VNG Realisatie

Gemeentelijke Telecommunicatie
GT Connect

Bijlage 14 Proof of Delivery (PoD)

Inhoudsopgave

1 Inleiding

GT Connect biedt een Communicatieplatform waar een groot aantal Deelnemers afhankelijk van is, zowel voor de interne communicatie als voor de communicatie naar de buitenwereld. Het is van groot belang dat deze Deelnemers kunnen vertrouwen op de goede werking van GT Connect. Het in gevaar komen van de dienstverlening van GT Connect heeft immers direct negatieve gevolgen voor het functioneren van een aantal bedrijfskritische processen van de Deelnemers. Het is om die reden van groot belang dat GT Connect in de volle breedte functioneert conform de specificaties, zodanig is beveiligd dat de beschikbaarheid, integriteit, vertrouwelijkheid en privacy zijn geborgd, en de dienstverlening van de Opdrachtnemer zodanig is ingericht dat een voldoende hoge kwaliteit mag worden verwacht.

Het belang van het goed functioneren van GT Connect heeft de Opdrachtgever doen besluiten om na de inwerkingtreding van de Raamovereenkomst eerst in een PoD (Proof of Delivery) te toetsen of de aangeboden oplossing ook in de praktijk voldoet aan de gestelde eisen. De PoD bestaat uit twee te toetsen onderdelen:

1. Toets op functionaliteit (paragraaf 2.2).
2. Toets op beveiliging (paragraaf 2.3).

In paragraaf 1.3.1 in het hoofddocument van het Beschrijvend Document is aangegeven dat de Raamovereenkomst zal eindigen als de Opdrachtnemer de PoD niet succesvol weet af te ronden. Om te voorkomen dat in dat geval een nieuwe aanbestedingsprocedure geïnitieerd dient te worden, kan de Opdrachtgever tegelijk met de Raamovereenkomst tevens een Schaduwovereenkomst sluiten met de Inschrijver die de op één na economisch meest voordelige Inschrijving op basis van de beste prijs-kwaliteitverhouding heeft uitgebracht. Deze Schaduwovereenkomst wordt beëindigd als de Opdrachtnemer van de Raamovereenkomst de PoD succesvol afrondt. Als dit echter niet het geval is, wordt de Raamovereenkomst beëindigd, en neemt de Schaduwovereenkomst (indien deze is gegund) de plaats van de Raamovereenkomst in.

In deze Bijlage wordt nader ingegaan op de inhoud en het verloop van de PoD.

2 Proof of Delivery

2.1 Het te toetsen platform

De PoD zal plaatsvinden op de GT Connect productieomgeving. De Opdrachtnemer krijgt na ondertekening van de Raamovereenkomst acht weken de tijd om dit platform gereed te maken voor de toets. Tijdens de PoD kan wat betreft de omvang van het platform worden volstaan met een omvang die volstaat voor het uitvoeren van de toets.

Het platform dient alle functionaliteit te kunnen leveren die in het Beschrijvend Document is opgenomen. Het is echter tijdens de toets niet noodzakelijk om verbindingen naar providers voor mobiele telefonie beschikbaar te hebben. Wel dient de Opdrachtnemer een verbinding beschikbaar te stellen naar het openbare vaste telefonienetwerk. De Aanbestedende Dienst kan met alle Endpoints en Profielen die tijdens de PoD beschikbaar zijn, gebruik maken van deze verbinding naar het openbare vaste telefonienetwerk.
Het platform dient bovendien aangesloten te zijn op het internet, onder meer voor het uitvoeren van toetsen met Softwarematige Endpoints op zelf gekozen locaties. Tot slot dient de Opdrachtnemer een vaste verbinding op een locatie naar keuze binnen Nederland beschikbaar te stellen voor gebruik door de Aanbestedende Dienst voor het uitvoeren van toetsen.

De Opdrachtnemer dient op het platform twee fictieve gemeenten aan te maken die niet met elkaar samenwerken en dus onafhankelijk van elkaar van GT Connect gebruik maken. Deze gemeenten dienen ieder de volgende aantallen Profielen in gebruik te hebben:

- 10 UC gebruikers.
- 10 TS gebruikers.
- 5 AT gebruikers.
- 3 KCC agenten.
- 3 KCC omnichannel agenten.
- 1 KCC supervisor.
- 1 KCC omnichannel supervisor.
- 1 Bedienpost gebruiker.
- 1 Fax Profiel.
- Voicemail: voor twee UC en twee AT gebruikers.
- Recording: Communicatiesessies van alle KCC agenten (inclusief omnichannel agenten) en 2 UC gebruikers dienen opgenomen te kunnen worden.

