragen als er geen meer is.
- **SCH-064** Staten: laden; leeg antwoordveld (de knop verstuurt niets en het scherm zegt wat er mist); een te lang antwoord (het scherm zegt hoeveel tekens mogen, en de tekst blijft staan, GEG-009); een collega antwoordde of sloot af terwijl de medewerker typte (het scherm toont dat, de eigen tekst blijft staan, en versturen vraagt dan om bevestiging); versturen mislukt (de tekst blijft staan, met een knop om opnieuw te versturen); niet gevonden (SCH-005).

Bron: de vragen die klanten invoeren en de antwoorden die binnendienstmedewerkers invoeren; de order, zijn stukken en zijn statuswijzigingen uit de koppeling met Exact Online.

Binnendienst: Klanten

- **SCH-070** Toont de relaties uit Exact Online met hun contactpersonen. Elke contactpersoon toont naam, e-mailadres en toegang (Kan inloggen of Geblokkeerd); bij Geblokkeerd ook wie blokkeerde en wanneer.
- **SCH-071** Een zoekveld vindt een contactpersoon op naam, relatie of e-mailadres.
- **SCH-072** Bij elke contactpersoon met Kan inloggen staat voor de beheerder een knop Blokkeren; bij Geblokkeerd een knop Toegang terugzetten. Een blokkade geldt voor dat e-mailadres bij die relatie (GEG-010). Blokkeren vraagt een bevestiging die zegt dat de klant daarna bij die relatie niet meer kan inloggen, ook als zijn adres later opnieuw in Exact Online staat; de bevestiging is die met de passkey van ROL-010. Na de bevestiging toont de regel direct de nieuwe toegang. Een binnendienstmedewerker ziet geen van beide knoppen (ROL-004).
- **SCH-073** Een contactpersoon die uit Exact Online verdwijnt, of geen e-mailadres meer heeft, staat niet meer in Klanten (GEG-002, GEG-011). Zijn blokkade blijft: staat het adres weer bij een contactpersoon van die relatie, dan toont zijn regel Geblokkeerd.
- **SCH-074** Staten: laden; geen zoekresultaat (met een knop om het zoeken te wissen, en de uitleg dat een persoon hier alleen staat als hij in Exact Online een e-mailadres heeft bij een relatie met een verkooporder); Exact Online niet bereikbaar (SCH-004).

Bron: de koppeling met Exact Online (relaties en contactpersonen met hun e-mailadres); de blokkades die de beheerder invoert.

8. Koppeling en import

Koppeling met Exact Online

De app heeft één koppeling: zij leest uit één administratie in Exact Online en schrijft er niets in.

- **KOP-001 Eén administratie, alleen lezen.** De app MUST lezen uit één administratie van Exact Online, via de REST API (`/api/v1/{division}/…`): verkooporders (`salesorder/SalesOrders`, met de sync-variant `sync/SalesOrder/SalesOrderHeaders`), documenten bij een order (`documents/Documents`, via `SalesOrderNumber`, met de bestanden via `DocumentAttachments`), contactpersonen (`crm/Contacts`) en relaties (`crm/Accounts`) (Exact Online REST API, resourceoverzicht en de pagina's van SalesOrders, Documents en Contacts, ongedateerd). De code die Exact Online aanroept MUST alleen GET-verzoeken kunnen maken: een ander verzoek bestaat in de app niet (BUITEN-001).

- **KOP-002 Alleen de nodige velden.** Elk verzoek MUST alleen de velden vragen die het Domeinmodel noemt. De app MUST NOT `Phone`, `Mobile` of `ModifierFullName` lezen (GEG-002, BUITEN-008).
- **KOP-003 Registratie en scopes.** De hoofdgebruiker van het installatiebedrijf registreert de app in het Exact App Center, in een abonnement op naam van het installatiebedrijf, met de scopes "Sales orders", "Organization documents" en "Crm accounts", en geen andere (Exact Online REST API, ongedateerd; Apideck, Exact Online configuration, ongedateerd). Een app voor de eigen administratie heeft geen review van Exact nodig (Exact Knowledge Base, App publication procedure, ongedateerd; Apideck, ongedateerd). De client-ID en het client-secret komen alleen via het geheimenformulier (WK-003). De bronnen noemen geen scope die alleen lezen toestaat (**VRAAG-KOP-1**: biedt Exact Online een scope of een gebruikersrol die alleen lezen toestaat?); tot die er is, maakt KOP-001 de app alleen-lezend. Het account in Exact Online dat de koppeling autoriseert, SHOULD alleen rechten hebben op verkooporders, documenten en relaties, want Exact Online beperkt de toegang ook tot de rechten van die gebruiker (Apideck, ongedateerd).
- **KOP-004 Synchroniseren.** De app MUST elke 5 minuten de wijzigingen lezen via de sync-endpoints van verkooporders, documenten, contactpersonen en relaties, zodat een wijziging in Exact Online binnen 10 minuten in de app staat (INVAR-005); en elke nacht alle contactpersonen en relaties via de bulk-endpoints (1.000 records per pagina; Exact Online REST API, ongedateerd; Chift, ongedateerd). Wat in die volledige lezing ontbreekt, verwijdert de app (GEG-011), en de toegang die erop steunde eindigt (ROL-007). De app gebruikt geen webhooks: `Status` van een verkooporder heeft er geen (Exact Online REST API, SalesOrders, ongedateerd), een webhook zegt niet wat er veranderde, zodat er toch een GET volgt (Hookdeck, ongedateerd), en een webhook vraagt de extra scope "Organization administration" en een adres dat iedereen op internet kan aanroepen. Elke wijziging van de status die een synchronisatie ziet, legt de app vast zoals Vastleggen en audit zegt (VAST-002, BUITEN-004).
- **KOP-005 Stukken op verzoek, bestanden niet bewaard.** De app MUST van een stuk alleen de gegevens bewaren die het Domeinmodel noemt, nooit de inhoud van zijn Bestand (GEG-007). Opent iemand een stuk, dan toetst de server ROL-004 en ROL-006, haalt het Bestand bij Exact Online op en geeft het meteen door aan de browser, tot 25 MB. Zo blijft Exact Online de bron (BUITEN-001, VKL-002), bewaart de app geen kopie van werkbonnen en facturen met namen en adressen (AVG-004), en groeit er geen opslag buiten de basis van Beheer (BEH-008).

- **KOP-006 Tokens.** De app MUST OAuth 2.0 met de authorization-code flow gebruiken. Een access token is 10 minuten geldig en pas te vernieuwen na 9 minuten en 30 seconden; eerder vernieuwen geeft een fout (Apideck; Nango; Hookdeck; Exact Knowledge Base, Get/use access tokens; alle ongedateerd). De app vernieuwt het daarna, en nooit tegelijk met een andere vernieuwing. Een refresh token is eenmalig te gebruiken en verloopt na 30 dagen zonder gebruik (Apideck; Exact Knowledge Base; Microsoft Power Users, "Old refresh token used"; alle ongedateerd). De app MUST elk nieuw refresh token in de geheimenopslag schrijven voordat zij het nieuwe access token gebruikt (BEV-009). Lukt dat niet, dan stopt de synchronisatie en geldt KOP-009. Het access token staat alleen in het geheugen.
- **KOP-007 Limieten.** Exact Online staat per app en per administratie 60 calls per minuut toe en 5.000 calls per dag, en per administratie een plafond voor alle apps samen: 20.000 calls per dag bij Essentials, Plus en Professional, 30.000 calls per dag bij Premium. Dat zijn de limieten die nu gelden, met de ingangsdatum die [11] noemt ([11]; Barcode Scan, ongedateerd; Apideck, ongedateerd). Parallelle calls zijn niet toegestaan (Apideck, ongedateerd). De app MUST één call tegelijk doen, de headers `X-RateLimit-Minutely-Remaining` volgen (Peliqan, ongedateerd), na een 429 wachten tot de volgende minuut, en zelf niet meer dan 4.000 calls per dag doen, waarvan 1.500 calls per dag voor KOP-004 vrij blijven: vier sync-endpoints in elke ronde van KOP-004 zijn 1.152 calls per dag, en de lezing van de nacht vraagt er enkele. Is het dagbudget op, dan opent een stuk die dag niet meer en zegt Order dat bij dat stuk (SCH-033); de synchronisatie gaat door. De app gebruikt de XML-API niet, want daar telt één call als 50 ([11]).
- **KOP-008 Fouten en wachttijden.** Na ongeveer 10 foutieve calls per uur blokkeert Exact Online een endpoint voor de rest van het uur (Apideck; Exact Support, API rate limits; beide ongedateerd). De app MUST een endpoint de rest van het uur niet meer aanroepen na 3 foutieve calls per uur op dat endpoint. Elke call aan Exact Online heeft een wachttijd van hooguit 30 seconden.
- **KOP-009 Als Exact Online niet antwoordt.** Is Exact Online niet bereikbaar, of werkt de koppeling niet meer, dan MUST elk scherm met gegevens uit Exact Online de stand van de laatste gelukte synchronisatie tonen, met haar tijd, en zeggen dat die niet actueel is; het MUST NOT een lege lijst tonen alsof er geen orders zijn (SCH-004). De beheerder krijgt er een e-mail over (Meldingen) en ziet de stand van de koppeling in de Beheeromgeving, waar hij de koppeling opnieuw maakt (ROL-010). Het installatiebedrijf kan de app in Exact Online op elk moment intrekken; dan geldt dit ook.

- **KOP-010 Testtoegang vóór Dag 0** (BC-005, WK-001 item 3 en 4). Exact Online heeft geen sandbox (Apideck; Cyclr, Exact Setup; beide ongedateerd). Het installatiebedrijf MUST de testadministratie in een ontwikkelaarsabonnement van Exact Online zetten, op zijn naam en voor zijn rekening (VKL-005), niet in een proefperiode: een proefperiode loopt af terwijl de Preview en elke herstelling in het Bugvenster de testadministratie nog nodig hebben (INV-008, PRIV-005). De hoofdgebruiker registreert de app in dat abonnement (KOP-003), of geeft daar het recht "Manage apps" (Genkgo, ongedateerd); de gegevens komen via het geheimenformulier. Een testadministratie bewijst niet dat het eigen pakket van het installatiebedrijf verkooporders heeft; dat bevestigt het installatiebedrijf vóór ondertekening. Vóór Start toetst de Bouwer in de testadministratie: (a) `SalesOrders` geeft de testorders; (b) bij minstens één order staan een werkbon en een factuur als document, te vinden via `SalesOrderNumber`; (c) er zijn contactpersonen met een e-mailadres bij een relatie met een verkooporder. Faalt een van de drie, dan is de Build niet Startklaar (WK-001).
- **KOP-011 Test en productie gescheiden.** De Preview MUST alleen de testadministratie lezen, met de gegevens van de testregistratie (INV-008, GEG-015). De gegevens voor de administratie in productie komen via het geheimenformulier op het moment dat Bouwplan per dag noemt, en staan alleen op de productieserver.

Open punten, naast VRAAG-ROL-1 en VRAAG-ROL-2 (vóór ondertekening) en VRAAG-KOP-1 (Dag 0):

- **VRAAG-KOP-2** Komt de factuur bij een order als document via `Documents`, of alleen via een ander endpoint? Een ander endpoint vraagt misschien een extra scope (KOP-003); de bronnen zeggen het niet.
- **VRAAG-KOP-3** Meldt een sync-endpoint ook dat een contactpersoon of relatie is verwijderd? Zo niet, dan ziet de app een verwijdering pas bij de volledige lezing van de nacht (KOP-004, Beveiliging, restrisico 3).
- **VRAAG-KOP-4** Telt het ophalen van een bestand via `DocumentAttachments` als één call? KOP-007 rekent er één call voor.
- **VRAAG-KOP-5** Welk pakket heeft het installatiebedrijf: Essentials, Plus, Professional of Premium? Het plafond van de administratie hangt ervan af (KOP-007), en de app deelt het met de andere apps van het installatiebedrijf (VKL-005).

Import

- **IMP-001 Geen importbestand.** Deze Build importeert geen bestand (BUITEN-002). De ongeveer 1.200 contactpersonen die de Aanvraag als CSV-export uit Exact Online noemde, met bedrijf, naam, e-mailadres en telefoonnummer, komen via de koppeling met Exact Online, als contactpersoon met zijn relatie (Domeinmodel).

- **IMP-002 Waarom niet.** Appwinst importeert alleen een schoon bestand: één rij per record, kolommen met een naam, geen opschoning door Appwinst (NIET-001, N4). Hier vraagt schoon ook een sleutel per rij die de contactpersoon aan zijn relatie in Exact Online koppelt: de relatiecode. De CSV noemt alleen de bedrijfsnaam, en een contactpersoon op naam aan een relatie koppelen is opschoning (twee relaties met dezelfde naam, een naam die anders gespeld is). De koppeling leest dezelfde contactpersonen met de identificatie van hun relatie, en houdt ze actueel: wie het installatiebedrijf in Exact Online toevoegt, kan inloggen; wie verdwijnt, niet meer (GEG-011). Een eenmalig bestand doet dat niet.
- **IMP-003 Waar elke kolom van de CSV nu vandaan komt.**

Kolom in de CSV	In de app	Via
bedrijf	De relatie van de contactpersoon	De identificatie van zijn relatie in Exact Online, niet de naam
naam	De naam van de contactpersoon	De koppeling
e-mailadres	Het e-mailadres van de contactpersoon, en zo de klant	De koppeling; welk e-mailveld van Exact Online, `Email` of `BusinessEmail`, staat in Bijlage: configuratiewaarden
telefoonnummer	Niets	Niet gelezen (GEG-002, BUITEN-008)

- **IMP-004 Niets aan te leveren.** Het installatiebedrijf levert op Dag 0 geen bestand aan, en niemand maakt in de app een klant aan. Een contactpersoon krijgt toegang alleen doordat hij in Exact Online met een e-mailadres bij een relatie met een verkooporder staat (VKL-003); de beheerder kan die toegang blokkeren (GEG-010).

9. Meldingen

- **MEL-001** De app meldt alleen per e-mail (BUITEN-009).
- **MEL-002** De app MUST elke e-mail versturen vanaf een adres op het eigen subdomein `mail.voorbeeld.example`, met SPF, DKIM en DMARC die op dat domein zijn afgestemd, zoals COM-010 het voor Appwinst regelt. Dat subdomein neemt geen mail aan (een null MX, RFC 7505), zoals Appwinst het voor haar eigen meldingen doet (COM-011, de terugvaloplossing in §27 van de Appwinst-specificatie).
- **MEL-003** Elke e-mail MUST een korte samenvatting bevatten en eindigen met één link, met verder alleen de afsluiting en de bedrijfsgegevens van het installatiebedrijf; de e-mail met de inloglink

bevat ook de inlogcode (BEV-002). Een e-mail MUST NOT de tekst van een vraag of antwoord bevatten, en MUST NOT een stuk als bijlage meesturen (zoals COM-010).

- **MEL-004** Inloglink. Wie op Klantportaal: Inloggen een link aanvraagt voor een adres met toegang, krijgt direct een e-mail met de inloglink en de inlogcode. Deze e-mail wordt nooit uitgesteld. Medewerkers loggen in met een passkey en krijgen geen inloglink (BEV-006).
- **MEL-005** Nieuw antwoord. Verstuurt een binnendienstmedewerker een antwoord, dan krijgt elke klant met een open vraag bij die order één e-mail met het ordernummer en een link naar de order.
- **MEL-006** Nieuwe vraag. Wordt een vraag gesteld bij een order zonder open vraag, dan krijgt elke binnendienstmedewerker één e-mail met het ordernummer, de relatie en een link naar Vraag. Een volgende vraag bij die order, terwijl er een open vraag is, stuurt geen e-mail.
- **MEL-007** Een antwoord op een e-mail. De app ontvangt geen e-mail. Een antwoord op een e-mail van de app komt terug bij de afzender, omdat het subdomein geen mail aanneemt (MEL-002), en zijn inhoud bereikt de app nooit. Wie een vraag heeft, volgt de link waarmee elke e-mail eindigt (MEL-003).
- **MEL-008** De app stuurt geen andere e-mail dan die van MEL-004, MEL-005, MEL-006 en MEL-009. Afsluiten (SCH-062), blokkeren en toegang terugzetten (SCH-072) sturen geen e-mail.
- **MEL-009** De koppeling. Lukt de synchronisatie met Exact Online niet meer (KOP-009), dan krijgt de beheerder één e-mail met een link naar de Beheeromgeving; lukt zij daarna weer, dan krijgt hij er één die dat zegt. Tussen die twee komt er geen e-mail over de koppeling.

10. Vastleggen en audit

De app legt vast wat een stap, een maat of de verantwoording van een handeling nodig heeft, en niet meer. Het installatiebedrijf antwoordde in de Aanvraag dat het niet achteraf hoeft aan te tonen wie wat veranderde; deze Build heeft daarom geen Audittrail (BUITEN-012).

- **VAST-001 Wat de app vastlegt.** Per vastlegging: wie of wat haar maakt en wanneer, waar zij staat in het Domeinmodel, en hoe lang zij blijft.

Wat	Wie of wat, en wanneer	Waar, en hoe lang
Een wijziging van `Status` of `DeliveryDate` van een order	De koppeling, bij de synchronisatie die haar ziet	Statuswijziging; zolang de order in de app staat
Een vraag: wie hem schreef en wanneer	De klant die hem stelt, bij het versturen	Vraag; VAST-007
Een antwoord: wie het schreef, wanneer, en wanneer een klant van de	De binnendienstmedewerker, bij het versturen; het zien	Antwoord; VAST-007

relatie het voor het eerst zag	door de app, bij het eerste openen van de order	
Een afsluiting: wie afsloot en wanneer	De binnendienstmedewerker, bij het afsluiten	Afsluiting; VAST-007
Blokkeren en toegang terugzetten: welk e-mailadres, bij welke relatie, door wie, wanneer	De beheerder, bij de handeling	Blokkade, met een vastlegging per handeling; VAST-007
Een wijziging van een documenttype: welk, van welke soort naar welke, door wie, wanneer	De beheerder, bij de handeling	Documenttype, met een vastlegging per handeling; zolang de app draait, de medewerker alleen bij zijn identificatie (VAST-004)
Een aangevraagde inloglink, en of hij gebruikt is	De app, bij aanvragen en gebruiken	Inloglink; VAST-007
Hoe vaak elke gebeurtenis van Kernproces per dag voorkomt (MEET-001)	De app, bij de gebeurtenis	Telling; 13 maanden: genoeg om een jaar met het vorige te vergelijken; geen persoonsgegevens (VAST-003)
Hoeveel vragen aan het eind van een dag open staan	De app, dagelijks, aan het eind van de dag	Telling; als de andere tellingen
Wanneer de koppeling voor het laatst slaagde, en de laatste fout	De koppeling, bij elke synchronisatie	Synchronisatie; alleen de laatste stand
Een waarde van `Status` die STAT-001 niet kent, met de sleutel van de order	De koppeling, bij de synchronisatie die haar ziet	Het serverlog (VAST-006); als het serverlog (PRIV-007)
Wie een tekst of beeld veranderde	Teksten en beelden, bij publiceren	Die module (ADD-006); zoals die module het bewaart
Wie een medewerker uitnodigde, een rol gaf of verwijderde	Organisatiebeheer, bij de handeling	Die module (ADD-006); zoals die module het bewaart

– **VAST-002 Statusgeschiedenis vanaf Live.** Exact Online bewaart alleen de huidige status van een order, niet de geschiedenis (Exact Online REST API, SalesOrderSalesOrders, ongedateerd). De app MUST daarom

elke wijziging die zij ziet zelf vastleggen, vanaf de eerste synchronisatie met de administratie in productie (GEG-015, BUITEN-004), met het moment waarop de app haar zag en het moment dat Exact Online als laatste wijziging noemt. Binnendienst: Vraag toont ze (SCH-061). Het moment gezien ligt ten hoogste één synchronisatie na de wijziging (KOP-004). Een wijziging die tussen twee synchronisaties ontstaat en weer verdwijnt, ziet de app niet. Wie de order in Exact Online wijzigde, legt de app niet vast (GEG-002).