2.2 Toets op functionaliteit

De toets op functionaliteit bestaat uit de volgende stappen:

1. **Opstellen lijst met te toetsen functionaliteiten**
   De Aanbestedende Dienst stelt een lijst op met functionaliteiten die tijdens de PoD worden getoetst. Bij de te toetsen functionaliteiten wordt indien nodig een korte omschrijving van de toetsing gegeven en wordt aangegeven op welke eisen en geconformeerde wensen uit de Conformiteitlijst de toetsing betrekking heeft. De Aanbestedende dienst houdt er rekening mee dat de PoD zodanig van inhoud en omvang dient te zijn dat deze in een beperkte tijd praktisch uitvoerbaar is. De lijst met te toetsen functionaliteiten wordt één Werkdag na inwerkingtreding van de Raamovereenkomst overhandigt aan de Opdrachtnemer.

2. **Start PoD op functionaliteit**
   Op de eerste dag dat het platform gereed is voor de toets, ontvangt de Opdrachtnemer de Aanbestedende Dienst op de locatie waar in het kader van de toets gebruik gemaakt kan worden van de vaste verbinding naar GT Connect. Op deze locatie dienen de volgende werkplekken te zijn ingericht:
   a. Twee werkplekken met UC-Endpoints.
   b. Twee mobiele toestellen voorzien van UC-Endpoints.
   c. Twee werkplekken met TS-Endpoints.
   d. Twee mobiele toestellen voorzien van TS-Endpoints.
   e. Twee AT-Endpoints (voor geavanceerde telefonie).
   f. Twee KCC-agent-Endpoints (voor agenten van het klant Contact Centrum).
   g. Twee KCC-agent-omnichannel-Endpoints (voor omnichannel agenten van het Klant Contact Centrum).
   h. KCC-supervisor-Endpoint (voor de supervisor van het klant Contact Centrum).
   i. KCC-omnichannel-supervisor-Endpoint (voor de omnichannel supervisor van het klant Contact Centrum).
   j. Bedienpost.
   k. Fax Profiel
   l. Drie Standaard vaste Toestellen
   m. Drie Geavanceerd vaste Toestellen.
   n. Standaard headset.
   o. Geavanceerd headset.
   p. DECT headset.

De Opdrachtnemer stelt accountgegevens beschikbaar waarmee de Aanbestedende Dienst op de hiervoor genoemde werkplekken kan inloggen op het systeem, en voorziet de aanwezige medewerkers van de Aanbestedende Dienst indien nodig/gewenst vooraf van een toelichting op het te toetsen platform. Met de accountgegeven kan de Aanbestedende Dienst op de werkplekken inloggen als medewerkers van de twee fictieve gemeenten.

3. **Uitvoering PoD op functionaliteit**
   De PoD wordt door de Aanbestedende Dienst uitgevoerd. De uitvoering duurt, inclusief de terugkoppeling van bevindingen maximaal 2 weken (zie ook paragraaf 4). Tijdens de uitvoering van de PoD dient de Opdrachtnemer beschikbaar te zijn voor het stellen van vragen. Aan het eind van de uitvoering levert de Aanbestedende Dienst een overzicht met bevindingen op, die mondeling wordt toegelicht.
4. **Herstel van bevindingen (indien nodig)**
   Als uit het overzicht met bevindingen functionaliteit blijkt te bestaan die niet of niet voldoende werkt, dan krijgt de Opdrachtnemer de gelegenheid deze functionaliteit alsnog (volledig) werkend te krijgen.
5. **Hertoets op bevindingen (indien nodig)**
   De herstelde functionaliteit wordt opnieuw getoetst. De Aanbestedende Dienst maakt aan het eind van deze hertoets schriftelijk de bevindingen kenbaar aan de Opdrachtnemer. Hierbij wordt tevens aangegeven of de toets op functionaliteit al dan niet succesvol is afgerond.
6. **Toelichtingsgesprek (indien nodig)**
   Indien gewenst kunnen de resultaten worden besproken dan wel van een toelichting worden voorzien.
7. **Afronding PoD op functionaliteit**
   Afhankelijk van de resultaten van de hertoets wordt de PoD afgerond (zie paragraaf 3).