- **VAST-003 Niet vastgelegd: wie wat bekeek.** De app MUST NOT vastleggen welke klant welke order bekeek of welk bestand opende, en een gebeurtenis van Kernproces MUST NOT een persoon, relatie of order dragen. De maten van Kernproces lezen de app uit Tellingen per gebeurtenis per dag, en een stuk dat geopend wordt telt per soort. Een maat die per sessie telt, telt per sessie hoogstens één gebeurtenis. De tijd tot het eerste antwoord leest de app uit de vragen en antwoorden zelf. Van het lezen legt de app alleen per antwoord vast wanneer het gezien is, zonder door wie (GEG-009, SCH-021). Geen stap heeft meer nodig (AVG art. 5 lid 1 onder c en art. 25 [27]).
- **VAST-004 Personen alleen bij hun identificatie.** Een vastlegging MUST een persoon noemen bij zijn identificatie, niet bij zijn naam; de naam komt bij het lezen uit de contactpersoon of uit Organisatiebeheer. Verdwijnt een persoon, dan blijft de vastlegging, met verwijderde contactpersoon of verwijderde medewerker waar de naam stond, zoals PRIV-009 het voor Appwinst zelf regelt. De enige uitzondering is de blokkade: zij noemt het e-mailadres, omdat zij moet blijven gelden als het adres terugkomt (GEG-010).
- **VAST-005 Geen Audittrail.** De vastleggingen zijn niet aan elkaar geketend, en er is geen aparte export van. De hele dataset van de app, vastleggingen inbegrepen, is op elk moment te exporteren (BEH-011). Een audittrail met export is de Uitbreiding Audittrail (BUITEN-012).
- **VAST-006 Geen inhoud in logboeken.** Server- en toegangslogs MUST NOT de tekst van een vraag of antwoord, een token, een inlogcode, een inloglink, een naam, een e-mailadres of de inhoud van een bestand bevatten (BEV-009). Zij en de back-ups volgen de termijnen van PRIV-007.
- **VAST-007 Bewaren naar doel.** Elk persoonsgegeven blijft zolang zijn doel het nodig heeft (AVG art. 5 lid 1 onder e [27]). Dit is de ene plek voor die termijnen; AVG-003 noemt het doel en verwijst hierheen, en houdt alleen de termijnen van het IP-adres, de logs en de back-ups.

Gegeven	Doel	Bewaard
Naam en e-mailadres van een contactpersoon, en de klant	Inloggen, en de vragen van de relatie	Zolang ze in Exact Online staan; verwijderd bij de synchronisatie die ziet

		dat ze er niet meer staan (GEG-011)
Een blokkade: het e-mailadres, de relatie, wie blokkeerde en wanneer	De toegang blijvend weigeren (ROL-007)	Tot de beheerder de toegang terugzet, of tot de relatie uit de app verdwijnt (GEG-010)
Een vraag of antwoord, met wie en wanneer, en een afsluiting	De vraag afhandelen, en hem bij een volgende vraag of het volgende jaarlijkse onderhoud terugvinden	24 maanden na het laatste bericht of de laatste afsluiting in het gesprek van die order, of korter als de order uit Exact Online verdwijnt (GEG-011)
Een inloglink	Inloggen	Tot hij gebruikt is, door een nieuwe aanvraag vervalt of verloopt (BEV-002)
Naam, e-mailadres en rol van een medewerker	Inloggen in Binnendienst, en bij een antwoord	Tot de beheerder hem verwijdert in Organisatiebeheer
De inhoud van een stuk	Tonen	Niet bewaard (GEG-007)

De termijn voor een gesprek dekt twee rondes van het jaarlijkse onderhoud, zodat een binnendienstmedewerker een vraag over een order bij het volgende bezoek terugvindt. Na de termijn MUST de app het gegeven verwijderen: wat GEG-011 noemt bij de synchronisatie die het ziet, en een gesprek met zijn afsluitingen binnen een dag na het einde van zijn termijn, door een opruimtaak. Een verwijdering is definitief; de back-ups volgen PRIV-007. Deze termijnen staan in de verwerkersovereenkomst (PRIV-007, de rij Client app production data); een andere termijn is een nieuwe versie van dit document (ALG-005). Eindigt de dienst, dan geldt BEH-012.

11. Beveiliging

De app volgt de basis van Appwinst voor elke client-app (SEC-017) en toetst beide apps aan OWASP ASVS 5.0, niveau 2 (Conformiteit). Elke grens die een aanvaller raakt, staat hieronder met zijn dreigingsmodel; daaronder de eisen die ze dichten.

Dreigingsmodel per grens

G1 Klantportaal: de browser van een klant en de server.

1. Wat een aanvaller wil: de orders, stukken en vragen van een relatie; de sessie of de inloglink van een klant.

2. Wie: een klant van een andere relatie met een geldige sessie; iemand die een inlog-e-mail doorgestuurd krijgt of een mailbox meeleest; een bot die e-mailadressen uitprobeert; een oud-contactpersoon.
3. De grens: naar binnen een e-mailadres, een inlogcode, sleutels van orders, stukken en vragen, een bestemming na het inloggen, en de tekst van een vraag; naar buiten de gegevens van de eigen relatie. Op de grens toetst de server de sessie, de rol en de relatie (ROL-001), bij elk gegeven het eigendom (ROL-004), de lengte van de invoer, de bestemming (BEV-014) en de herkomst van het verzoek (BEV-001).
4. STRIDE: **S** een inloglink logt alleen in de browser in die hem vroeg (BEV-002). **T** een klant wijzigt geen gegeven uit Exact Online; de tekst van een vraag wordt als tekst getoond (BEV-007). **R** wie een vraag stelde en wanneer, ligt vast (Vastleggen en audit). **I** een sleutel raden geeft niets (ROL-009); of een e-mailadres bekend is, lekt niet (BEV-003). **D** inlogaanvragen, vragen en geopende stukken per klant zijn begrensd (BEV-004). **E** de browser draagt geen rol; een sessie van het Klantportaal geldt niet op Binnendienst (ROL-008).
5. Misbruik: een klant opent stukken tot het dagbudget van Exact Online op is (BEV-004, KOP-007); iemand vraagt steeds inloglinks aan voor het adres van een ander (BEV-004); een vraag met een link om een medewerker te misleiden (BEV-007); een inloglink met een bestemming op een andere site (BEV-014).
6. Invariant: geen antwoord van het Klantportaal bevat een gegeven van een relatie waartoe de ingelogde persoon op dat moment geen toegang heeft.

G2 Binnendienst: de browser van een medewerker en de server.

1. Wat een aanvaller wil: alle vragen en antwoorden, de lijst van klanten, een blokkade opheffen, de koppeling.
2. Wie: een klant die zich als medewerker voordoet; een vertrokken medewerker; iemand die de beheerder phisht of een mailbox van een medewerker meeleest.
3. De grens: naar binnen antwoorden, blokkades, uitnodigingen en instellingen; naar buiten vragen, orders bij een vraag en klanten. Op de grens toetst de server de passkey-sessie, de rol (ROL-004) en voor de handelingen van ROL-010 een verse bevestiging.
4. STRIDE: **S** medewerkers loggen in met een passkey, die niet te phishen is, en er is geen terugval naar een inloglink (BEV-006). **T** een antwoord wordt als tekst getoond (BEV-007). **R** wie blokkeerde, toegang terugzette, uitnodigde of antwoordde, en wanneer, ligt vast (Vastleggen en audit). **I** een medewerker ziet een order alleen bij een vraag (ROL-004). **D** niet van toepassing buiten BEV-004: er zijn vijf medewerkers en geen open aanmelding. **E** meer rechten krijgt een

medewerker alleen via Organisatiebeheer, met een passkey-bevestiging (ROL-010).

5. Misbruik: een medewerker die vertrekt en nog een open sessie heeft (ROL-007); een beheerder die per vergissing iemand blokkeert (hij zet de toegang terug, ROL-004); iemand die zich voordoet als een medewerker die zijn passkey kwijt is, om een uitnodiging te krijgen (alleen de beheerder nodigt opnieuw uit, met zijn passkey; BEV-006).
6. Invariant: alleen een beheerder met een passkey-bevestiging van de laatste 10 minuten verandert een blokkade, een rol, een uitnodiging, de documenttypen per soort of de koppeling.

G3 De server en Exact Online.

1. Wat een aanvaller wil: het refresh token en het client-secret, want daarmee leest hij de hele administratie binnen de scopes; een schrijfactie in Exact Online.
2. Wie: wie de server, een log of een back-up leest; een vervalste of kapotte respons; een fout in de app.
3. De grens: naar buiten alleen GET-verzoeken met een access token; naar binnen orders, documenten, contactpersonen, relaties en bestanden. De server toetst de host, het type en de grootte van elke respons.
4. STRIDE: **S** de app praat alleen via HTTPS met de host van Exact Online, en haalt een adres dat Exact Online teruggeeft alleen op als het op die host staat (BEV-010). **T** elke respons wordt op vorm en grootte getoetst (KOP-005, BEV-008). **R** niet van toepassing: de app schrijft niets in Exact Online (KOP-001). **I** tokens en secret staan alleen in de geheimenopslag en het geheugen, nooit in de database of een log (BEV-009). **D** het budget, de wachttijd en de foutgrens houden Exact Online open (KOP-007, KOP-008). **E** alleen GET bestaat in de code (KOP-001), met de kleinste set scopes (KOP-003).
5. Misbruik: een klant die via veel stukken het dagbudget van de administratie opmaakt, ook voor de andere apps van het installatiebedrijf (KOP-007, BEV-004); een adres in een respons dat naar een interne dienst wijst (BEV-010).
6. Invariant: de app stuurt naar Exact Online alleen GET-verzoeken, alleen naar de host van Exact Online, en het refresh token staat alleen in de geheimenopslag.

G4 E-mail: de app en de mailbox.