2.3 Toets op beveiliging

2.3.1 Procedure

Voor de toets op beveiliging worden de volgende stappen doorlopen:

1. **Indienen beveiligingsontwerp**

De Opdrachtnemer dient één Werkdag na inwerkingtreding van de Raamovereenkomst een beveiligingsontwerp te verstrekken aan de Opdrachtgever (CBO). Het beveiligingsontwerp is bedoeld als input voor de onafhankelijke partij, die namens de Opdrachtgever in de PoD penetratietesten gaat valideren en uitvoeren (zie ook paragraaf 2.3.2). Het ontwerp geeft voorinformatie waardoor de penetratietesten beter voorbereid en efficiënter uitgevoerd kunnen worden. Eisen waaraan dit ontwerp dient te voldoen zijn beschreven in paragraaf 2.3.3.

2. **Penetratietest door Opdrachtnemer**

Vlak voor vrijgave van het platform voor de PoD voert de Opdrachtnemer zelf een penetratietest uit en levert hiervan een rapportage op. Deze penetratietest is dezelfde test die de Opdrachtnemer (conform eis 7.7.1) gedurende de looptijd van Raamovereenkomst periodiek dient uit te voeren. Doel is dat de Opdrachtgever naast inzicht in eventueel aanwezige zwakheden ook inzicht krijgt in de kwaliteit van de uitgevoerde testen en de op te leveren rapportages.

3. **Kick-off PoD**

Als het platform gereed is voor het uitvoeren van de PoD stelt de Opdrachtnemer o.a. de volgende gegevens beschikbaar:

- Accounts en inloggegevens.
- Technische detailgegevens van koppelvlakken van het platform (URL's, IP-adressen, etc.).
- (Softwarematige) Endpoints.
- Documentatie GT Connect API.

Deze gegevens zijn input voor de onafhankelijke pentester om de testen voor te bereiden.

4. **Validatie penetratietest door onafhankelijke partij namens Opdrachtgever**

De rapportage van de penetratietest door de Opdrachtnemer wordt gevalideerd door een onafhankelijke door de Opdrachtgever ingehuurde partij. Deze vormt een oordeel over de rapportage en de classificatie van de bevindingen (conform CVSS-methodiek).

5. **Penetratietest door onafhankelijke derde partij**

De onafhankelijke door de Opdrachtgever ingehuurde partij voert zelf (een) aanvullende penetratietest(en) (zie paragraaf 2.3.2) uit. De bevindingen van deze test(en) worden samen met bevindingen uit de rapportage over de penetratietest van de Opdrachtnemer samengevoegd in een geconsolideerd rapport. Dit geconsolideerde rapport wordt beschikbaar gesteld aan de Opdrachtnemer. In dit rapport staat aangegeven of de toets op beveiliging al dan niet succesvol is afgerond.

6. **Herstel van bevindingen (indien nodig)**

Als de toets nog niet succesvol is afgerond moet de Opdrachtnemer kritieke kwetsbaarheden met CVSS-score >= 7 herstellen (conform eis 7.7.3). Bij tegenstrijdigheid over de classificatie c.q. de ernst van een kwetsbaarheid prevaleert het oordeel van de onafhankelijke partij.
In deze periode wordt tevens in overleg met de CBO de rapportagevorm voor de periodieke penetratietesten vastgelegd. De Opdrachtnemer zal in het vervolg conform dit vastgelegde formaat over uitgevoerde penetratietesten rapporteren.

7. **Hertoets op bevindingen (indien nodig)**

De kwetsbaarheden die hersteld zijn, worden opnieuw getoetst. Deze hertoets wordt door de onafhankelijke partij uitgevoerd. Ook de resultaten van deze hertoets worden door de onafhankelijke partij in een rapport vastgelegd en aan de Opdrachtgever en Opdrachtnemer opgeleverd. In dit rapport staat aangegeven of de toets op beveiliging al dan niet succesvol is afgerond.

8. **Toelichtingsgesprek (indien nodig)**

Indien gewenst kunnen de resultaten worden besproken dan wel van een toelichting worden voorzien.

9. Afronding PoD op beveiliging

Afhankelijk van de resultaten van de hertoets wordt de PoD afgerond (zie paragraaf 3).