1. Wat een aanvaller wil: een inloglink; de inhoud van een vraag of antwoord.
2. Wie: iemand die een e-mail doorgestuurd krijgt, een mailbox meeleest of zich als afzender voordoet.
3. De grens: naar buiten een korte melding met een link; naar binnen niets. Het verzenddomein neemt geen e-mail aan (null MX, RFC 7505; MEL-002): een antwoord op een e-mail van de app komt terug bij de afzender en bereikt de app nooit (BEV-015).

4. STRIDE: **S** de app verstuurt vanaf een eigen subdomein met SPF, DKIM en DMARC (MEL-002). **T** niet van toepassing: de app ontvangt geen e-mail, dus er is geen binnenkomende inhoud om te vervalsen, geen automatisch antwoord dat een vervalste afzender kan misbruiken en geen lus met een ander automatisch antwoord. **R** niet van toepassing, om dezelfde reden. **I** een e-mail bevat geen tekst van een vraag of antwoord, geen stuk en geen bijlage (BEV-011); wat iemand terugschrijft, komt nooit in de app of haar logs. **D** inlogaanvragen zijn begrensd (BEV-004). **E** een inloglink geeft in een andere browser geen sessie (BEV-002), en een medewerker logt nooit in met een e-mail (BEV-006).
5. Misbruik: de app gebruiken om veel e-mail naar een adres te sturen (BEV-004).
6. Invariant: geen e-mail van de app bevat de tekst van een vraag of antwoord, een stuk, of iets waarmee een andere browser dan de aanvrager inlogt; en geen e-mail bereikt de app.

Eisen

- **BEV-001 Basis.** De app MUST de basis van SEC-017 halen, alleen cookies met het voorvoegsel `__Host-` zetten en elk verzoek dat iets verandert weigeren als het van een andere herkomst komt (LIVE-011).
- **BEV-002 Inloggen als klant.** Een klant logt in met zijn e-mailadres en een inloglink. De link MUST alleen inloggen in de browser die hem aanvroeg; een andere browser, of een scanner van de mailbox, logt er niet mee in en verbruikt hem niet. De e-mail toont ook de code van de link, om in de browser van de aanvraag te plakken of over te nemen; het veld voor de code laat plakken en aanvullen door de browser toe (TOE-004). Een link en zijn code zijn 10 minuten geldig, eenmalig te gebruiken, en vervallen bij een nieuwe aanvraag of na 5 foute pogingen. De app kent geen wachtwoorden.
- **BEV-003 Geen opsporing.** Een inlogaanvraag MUST hetzelfde antwoord krijgen, in ongeveer dezelfde tijd, of het e-mailadres nu van een klant is, van een geblokkeerde klant of van niemand. Alleen een adres met toegang krijgt de e-mail (SCH-011).
- **BEV-004 Grenzen.** De app MUST weigeren: meer dan 5 inlogaanvragen per uur per e-mailadres, meer dan 20 inlogaanvragen per uur per IP-adres, meer dan 20 vragen per dag per klant, een vraag of antwoord van meer dan 2.000 tekens (GEG-009), en meer dan 100 geopende stukken per dag per klant.
- **BEV-005 Sessies.** Een sessie op het Klantportaal MUST eindigen na 14 dagen zonder gebruik, een sessie op Binnendienst na 12 uur zonder gebruik. Uitloggen beëindigt de sessie op de server. Bij elke inlog krijgt de sessie een nieuwe sleutel.
- **BEV-006 Inloggen als medewerker.** Een binnendienstmedewerker en een beheerder MUST op Binnendienst inloggen met een passkey, die hij

vastlegt bij zijn uitnodiging via Organisatiebeheer. Binnendienst stuurt geen inloglink, ook niet als herstel: die zou de passkey omzeilbaar maken voor wie een mailbox meeleest (G4). Heeft een medewerker op een apparaat geen passkey, dan werkt (a) een passkey die zijn eigen wachtwoordbeheer synchroniseert, op elk van zijn apparaten; (b) anders stuurt de beheerder hem in Organisatiebeheer een nieuwe uitnodiging, bevestigd met de passkey van de beheerder (ROL-010), en legt de medewerker daarmee een nieuwe passkey vast. Er is één beheerder en alleen hij nodigt uit. De beheerder MUST daarom bij zijn eerste inlog twee passkeys vastleggen, op twee apparaten. Verliest hij ze toch allebei, dan vraagt de Organisatie dat in het platform (INV-001); na bevestiging door de Beslisser daar stuurt Appwinst een nieuwe uitnodiging voor de rol beheerder.

- **BEV-007 Tekst blijft tekst.** De tekst van een vraag en een antwoord MUST als platte tekst worden opgeslagen en getoond; een adres erin wordt geen aanklikbare link. Elke pagina MUST een strikte Content Security Policy sturen en geen script van derden of inline script laden.
- **BEV-008 Bestanden uit Exact Online.** Een Bestand MUST alleen in de browser openen als zijn inhoud PDF, JPEG of PNG is, met de headers `Content-Security-Policy: sandbox` en `X-Content-Type-Options: nosniff`; elk ander Bestand alleen als download. Een Bestand groter dan 25 MB geeft de app niet door (KOP-005).
- **BEV-009 Geheimen.** Het client-secret en het refresh token MUST alleen in de geheimenopslag staan (SEC-006), het access token alleen in het geheugen; geen van drieën staat in de database, een log, een foutmelding, een adres of een e-mail. Logs bevatten alleen sleutels, geen namen, e-mailadressen of tekst van vragen (SEC-016, VAST-006).
- **BEV-010 Uitgaande verzoeken.** De server MUST alleen verzoeken sturen naar de host van Exact Online en naar de dienst die de e-mail verstuurt. Een adres dat Exact Online teruggeeft, haalt hij alleen op via HTTPS en op de host van Exact Online. Elk verzoek heeft een wachttijd (KOP-008).
- **BEV-011 E-mail.** Een e-mail van de app MUST alleen een korte melding en een link bevatten (MEL-003), nooit de tekst van een vraag of antwoord, een stuk of een bijlage.
- **BEV-012 Getoetste scheiding.** Geautomatiseerde tests MUST elk adres van het Klantportaal aanroepen met de sleutels van een order, stuk en vraag van een andere relatie, en de build laten falen als er één gegevens teruggeeft (zoals SEC-008 dat voor Appwinst eist). Een test MUST elke route van de koppeling op een ander verzoek dan GET laten falen.
- **BEV-013 Lekken.** Een lek van persoonsgegevens meldt Appwinst aan het installatiebedrijf zoals SEC-015 zegt; de melding aan de Autoriteit

Persoonsgegevens en aan betrokkenen is van het installatiebedrijf (VKL-004).

- **BEV-014 Bestemming na het inloggen.** Opent de app na het inloggen de pagina waarvoor iemand moest inloggen (SCH-012, SCH-042), dan MUST die bestemming een pad binnen hetzelfde portaal zijn. Een andere bestemming negeert de app; zij opent dan Orders of Vragen.
- **BEV-015 Geen binnenkomende e-mail.** De app MUST NOT e-mail ontvangen: het verzenddomein heeft een null MX (RFC 7505; MEL-002), en de app heeft geen adres, postbus of ingang die e-mail aanneemt.

Als een deel in handen van een aanvaller is

- **De productieserver.** De aanvaller leest de database (namen en e-mailadressen, vragen en antwoorden, gegevens van orders en stukken) en, uit het geheugen en de geheimenopslag van de server, het refresh token, en daarmee de administratie binnen de scopes. Hij vindt geen bestanden (KOP-005). Het kost dus niet alles: het installatiebedrijf trekt de app in Exact Online in of vervangt het client-secret, en de koppeling is dicht; Appwinst behandelt het als Kritiek (BEH-003) en meldt het (BEV-013).
- **Een gestolen back-up.** Versleuteld (SEC-007); hij bevat geen tokens, want die staan niet in de database (BEV-009), en geen bestanden.
- **Een mailbox van een klant.** Wie die beheerst, logt in als die klant. De beheerder blokkeert hem (ROL-007).
- **Een mailbox van een medewerker.** Geeft geen toegang tot Binnendienst: daar logt alleen een passkey in (BEV-006).
- **Exact Online zelf.** Valt buiten deze app; het abonnement is van het installatiebedrijf (VKL-005).

Restrisico

1. Wie de mailbox van een klant beheerst, beheerst zijn toegang. Aanvaard: zo werkt elke inlog per e-mail; de beheerder blokkeert.
2. Zolang VRAAG-KOP-1 open is, kan wie de productieserver volledig beheerst met het token schrijven in Exact Online, binnen de rechten van het account dat de koppeling autoriseerde. Verkleind door KOP-003 (een account met de kleinste rechten).
3. Verdwijnt een contactpersoon uit Exact Online, dan houdt hij toegang tot de eerstvolgende synchronisatie die het ziet: hooguit 10 minuten, of tot de volledige lezing van de nacht als VRAAG-KOP-3 nee is. Wie direct weg moet, blokkeert de beheerder.
4. De status in de app loopt hooguit 10 minuten achter op Exact Online (KOP-004); het scherm toont de tijd van de stand (KOP-009).
5. Verliest de beheerder beide passkeys, dan nodigt niemand in de app een medewerker uit tot Appwinst de rol beheerder opnieuw uitnodigt (BEV-006). Aanvaard: een snellere weg zou de passkey omzeilbaar maken.

12. Privacy

- **AVG-001 Rollen.** Het installatiebedrijf is verwerkingsverantwoordelijke (VKL-004). Appwinst is verwerker onder de verwerkersovereenkomst, getekend vóór Dag 0 (PRIV-001; WK-001 item 6), met de subverwerkers die PRIV-002 noemt. Exact Online is een verwerker van het installatiebedrijf zelf: de app leest daar in opdracht van het installatiebedrijf, en Exact Online is geen subverwerker van Appwinst.
- **AVG-002 Geen bijzondere gegevens.** De app verwerkt geen bijzondere persoonsgegevens, geen strafrechtelijke gegevens, geen BSN en geen gegevens van kinderen: de Aanvraag noemt geen van deze, en de klanten zijn contactpersonen van bedrijven en scholen, geen leerlingen.
- **AVG-003 Elk gegeven met zijn doel.** De app verwerkt alleen de persoonsgegevens hieronder. Hoe lang ze blijven, staat in Vastleggen en audit (VAST-007, en VAST-001 voor een vastlegging), of hier waar die het gegeven niet noemen.