2.3.2 Penetratietest

In de PoD fase worden penetratietesten uitgevoerd om te controleren of de geïmplementeerde oplossing veilig genoeg is om door Deelnemers in gebruik te worden genomen. Deze testen worden in twee stappen uitgevoerd.

Eerst voert de Opdrachtnemer zelf een penetratietest uit en levert hiervan een rapportage op aan de Opdrachtgever. Dit zijn dezelfde testen en rapportages die Opdrachtnemer twee keer per jaar zal uitvoeren op het platform. GT Connect moet blijvend veilig zijn. Informatiebeveiliging vereist continue aandacht en de Opdrachtgever wil controleren of monitoring en controles van de Opdrachtnemer van voldoende kwaliteit zijn, om de veiligheid gedurende de looptijd van de Raamovereenkomst te kunnen blijven waarborgen.

Om de kwaliteit te controleren zal daarna een door de Opdrachtgever ingehuurde onafhankelijke partij, die gespecialiseerd is in het uitvoeren van penetratietesten, de opgeleverde resultaten toetsen op compleetheid en juiste classificatie van geconstateerde zwakheden. Dit gebeurt o.a. door het uitvoeren van (een) additionele penetratietest(en) door deze onafhankelijke partij. Deze partij zal de volgende testen uitvoeren:

- Black box testen op de internet-facing apparatuur
- Grey box testen op user- & admin interfaces
- Grey box testen op VoIP-functies
- Grey box testen op messaging functies
- Grey box testen op API’s
- Grey box testen met fraudescenarios

Hierbij worden eerst (web)applicatie(s) op mogelijke kwetsbaarheden onderzocht. Focus ligt op (web)interfaces waar gebruikersinteractie plaatsvindt. Vervolgens wordt een test uitgevoerd waarbij de testers eerst verifiëren wat iemand zonder inloggegevens kan doen. Het onderzoek wordt daarna gevolgd door een test met inloggegevens. Hiervoor zijn minimaal twee testaccounts per site/ autorisatielaag met vooraf bepaalde privileges (één met gebruikers- en één met beheerautorisatie) nodig om na te gaan hoe een geregistreerde gebruiker misbruik kan maken van de GT Connect-omgeving. Ten slotte zal ook onderzocht worden of via de GT Connect API misbruik gemaakt kan worden van GT Connect.

De onafhankelijke testpartij levert een geconsolideerde rapportage op. Deze bevat de bevindingen uit de rapportage van de Opdrachtnemer, eventueel gecorrigeerd en aangevuld voor wat betreft de classificatie, risico-inschatting en voorgestelde mitigerende maatregelen. Deze bevindingen kunnen aangevuld worden met bevindingen en constateringen door de onafhankelijke testpartij.

2.3.3 Beveiligingsontwerp

Ter voorbereiding op een door een onafhankelijke door de Opdrachtgever ingehuurde partij uit te voeren penetratietest(en), dient de Opdrachtnemer een beveiligingsontwerp aan te leveren. Het beveiligingsontwerp dient minimaal de volgende elementen te bevatten:

- Een ontwerp van GT Connect met componenten en koppelvlakken.
- Een beschrijving van de in te zetten systemen en software.
- Een beschrijving van de in te zetten monitoring- en beheersystemen.
- Een beschrijving van de beveiliging van de volgende koppelvlakken:

    - Koppelvlakken met infrastructuur van Deelnemers.
    - koppelvlakken tussen Deelnemers.
    - koppelvlakken met infrastructuur van derden.
    - koppelvlakken met te koppelen (informatie)systemen.
- Een beschrijving van maatregelen tegen call fraude.
- Een overzicht van de wijze waarop (technische) eisen worden geïmplementeerd/ terugkomen in de oplossing. In het ontwerp moeten minimaal de volgende eisen uit de Conformiteitlijst onderbouwd worden:
    - Toegangsbeveiliging (sectie 7.3).
    - Scheiding van omgevingen (eisen 7.5.1 en 6.4.2).
    - Communicatiebeveiliging (sectie 7.6).
    - Beveiliging van systeem/integratiekoppelingen (eisen 7.7.4 t/m 7.7.6).
    - Bescherming tegen DDoS-aanvallen (eis 7.10.2).

3 Afronden van de Proof of Delivery

De PoD bestaat uit twee delen; een toets op functionaliteit en een toets op beveiliging. De PoD is geslaagd als beide delen succesvol zijn afgerond, en is mislukt als één deel of beide delen niet succesvol is/zijn afgerond.

Als de Opdrachtnemer er niet in slaagt om beide delen van de PoD succesvol af te ronden, dan zal de Raamovereenkomst worden beëindigd.
Als op het moment van beëindigen van de Raamovereenkomst een Schaduwovereenkomst aanwezig is, dan zal de Schaduwovereenkomst de Raamovereenkomst vervangen. In dat geval zal opnieuw een PoD worden uitgevoerd, dit keer met de Inschrijver die de Schaduwovereenkomst gegund heeft gekregen. Als de PoD onder Schaduwovereenkomst ook niet succesvol wordt afgerond, dan zal ook de Schaduwovereenkomst worden beëindigd.
Als op het moment van beëindigen van de Raamovereenkomst geen Schaduwovereenkomst aanwezig is, of als ook de PoD onder de Schaduwovereenkomst niet succesvol is, dan kan de Aanbestedende Dienst besluiten de opdracht opnieuw in de markt te zetten.

4 Tijdschema

	Start	Eind	18-3 t/m 24-3	25-3 t/m 31-3	1-4 t/m 7-4	8-4 t/m 14-4	15-4 t/m 21-4	22-4 t/m 28-4	29-4 t/m 5-5	6-5 t/m 12-5	13-5 t/m 19-5	20-5 t/m 26-5	27-5 t/m 2-6	3-6 t/m 9-6	10-6 t/m 16-6	17-6 t/m 23-6	24-6 t/m 30-6	1-7 t/m 7-7	8-7 t/m 14-7	15-7 t/m 21-7
Start Raamovereenkomst/PoD	-	22-mrt																		
Opbouw platform	22-mrt	17-mei																		
Toets op Functionaliteit:																				
Overhandiging PoD lijst	-	25-mrt																		
Start en uitvoering functionele PoD	20-mei	2-jun																		
Herstel van bevindingen	3-jun	16-jun																		
Hertoets en toelichtingsgesprek	17-jun	30-jun																		
Afronding PoD functionaliteit	1-jul	5-jul																		
Toest op beveiliging:																				
Inleveren beveiligingsplan		25-mrt																		
Pentest + rapportage Opdrachtnemer	-	17-mei																		
Kickoff PoD	20-mei	20-mei																		
Validatie pentest Opdrachtnemer	20-mei	16-jun																		
Pentest onafhankelijke partij	20-mei	16-jun																		
Herstel bevindingen (indien nodig)	17-jun	30-jun																		
Hertoets en toelichtingsgesprek	1-jul	14-jul																		
Afronding PoD beveiliging	15-jul	17-jul																		

De PoD gaat volgens bovenstaande tijdschema op vrijdag 22 maart van start, gelijktijdig met de geplande inwerkingtreding van de Raamovereenkomst. Als de inwerkingtreding van de Raamovereenkomst echter later dan 22 maart 2019 plaatsvindt, dan gaat de PoD van start op de eerste vrijdag die gelijk valt met of volgt op de nieuwe datum van inwerkingtreding van de Raamovereenkomst. Alle overige in het tijdschema opgenomen data verschuiven dan met hetzelfde aantal dagen als het aantal dagen waarmee de start van PoD is uitgesteld.

Als de PoD niet succesvol wordt afgerond en er in het kader van de Schaduwovereenkomst een nieuwe PoD opgestart dient te worden, dan zal deze nieuwe PoD van start gaan op de eerste vrijdag die volgt op de datum waarop de eerste PoD definitief is mislukt en de Schaduwovereenkomst in de plaats is gekomen van de originele Raamovereenkomst. Alle in het overzicht opgenomen data zullen in dat geval vanaf deze nieuwe startdatum op een zodanige wijze worden doorgerekend dat dezelfde termijnen ontstaan voor zowel alle genoemde onderdelen van de PoD en als voor de perioden tussen de onderdelen.

Om praktische redenen kan De Opdrachtgever in overleg met de Opdrachtnemer besluiten om in het schema opgenomen start- of einddata enkele dagen te verschuiven. Het is echter niet mogelijk om de totale termijn waarbinnen de PoD dient plaats te vinden te verlengen.