Naam en e-mailadres, met de sleutel van de contactpersoon en zijn relatie in Exact Online. Van wie: klanten. Doel: inloggen, de klant tonen bij zijn vragen, hem e-mail sturen. Bron: de koppeling. Bewaard: VAST-007.

Blokkade: het genormaliseerde e-mailadres en de relatie, wie blokkeerde en wanneer. Van wie: klanten, medewerkers. Doel: de toegang blijvend weigeren, ook als het adres uit Exact Online verdwijnt en terugkomt (ROL-007), en zeggen wie dat besliste. Bron: de beheerder. Bewaard: tot de beheerder de toegang terugzet of de relatie verdwijnt (VAST-007).

Naam, e-mailadres en rol van een medewerker. Van wie: medewerkers. Doel: inloggen, de medewerker tonen bij zijn antwoorden. Bron: Organisatiebeheer. Bewaard: VAST-007.

Vragen en antwoorden, met wie ze schreef en wanneer, wanneer een klant een antwoord opende, en wie een vraag afsloot. Van wie: klanten en medewerkers. Doel: een vraag over een order afhandelen en terugvinden. Bron: wat gebruikers invoeren. Bewaard: VAST-007.

Wie de documenttypen per soort wijzigde, en wanneer (alleen de identificatie van de beheerder, VAST-004). Van wie: de beheerder. Doel: zeggen wie besliste wat klanten zien (ROL-006). Bron: de beheerder. Bewaard: VAST-001.

Inloglink. Van wie: klanten. Doel: inloggen. Bron: de app. Bewaard: VAST-007.

Gegevens van orders en stukken, zoals het onderwerp van een document. Van wie: soms een naam in een onderwerp. Doel: tonen wat er bij een order is. Bron: de koppeling. Bewaard: zolang ze in Exact Online staan (GEG-011).

De inhoud van werkbonnen, facturen en documenten, met de namen en adressen die erin staan. Van wie: wie erin staat. Doel: tonen bij een order.

Bron: de koppeling. Bewaard: niet: doorgegeven, niet bewaard (GEG-007, KOP-005).

IP-adres. Van wie: bezoekers. Doel: misbruik begrenzen (BEV-004). Bron: de browser. Bewaard: alleen in het geheugen, hooguit 1 uur.

Server- en toegangslogs. Van wie: iedereen, alleen met sleutels. Doel: storingen en misbruik vinden. Bron: de app. Bewaard: VAST-006.

Back-ups van al het bovenstaande. Van wie: iedereen. Doel: herstellen. Bron: de app. Bewaard: PRIV-007.

Een contactpersoon zonder e-mailadres houdt de app niet (GEG-002). De Tellingen van Kernproces (VAST-003) zijn geen persoonsgegevens: ze noemen geen persoon en geen order. Wat iemand op een e-mail van de app terugschrijft, bereikt de app niet (BEV-015). Na de termijn MUST de app het gegeven verwijderen. Spreekt het installatiebedrijf in de verwerkersovereenkomst een andere termijn af (PRIV-007, de rij Client app production data), dan is dat een nieuwe versie van dit document (ALG-005).

- **AVG-004 Zo min mogelijk.** De app leest alleen de velden van KOP-002, nooit een telefoonnummer (BUITEN-008), bewaart geen bestanden uit Exact Online (KOP-005), zet alleen het sessiecookie (BEV-001) en gebruikt geen analytics of trackingcookies (MEET-002). Gegevens over een persoon worden alleen in Exact Online gecorrigeerd, de bron (VKL-002).
- **AVG-005 Wat klanten van elkaar zien.** De klanten van één relatie zien bij een order van die relatie elkaars vragen, met de naam van wie vroeg, en de antwoorden (ROL-004, VRG-003). Een klant van een andere relatie ziet niets daarvan.
- **AVG-006 Rechten van betrokkenen.** Een verzoek om inzage, correctie of verwijdering beantwoordt het installatiebedrijf als verwerkingsverantwoordelijke; Appwinst helpt kosteloos met wat zij heeft, en ook bij een gegevensbeschermingseffectbeoordeling als het installatiebedrijf die nodig vindt (PRIV-011). Het installatiebedrijf krijgt via het platform op elk moment een export van alle gegevens (BEH-011).
- **AVG-007 Privacy door ontwerp en beveiliging van de verwerking.** AVG-004, ROL-001 en KOP-005 geven invulling aan artikel 25 AVG, het hoofdstuk Beveiliging aan artikel 32 AVG ([27]). Alle gegevens staan in de EU (INV-009).

13. Toegankelijkheid en taal

- **TOE-001** De app is in het Nederlands (BUITEN-010). Elke pagina en elke e-mail draagt Nederlands als taal. Teksten uit Exact Online, zoals een omschrijving, toont de app zoals ze daar staan.

- **TOE-002** Elk scherm MUST voldoen aan WCAG 2.2 niveau AA ([41]) en de geautomatiseerde toegankelijkheidspoort halen (A11Y-006). Dit document maakt geen uitzondering.
- **TOE-003** Een status, een toegang en het label Nieuw antwoord MUST NOT alleen op kleur steunen: elk heeft tekst, en een status ook een eigen pictogram.
- **TOE-004** Inloggen vraagt geen wachtwoord en niets om te onthouden. De inloglink werkt zonder iets over te nemen; de inlogcode is alleen een terugval, en haar veld laat plakken toe en laat de browser de code aanvullen; een medewerker logt in met een passkey. Zo voldoet inloggen aan WCAG 2.2, succescriterium 3.3.8 ([41]). Het e-mailveld laat de browser aanvullen.
- **TOE-005** Na versturen van een vraag of antwoord, na afsluiten, na blokkeren en na toegang terugzetten MUST een schermlezer de bevestiging voorlezen zonder dat de focus verspringt (WCAG 2.2, succescriterium 4.1.3, [41]).
- **TOE-006** Elke link naar een bestand noemt de soort en het onderwerp van het stuk en het bestandstype. De toegankelijkheid van de bestanden zelf is die van de bestanden in Exact Online (VKL-002).
- **TOE-007** Elk scherm werkt met alleen het toetsenbord, in een volgorde die de lezer volgt, met een zichtbare focus. Elk doel om op te tikken voldoet aan WCAG 2.2, succescriterium 2.5.8. Elk scherm blijft bruikbaar bij vergroten tot de grens van succescriterium 1.4.10, zonder horizontaal te scrollen ([41]).
- **TOE-008** De app respecteert de instelling voor minder beweging.
- **TOE-009** De woorden zijn die van Begrippen: kort en duidelijk, zonder vakjargon. De statussen heten zoals in STAT-001.
- **TOE-010** De app wordt niet aan consumenten aangeboden. Een ontwerp van een toegankelijkheidsverklaring hoort daarom niet bij de Overdracht (A11Y-007).

14. Niet-lijst

De openbare Niet-lijst van Appwinst geldt voor deze Build onverkort (Appwinst-specificatie, NIET-003). Deze Build voegt de volgende items toe.

- **BUITEN-001 Alleen lezen uit Exact Online.** De app MUST NOT iets schrijven in Exact Online. Orders, werkbonnen, facturen, documenten en contactpersonen veranderen alleen in Exact Online.
- **BUITEN-002 Geen importbestand.** De Build importeert geen bestand. De contactpersonen en hun relaties komen via de koppeling met Exact Online.
- **BUITEN-003 Geen onderhoud plannen.** Een klant kiest in deze Build geen moment voor onderhoud. Dat is de Uitbreiding Afspraken: optie 2 van de Bouwcheck, of later met Doorbouwen.

- **BUITEN-004 Geen statusgeschiedenis van vóór Live.** Exact Online bewaart alleen de huidige status van een order. De app legt statuswijzigingen vast vanaf Live, niet daarvoor.
- **BUITEN-005 Geen betalingen.** De app toont de factuur bij een order. Betalen gebeurt buiten de app.
- **BUITEN-006 Geen track-and-trace.** De app toont de status en de geplande datum van een order (STAT-001, STAT-002), niet de rit van een vervoerder.
- **BUITEN-007 Geen bestanden bij een vraag.** Een vraag is tekst. Klanten en binnendienstmedewerkers voegen geen bestanden toe aan een vraag of antwoord.
- **BUITEN-008 Geen telefoonnummers.** De app leest en bewaart geen telefoonnummer van een contactpersoon.
- **BUITEN-009 Alleen e-mail als melding.** De app meldt per e-mail. Er is geen sms, WhatsApp of pushmelding.
- **BUITEN-010 Alleen Nederlands.** De app is in het Nederlands. Een andere taal is de Uitbreiding Vertaalmodule.
- **BUITEN-011 Geen app in een appwinkel.** De app werkt in de browser op desktop, tablet en telefoon. Een app in de App Store is de Native app, een eigen Extra sprint na Live.
- **BUITEN-012 Geen audittrail.** De app legt vast wat Vastleggen en audit noemt. Een audittrail met export is de Uitbreiding Audittrail en zit niet in deze Build.
- **BUITEN-013 Geen support aan klanten door Appwinst.** De binnendienstmedewerkers van het installatiebedrijf beantwoorden de vragen van klanten. Appwinst helpt de organisatie van het installatiebedrijf, via het platform.

15. Klaar is als

Elk criterium beantwoordt het installatiebedrijf met ja of nee door de app te gebruiken: in de Preview op testgegevens, en na Live in de app zelf (BB-003). Alleen deze criteria bepalen of een Pin een Fout of een Wens is (PIN-016). Achter elk criterium staat wat het toetst.

Klantportaal: Inloggen

- **KLAAR-001** Een klant vraagt op Inloggen een inloglink aan met het e-mailadres dat in Exact Online bij zijn contactpersoon staat, en is met de link uit de e-mail binnen in Orders, zonder wachtwoord, in ten hoogste 2 stappen op Mobiel. (PROC-001, REIS-001, SCH-010, SCH-012.)
- **KLAAR-002** Wie op Inloggen een e-mailadres zonder toegang invult, onbekend of bij elke relatie geblokkeerd, ziet dezelfde melding als bij een adres met toegang, en krijgt geen e-mail. (SCH-011, BEV-003.)
- **KLAAR-003** Een inloglink die al gebruikt is of ouder is dan 10 minuten, logt niet in; hij opent een pagina die dat zegt, met één knop voor een nieuwe link. (SCH-013, BEV-002.)

- **KLAAR-004** Een inloglink die in een andere browser wordt geopend dan de browser die hem aanvroeg, logt niet in; met de inlogcode uit dezelfde e-mail, getypt of geplakt, logt de klant in de browser van zijn aanvraag wel in. (SCH-011, SCH-012, BEV-002, TOE-004.)
- **KLAAR-043** De pagina die een klant ziet als hij de inloglink in een andere browser opent, zegt dat de link alleen werkt in de browser waarin hij hem aanvroeg en dat hij daar de inlogcode uit de e-mail kan invullen; de pagina toont de inlogcode niet. (SCH-014.)

Klantportaal: Orders

- **KLAAR-005** Orders toont alleen de orders van de relatie van de klant, eerst de lopende, elk met ordernummer, omschrijving, status en, waar STAT-002 dat zegt, de geplande datum. (PROC-002, SCH-020, SCH-021, INVAR-001.)
- **KLAAR-006** Een klant ziet vanuit de e-mail met de inloglink de status en de geplande datum van een order van zijn relatie in ten hoogste 3 stappen op Mobiel. (PROC-002, REIS-002.)
- **KLAAR-007** Elke order toont precies één status, die STAT-001 geeft voor zijn waarden in Exact Online, nooit leeg en nooit naast een tweede status; de geplande datum staat er alleen waar STAT-002 dat zegt. (STAT-001 tot en met STAT-003, INVAR-004.)
- **KLAAR-008** Heeft de relatie van een klant geen lopende order, dan zegt Orders dat op de plek van Lopend, met hoe de klant het installatiebedrijf bereikt, en staan de eerdere orders eronder; geen lege lijst. (SCH-024.)
- **KLAAR-009** Een klant die met hetzelfde e-mailadres bij twee relaties staat, logt één keer in, kiest in Orders een relatie en ziet daarna alleen haar orders; de andere relatie kan hij ook kiezen. (SCH-023, GEG-003, ROL-005.)

Klantportaal: Order

- **KLAAR-010** Een klant opent vanaf Orders het bestand van een werkbon van een order in ten hoogste 2 stappen. (PROC-003, REIS-003, SCH-031.)
- **KLAAR-011** Order toont altijd de drie groepen werkbonnen, factuur en documenten. Elk stuk dat in Exact Online bij die order staat en waarvan het documenttype volgens Documenttypen per soort een soort heeft, staat in zijn groep, één keer, met onderwerp en datum, en elk bestand ervan opent. (PROC-003, SCH-030, SCH-031, GEG-005, GEG-006, KOP-005.)
- **KLAAR-012** Een groep zonder stukken zegt in Order dat er nog geen stukken in staan; een order zonder stukken toont zo drie lege groepen en het veld voor een vraag. (SCH-031, SCH-033.)
- **KLAAR-013** Een stuk waarvan het documenttype in Documenttypen per soort geen soort heeft, of niet in die tabel staat, toont de app niemand, ook niet in Binnendienst. (ROL-006, GEG-006.)

- **KLAAR-014** Een klant die het adres opent van een order, stuk of vraag van een andere relatie, krijgt dezelfde pagina "niet gevonden" als bij een order die niet bestaat, en niets van die order. (SCH-005, ROL-009, INVAR-001.)
- **KLAAR-015** Een klant typt in Order een vraag en verstuurt hem in 1 stap; de vraag staat daarna bij die order, met de tijd, en het scherm zegt dat hij een e-mail krijgt als er een antwoord is. (PROC-004, REIS-004, SCH-032, INVAR-006.)
- **KLAAR-016** Een andere klant van dezelfde relatie ziet die vraag bij dezelfde order; een klant van een andere relatie ziet hem nergens. (VRG-003, AVG-005.)
- **KLAAR-017** Bij elke vraag en elk antwoord staat wie het schreef en wanneer, en niemand kan een verstuurde vraag of een verstuurd antwoord wijzigen of verwijderen. (VRG-001, VRG-004, GEG-009.)
- **KLAAR-018** Een vraag van meer dan 2.000 tekens gaat niet weg; de app zegt hoeveel tekens mogen, en de tekst blijft staan. (GEG-009, BEV-004.)

Binnendienst: Inloggen en Organisatiebeheer

- **KLAAR-019** Een medewerker logt in op Binnendienst met zijn passkey; Binnendienst stuurt geen inloglink. Een klant kan daar niet inloggen, ook niet met zijn eigen e-mailadres. (SCH-040, SCH-041, ROL-008, BEV-006.)
- **KLAAR-044** Breekt een medewerker het inloggen af, of mislukt het, dan zegt Binnendienst: Inloggen dat, met een knop om het opnieuw te proberen; heeft hij op dit apparaat geen passkey, dan zegt het scherm dat hij de beheerder om een nieuwe uitnodiging vraagt. (SCH-040, SCH-043.)
- **KLAAR-045** Een medewerker wiens passkey met zijn wachtwoordbeheer wordt gesynchroniseerd, logt met die passkey ook in op een tweede apparaat. (BEV-006.)
- **KLAAR-020** Een beheerder nodigt in Organisatiebeheer een nieuwe binnendienstmedewerker uit en bevestigt dat met zijn passkey; de medewerker legt bij de uitnodiging zijn passkey vast en logt daarmee in op Binnendienst. Een medewerker die de beheerder verwijdert, ziet bij zijn volgende klik niets meer. (ROL-003, ROL-007, ROL-010, BEV-006.)
- **KLAAR-046** Een medewerker zonder passkey op zijn apparaat krijgt van de beheerder een nieuwe uitnodiging, bevestigd met de passkey van de beheerder, legt daarmee een nieuwe passkey vast en logt daarna in. (BEV-006, ROL-010.)
- **KLAAR-047** Een beheerder komt bij zijn eerste inlog pas verder als hij twee passkeys heeft vastgelegd. (BEV-006.)

Binnendienst: Vragen en Vraag

- **KLAAR-021** Een vraag bij een order zonder open vraag stuurt elke binnendienstmedewerker een e-mail met een link naar Vraag; een

volgende vraag bij die order, terwijl er een open vraag is, stuurt er geen. (PROC-004 naar PROC-005, MEL-006.)

- **KLAAR-022** Vragen toont elke open vraag, de oudste bovenaan, met relatie, ordernummer, naam van de klant en sinds wanneer hij open staat; een beantwoorde of afgesloten vraag staat er niet tussen. (SCH-050, VRG-002.)
- **KLAAR-023** Een binnendienstmedewerker beantwoordt vanaf Vragen een open vraag in ten hoogste 2 stappen. (PROC-005, REIS-005, SCH-060.)
- **KLAAR-024** Vraag toont de status, de geplande datum en de stukken van de order naast de vragen en antwoorden. (SCH-061.)
- **KLAAR-025** Bij een antwoord krijgt elke klant met een open vraag bij die order precies één e-mail met het ordernummer en een link. Een klant die niet is ingelogd, komt via die link na het inloggen op die order, en ziet daar het antwoord. (PROC-005, REIS-005, MEL-005, SCH-012, INVAR-007.)
- **KLAAR-026** Een binnendienstmedewerker sluit een open vraag af; die staat daarna niet meer bij de open vragen, de klant ziet bij die vraag afgesloten, en hij krijgt geen e-mail. (SCH-062, VRG-002, MEL-008.)
- **KLAAR-027** Antwoordt een collega terwijl een binnendienstmedewerker typt, dan ziet die bij versturen dat antwoord, en zijn eigen tekst blijft staan. (SCH-064.)

Binnendienst: Klanten

- **KLAAR-028** Klanten toont per relatie de contactpersonen uit Exact Online, elk met naam, e-mailadres en toegang, en vindt een contactpersoon op naam, relatie of e-mailadres. (SCH-070, SCH-071.)
- **KLAAR-029** Een beheerder blokkeert vanaf Klanten de toegang van een klant bij een relatie in ten hoogste 3 stappen, de bevestiging met zijn passkey meegeteld. Die klant ziet bij zijn volgende klik in een open sessie niets meer van die relatie; heeft hij geen andere relatie, dan krijgt hij ook geen inloglink meer. (REIS-006, SCH-072, ROL-007, ROL-010, INVAR-003.)
- **KLAAR-030** Een binnendienstmedewerker ziet in Klanten geen knop om te blokkeren; een beheerder wel, en bevestigt het blokkeren met zijn passkey. (ROL-004, ROL-010.)
- **KLAAR-031** Een beheerder zet met zijn passkey de toegang van een geblokkeerde klant terug, en die klant kan weer inloggen. (SCH-072, ROL-010.)
- **KLAAR-032** Een blokkade van een klant bij een relatie blijft gelden na een synchronisatie, ook als zijn e-mailadres uit Exact Online verdwijnt en later terugkomt; zij eindigt alleen als de beheerder de toegang terugzet of de relatie verdwijnt. Klanten toont bij Geblokkeerd wie blokkeerde en wanneer. (GEG-010, ROL-007, SCH-070, SCH-073, VAST-001.)

De koppeling met Exact Online

- **KLAAR-033** Een contactpersoon met een e-mailadres die het installatiebedrijf in Exact Online toevoegt bij een relatie met een order, kan na de volgende synchronisatie inloggen en ziet de orders van die relatie, zonder dat iemand in de app een account aanmaakt of een bestand aanlevert. (GEG-002, GEG-003, IMP-004.)
- **KLAAR-034** Een contactpersoon die uit de testadministratie in Exact Online is verwijderd, kan uiterlijk na de volledige lezing van de nacht niet meer inloggen, ook niet in een sessie die openstond; zijn vragen staan nog bij hun order, met verwijderde contactpersoon als afzender. (ROL-007, KOP-004, GEG-011, VAST-004.)
- **KLAAR-035** Verandert in de testadministratie de status van een order, of komt er een order of stuk bij, dan staat dat binnen 10 minuten in de app, en de statuswijziging staat in Vraag bij die order, met de datum waarop de app haar zag. (KOP-004, GEG-008, VAST-002, SCH-061, INVAR-005.)
- **KLAAR-036** Is Exact Online niet bereikbaar, of is de koppeling verbroken, bijvoorbeeld omdat het installatiebedrijf de app in Exact Online heeft ingetrokken, dan tonen Orders, Order en Klanten de laatst bekende gegevens met de tijd waarop ze zijn bijgewerkt, zeggen ze dat die niet actueel zijn, en tonen ze geen lege lijst. De beheerder krijgt dan één e-mail, en nog één als de koppeling weer werkt; daartussen geen. (SCH-004, KOP-009, MEL-009, INVAR-005.)
- **KLAAR-037** Na een week gebruik van de Preview is in de testadministratie geen order, stuk, contactpersoon of relatie door de app gewijzigd. (KOP-001, BUITEN-001, INVAR-002.)

E-mail en gegevens

- **KLAAR-038** Wie een e-mail van de app beantwoordt, krijgt zijn antwoord terug als onbestelbaar; het wordt geen vraag of antwoord, en de app ontvangt het niet. Elke e-mail van de app eindigt met zijn link. (MEL-002, MEL-003, MEL-007, BEV-015.)
- **KLAAR-039** Geen e-mail van de app bevat de tekst van een vraag of antwoord, of een stuk of andere bijlage. (MEL-003, BEV-011.)
- **KLAAR-040** Nergens in de app, en niet in de export van BEH-011, staat een telefoonnummer van een contactpersoon. (GEG-002, KOP-002, BUITEN-008.)

De hele app

- **KLAAR-041** Elk scherm van beide apps werkt op Mobiel, Tablet en Desktop van de Preview en met alleen het toetsenbord, en elke status, toegang en elk label is ook zonder kleur te lezen. (SCH-002, TOE-003, TOE-007, A11Y-006.)
- **KLAAR-042** Elke gebeurtenis die Kernproces noemt, telt de app per dag, zonder persoon, relatie of order, en de tellingen staan in de export van de gegevens (BEH-011). (MEET-001, MEET-002, VAST-003; elke reis haar maat.)

16. Eigendom, zeggenschap en vertrek

- **EIG-001 Het installatiebedrijf houdt de zeggenschap.** Voor deze app geldt INV-013. Dit hoofdstuk noemt wat dat hier betekent en herhaalt de regels niet.
- **EIG-002 Code en rechten.** De repositories van de app volgen INV-007 en LIVE-010; het auteursrecht volgt de IP-akte (LEG-017); Fundamental komt met de licentie van LIC-001 en een eigen Fundamental-kopie (MIR-002).
- **EIG-003 Domeinen.** Het domein `voorbeeld.example` staat op naam van het installatiebedrijf. Het Klantportaal staat op `portaal.voorbeeld.example` en Binnendienst op `binnendienst.voorbeeld.example`, gekoppeld zoals LIVE-011 zegt, naast hun adres bij Appwinst. De DNS-records van het verzenddomein (MEL-002), met zijn null MX (BEV-015), staan in het domein van het installatiebedrijf.
- **EIG-004 Accounts van derden.** Het abonnement op Exact Online, de registraties van de app in het Exact App Center voor test en productie, en het ontwikkelaarsabonnement voor de testadministratie (KOP-010) staan op naam van het installatiebedrijf (VKL-005, INV-013). Het installatiebedrijf trekt de app in Exact Online in wanneer het wil; dan stopt de koppeling (KOP-009).
- **EIG-005 Gegevens.** Het installatiebedrijf krijgt via het platform op elk moment een volledige export (BEH-011). Orders, werkbonnen, facturen, documenten en contactpersonen blijven in Exact Online; de app is daar nooit de bron van.
- **EIG-006 Beheer.** Appwinst draait en onderhoudt de app onder Beheer (BEH-001), op de basis van Beheer Normaal (BEH-008). De koppeling voegt geen server, geen opslag van bestanden en geen dienst toe: de app leest volgens schema, bewaart geen bestanden (KOP-005) en heeft geen webhook (KOP-004). Er is dus geen toeslag (BEH-009).
- **EIG-007 Vertrek.** Bij vertrek gelden de overdracht van BEH-012 en, zonder keuze na Live, LIVE-009. Appwinst verwijdert dan de gegevens van de koppeling uit haar geheimenopslag (BEH-012); het installatiebedrijf SHOULD daarna het client-secret in het Exact App Center vervangen of de app daar intrekken.

17. Verantwoordelijkheid van de klant

Wat de Appwinst-specificatie in LEG-019 bij de opdrachtgever legt, geldt voor deze app zo. De opdrachtgever is hier het installatiebedrijf; een klant is in dit document altijd de rol Klant.

- **VKL-001 Bedrijfsvoering en gebruikers.** Het installatiebedrijf is alleen verantwoordelijk voor zijn bedrijfsvoering, voor de inhoud en het gebruik van de app, en voor zijn gebruikers: de klanten en zijn eigen medewerkers. Wat het installatiebedrijf zijn relaties belooft, zoals hoe snel een vraag een antwoord krijgt, is zijn belofte (LEG-019).

- **VKL-002 De gegevens in Exact Online.** Het installatiebedrijf is verantwoordelijk voor de juistheid van de orders, werkbonnen, facturen en documenten in Exact Online. De app toont wat Exact Online levert.
- **VKL-003 Wie toegang heeft.** Een contactpersoon met een e-mailadres bij een relatie die in Exact Online een verkooporder heeft, kan als klant inloggen en ziet de orders van die relatie. Het installatiebedrijf houdt de contactpersonen in Exact Online juist, en blokkeert wie geen toegang meer mag hebben.
- **VKL-004 Verwerkingsverantwoordelijke.** Het installatiebedrijf is verwerkingsverantwoordelijke voor de persoonsgegevens in de app: namen en e-mailadressen, vragen en antwoorden, en de stukken uit Exact Online. Appwinst is verwerker onder de verwerkersovereenkomst (PRIV-001; AVG art. 28 lid 3 [27]). De grondslag voor de verwerking is die van het installatiebedrijf (LEG-019).
- **VKL-005 Abonnementen en accounts.** Het abonnement op Exact Online, de registratie van de app in het App Center door de hoofdgebruiker van het installatiebedrijf, en het ontwikkelaarsabonnement van Exact Online met de testadministratie voor de Preview (KOP-010) zijn van het installatiebedrijf, op zijn naam en voor zijn rekening (INV-013, LEG-019). De API-limieten van Exact Online per administratie deelt de app met de andere apps van het installatiebedrijf [11]. Het domein van beide apps staat op naam van het installatiebedrijf (LIVE-011).
- **VKL-006 Het opleverdossier.** Bij de melding dat het werk klaar is voor oplevering moet een aannemer de opdrachtgever een dossier geven (art. 7:757a BW [17], [18], [19]). Die plicht blijft van het installatiebedrijf. De app toont documenten bij een order; of en hoe het installatiebedrijf daar het dossier mee levert, beslist het installatiebedrijf.
- **VKL-007 Aansprakelijkheid.** Het installatiebedrijf vrijwaart Appwinst zoals LEG-019 zegt. De aansprakelijkheid van Appwinst voor haar eigen prestatie is die van LEG-015; dit document voegt daar niets aan toe en neemt er niets van af.

18. Conformiteit

- **CONFORM-001** De app voldoet aan deze specificatie als elk criterium van Klaar is als met ja wordt beantwoord en geen eis van dit document wordt geschonden. Vóór Live heeft elk criterium zijn bewijs (LIVE-001 item 1).
- **CONFORM-002** Elke eis wordt zo getoetst:

Sectie	Hoe het getoetst wordt
Invarianten	Een geautomatiseerde test per invariant, met twee relaties in de testgegevens; voor INVAR-001 en

	INVAR-003 de tests van BEV-012, en een test van een sessie na een blokkade.
Rollen en rechten	Een test per rol en per handeling van ROL-004, die toont dat alles geweigerd is wat de rol niet uitdrukkelijk mag (ROL-001).
Domeinmodel; Vastleggen en audit	Tests op het schema, op de leespaden van GEG-013, en op wat bij elke handeling wordt vastgelegd.
Kernproces	De Demo loopt PROC-001 tot en met PROC-005 op testgegevens (DEM-001); een test per gebeurtenis van MEET-001.
Schermen	De criteria van Klaar is als per scherm, in de Preview, op Mobiel, Tablet en Desktop.
Koppeling en import	De controles van KOP-010 en BOUW-002 vóór de Start; tests op opgenomen antwoorden van de testadministratie; een test die elke route van de koppeling laat falen op een ander verzoek dan GET (BEV-012); KLAAR-033 tot en met KLAAR-037 in de Preview.
Meldingen	De e-mails in de Preview, waar de app ze opvangt (PRV-010); vóór Live de records van het verzenddomein (MEL-002), en dat dat domein geen mail aanneemt (KLAAR-038).
Beveiliging	OWASP ASVS 5.0, niveau 2 [42], voor beide apps; de poorten van §22 van de Appwinst-specificatie; de tests van BEV-012.
Privacy	Een controle dat de app alleen de gegevens van AVG-003 bewaart, en geen telefoonnummer (KLAAR-040).
Toegankelijkheid en taal	De geautomatiseerde toegankelijkheidspoort (A11Y-006) op elk scherm, en KLAAR-041 met toetsenbord en schermlezer, tegen WCAG 2.2 niveau AA [41].

- **CONFORM-003** Het Klantportaal SHOULD op Inloggen, Orders en Order op Mobiel de grenzen "goed" van Core Web Vitals halen die de Appwinst-specificatie in §23 voor haar eigen sites stelt: LCP ten hoogste 2,5 s, INP ten hoogste 200 ms en CLS ten hoogste 0,1, bij het 75e percentiel; en SHOULD de server op die schermen antwoorden binnen 500 ms bij het 95e percentiel. Het openen van een bestand telt niet mee: de app haalt het bij Exact Online op (KOP-005), en hoe snel dat gaat, hangt af van Exact Online.
- **CONFORM-004** Binnendienst SHOULD op Inloggen, Vragen, Vraag en Klanten op Desktop dezelfde grenzen halen als CONFORM-003.
- **CONFORM-005** CONFORM-003 en CONFORM-004 worden gemeten op de Testversie, met testgegevens, op het profiel Mobiel of Desktop; na Live meet de bewaking van Beheer de antwoordtijd van de server (BEH-001).
- **CONFORM-006** Onder Beheer gelden voor elk van beide portalen de beschikbaarheid van BEH-005 en het herstel van BEH-013, in de vorm van Beheer die het installatiebedrijf kiest (BEH-001).

19. Bouwplan per dag

Het bouwplan volgt de bouwweek van de Appwinst-specificatie (§7). De Bouwbrief geeft elke dag met zijn datum en tijden (CAL-011). Het fundament staat vóór de Start (CAL-013). Daarna bouwt elke sectie zijn eigen codepaden, ten hoogste één bouwdag werk, met een eigen ontwikkelaar, zodat de secties naast elkaar worden gebouwd (BC-016).

- **BOUW-001** Het fundament MUST af zijn vóór de Start: het datamodel (Domeinmodel); inloggen op beide apps zoals Beveiliging zegt, met de inloglink en inlogcode voor klanten en de passkey voor medewerkers, met de rollen en alles standaard geweigerd (ROL-001); de koppeling met Exact Online (KOP-001 tot en met KOP-009), met de synchronisatie en de stand ervan; de afleiding van de status (STAT-001); de toets op toegang bij elk verzoek (INVAR-001, INVAR-003); het versturen van e-mail via de outbox (GEG-012), vanaf het adres van MEL-002; het tellen van de gebeurtenissen (MEET-001); beide apps in het merk van het brandbook, met de plek in Order waar de vragen komen; en de testgebruikers, één per rol (PRV-008).
- **BOUW-002** De testadministratie staat in het ontwikkelaarsabonnement van het installatiebedrijf (KOP-010). Naast de controles van KOP-010 MUST de Bouwer vóór de Start daarin vastleggen dat zij bevat: ten minste twee relaties met een order, elk met ten minste één contactpersoon met een e-mailadres; voor elk van de vijf statussen van STAT-001 een order, en daarnaast een open order met een geplande datum die voorbij is; een relatie met alleen eerdere orders; een order zonder stukken; en een relatie zonder verkooporder, met een contactpersoon met een e-mailadres, die niet kan inloggen (VKL-003).

Hij toetst dat het veld dat het installatiebedrijf vóór ondertekening als antwoord op VRAAG-ROL-1 noemde, bij elke order gevuld is (ROL-005). Met het installatiebedrijf stelt hij in de testadministratie vast: de documenttypen per soort (GEG-006); het e-mailveld van een contactpersoon (IMP-003); de velden voor de omschrijving van een order, en voor het onderwerp en de datum van een stuk en de bestandsnaam, het bestandstype en de grootte van zijn bestanden (SCH-021, SCH-030, SCH-031); en hoeveel orders een relatie heeft en hoeveel stukken een order (GEG-014). Ontbreekt iets, dan is item 4 van WK-001 niet gedaan en zegt de Bouwer wat ontbreekt (WK-002).

– **BOUW-003** De secties zijn:

Sectie	Wat	Criteria
A	Klantportaal: Orders en Order, met de stukken, de keuze van de relatie, de lege staten en de stand van de koppeling	KLAAR-005 tot en met KLAAR-014
B	Binnendienst: Klanten, met blokkeren en toegang terugzetten; het uitnodigen van medewerkers met Organisatiebeheer, met hun passkey; de documenttypen per soort en de stand van de koppeling in de Beheeromgeving	KLAAR-020, KLAAR-028 tot en met KLAAR-032, KLAAR-046, KLAAR-047
C	Klantportaal: de vraag in Order en de antwoorden eronder (A5)	KLAAR-015 tot en met KLAAR-018
D	Binnendienst: Vragen en Vraag, met afsluiten, en de e-mails bij een nieuwe vraag en een nieuw antwoord (A5)	KLAAR-021 tot en met KLAAR-027, KLAAR-039

Het fundament dekt KLAAR-001 tot en met KLAAR-004, KLAAR-019, KLAAR-033 tot en met KLAAR-038, KLAAR-040 en KLAAR-042 tot en met KLAAR-045; elke sectie dekt KLAAR-041 voor zijn eigen schermen.

Dag	Wat er gebeurt

Vóór Dag 0	Het fundament (BOUW-001), gebouwd op de gedocumenteerde API van Exact Online.
Dag 0	De controles van KOP-010 en BOUW-002, in de testadministratie van het ontwikkelaarsabonnement van het installatiebedrijf. De Build wordt Startklaar als elk item van WK-001 gedaan is.
Dag 1	Start. De secties A, B, C en D worden naast elkaar gebouwd. De Preview staat live met inloggen, Orders en Order op de testadministratie (PRV-001).
Dag 2	De secties zijn af. De Demo loopt PROC-001 tot en met PROC-005 (DEM-001).
Dag 3	Het venster van de stopknop sluit (DEM-008). Wensen uit Pins tot de feedbackgrens van §7; de productieomgeving in de EU wordt ingericht.
Dag 4	De Testversie: daarna alleen nog Fouten (WK-012). Productie draait, met back-ups en een geteste restore (LIVE-001 item 4). Het installatiebedrijf geeft de toegang tot zijn administratie in productie via het geheimenformulier (KOP-011, LIVE-001 item 6).
Dag 5 en 6	Er wordt niet gebouwd (WK-013). Pins plaatsen kan in de Preview.
Dag 7	Live. De app synchroniseert met de administratie in productie; geen klant krijgt vanzelf een e-mail. De beheerder legt bij zijn eerste inlog zijn passkeys vast (KLAAR-047). De portalen draaien op hun adres bij Appwinst, en op de eigen adressen van het installatiebedrijf zodra zijn DNS het record van LIVE-011 heeft (EIG-003). De Overdracht voor Live (LIVE-003).

20. Bijlage: configuratiewaarden

Elke instelling van de app, met de eis die haar vastlegt (ALG-005). Een waarde die op Dag 0 wordt vastgesteld, staat na BOUW-002 in het verslag van Dag 0 en geldt als deel van deze Bijlage.

De koppeling met Exact Online

Waarde	Instelling	Eis
Synchronisatie van wijzigingen	elke 5 minuten	KOP-004
Volledige lezing van contactpersonen en relaties	elke nacht	KOP-004
Eigen dagbudget aan calls	4.000 calls per dag, waarvan 1.500 calls per dag vrij voor de synchronisatie	KOP-007
Foutgrens per endpoint	3 foutieve calls per uur	KOP-008
Wachttijd van een call	30 seconden	KOP-008
Grootste bestand dat de app doorgeeft	25 MB	KOP-005, BEV-008
Het veld van een verkooporder dat hem aan zijn relatie bindt	het veld dat het installatiebedrijf vóór ondertekening noemt (VRAAG-ROL-1); op Dag 0 toetst de Bouwer dat het gevuld is	ROL-005, BOUW-002
Het e-mailveld van een contactpersoon	`Email` of `BusinessEmail`, vastgesteld op Dag 0	IMP-003
De velden voor de omschrijving van een order, en voor onderwerp, datum, bestandsnaam, bestandstype en grootte van een stuk en zijn bestanden	vastgesteld op Dag 0	BOUW-002

Gegevens die de beheerder beheert (geen instelling, ALG-005)

Waarde	Beginstand	Eis
Documenttypen per soort (werkbon, factuur, document of niet zichtbaar)	op Dag 0 vastgesteld; daarna wijzigt de beheerder ze in de Beheeromgeving	GEG-006, ROL-006

Inloggen, sessies en grenzen

Waarde	Instelling	Eis
Geldigheid van een inloglink en zijn inlogcode	10 minuten	BEV-002
Foute pogingen per inloglink	5 foute pogingen	BEV-002
Sessie op het Klantportaal	14 dagen zonder gebruik	BEV-005
Sessie op Binnendienst	12 uur zonder gebruik	BEV-005
Verse bevestiging met de passkey	binnen de laatste 10 minuten	ROL-010
Passkeys van de beheerder bij zijn eerste inlog	twee	BEV-006
Inlogaanvragen	ten hoogste 5 inlogaanvragen per uur per e-mailadres, en 20 inlogaanvragen per uur per IP-adres	BEV-004
Vragen per klant	ten hoogste 20 vragen per dag	BEV-004
Geopende stukken per klant	ten hoogste 100 geopende stukken per dag	BEV-004
Langste vraag of antwoord	2.000 tekens	GEG-009, BEV-004

Bewaren

Waarde	Instelling	Eis
Het gesprek bij een order, met zijn afsluitingen	24 maanden na het laatste bericht of de laatste afsluiting in het gesprek, of korter als de order uit Exact Online verdwijnt	VAST-007
Naam en e-mailadres van een contactpersoon	zolang ze in Exact Online staan; verwijderd bij de synchronisatie die ziet dat ze er niet meer staan	VAST-007, GEG-011
Een blokkade	tot de beheerder de toegang terugzet, of tot de relatie uit de app verdwijnt	VAST-007, GEG-010

Naam, e-mailadres en rol van een medewerker	tot de beheerder hem verwijdert in Organisatiebeheer	VAST-007
Tellingen van Kernproces	13 maanden	VAST-001
IP-adres	alleen in het geheugen, hooguit 1 uur	AVG-003

E-mail en teksten

Waarde	Instelling	Eis
Verzenddomein	`mail.voorbeeld.example`, een domein dat geen mail aanneemt	MEL-002
Hoe een klant het installatiebedrijf bereikt, bij geen lopende orders	een tekst in Teksten en beelden	SCH-024

Snelheid

Waarde	Instelling	Eis
LCP op de hoofdschermen, 75e percentiel	2,5 s	CONFORM-003, CONFORM-004
INP op de hoofdschermen, 75e percentiel	200 ms	CONFORM-003, CONFORM-004
CLS op de hoofdschermen, 75e percentiel	0,1	CONFORM-003, CONFORM-004
Antwoordtijd van de server op de hoofdschermen, 95e percentiel	500 ms	CONFORM-003, CONFORM-004