Nota van inlichtingen 1 – Toegangscontrolesysteem – Gemeenten DOWR

30-01-2026

Begin nota van inlichtingen:

De bijlagen bij deze nota worden toegestuurd, mocht u deze niet hebben ontvangen horen wij dit graag via schijndel@inkada.nl

Nr.	Pag.	Par.	Vraag	Antwoord
Aanbestedingsleidraad				
1.		Algemeen	Kunt u ons tekeningen (plattegronden) aanleveren in DWG formaat?	Nee, de DWG documenten worden verstrekt na gunning opdracht.
2.		Algemeen	Kunt u ons Kabelgoten tekeningen (plattegronden) aanleveren in DWG formaat?	Zie vraag 1.
3.		Algemeen	Kunt u tekeningen aanleveren waarop de locaties staan aangeven waar de apparatuur van het toegangscontrolesysteem (versie asbuild) zich bevindt?	Paslezers zijn op de opvraagbare tekeningen aangegeven en blokschema's zijn beschikbaar. Geen As-Built dossier.
4.		Algemeen	Hoe dient de aannemer van het bestek om te gaan, zoals tijdens de schouw is getoond in het Gemeentehuis Deventer, met het gecombineerde systeem (inbraak en toegangscontrole)?	Dit zal zijn in gezamenlijkheid met de huidige leverancier met als doel een soepele overgang.
5.		Algemeen	Kunt u ons het type kaartlezer en het type kabel van de kaartlezer aanleveren i.v.m. OSDP (communicatie protocol tussen kaartlezer en onderstation)?	Type kabel KL, zie blokschema, type KL Deventer: type HID Global RW100; Raalte: EAL Olst/Wijhe: XMP-TMC2250 Voor de gemeentewerf Olst-Wijhe kunnen we daarnaast meegeven dat systeem ATS8520 de Eindgebruikers Software is van de huidige leverancier.
6.	6	2.1	Zijn er tekeningen met locaties van centrale hardware incl. posities kaartlezers van de verschillende locaties? Tevens willen wij graag blokschema's ontvangen van de opbouw van de toegangscontrole-installaties	Zie antwoord 3.
7.	6	2.1	Maken de huidige kaartlezers van de locaties gebruik van het Mifare Classic protocol?	Ja, zie antwoord 44.

8.	6	2.1	Kunt u aangeven welke deuren en evt. hek/slagbomen er bij de gemeentewerf in Raalte van toegangscontrole voorzien dienen te worden?	Zie toegestuurde bijlagen.
9.	6	2.1	Zijn er tekeningen beschikbaar van kabeltracés (kablgoten e.d.) i.v.m. de gevraagde uitbreiding van deuren?	Zie vraag 1 en 2.
10.	13-14	5.4.3	Aan het begin van de schouw op locatie is aangegeven dat bepaalde normeringen in deze paragraaf komen te vervallen. Kunt u aangeven welke komen te vervallen?	Er zijn wijzigingen geweest die gerectificeerd zijn. Het document dat op 8 januari is gepubliceerd bevat de geldende geschiktheidseisen (kerncompetenties en ISO27001).
11.	13	5.4.3	In paragraaf 5.4.3 wordt gevraagd om een referentieproject van minimaal 3 gebouwen met totaal minimaal 16 deuren, terwijl de omvang van de opdracht meer dan 200 deuren en bijna 4000 gebruikers betreft.	Zie antwoord 12.
12.	13	5.4.3	Kunt u toelichten hoe deze referentie-eis zich verhoudt tot de omvang en complexiteit van de opdracht?	Het doel is om aan te tonen dat inschrijvers relevante ervaring hebben met toegangscontrole over meerdere gebouwen en deurpunten met één centraal systeem. Dit is in lijn met de complexiteit van deze opdracht.
13.	18	5.5.3	Kunt u wat meer informatie geven over wat u bedoelt met “Het proces van uitschakelen van een gebruiker en doorwerking op andere processen”?	Wanneer wij spreken over “het proces van uitschakelen van een gebruiker en doorwerking op andere processen”, gaat het in de kern om het volledig beëindigen van toegang zodra een account in Microsoft Entra Identity wordt gedeactiveerd. Het toegangscontrolesysteem moet daarom gekoppeld zijn aan Entra en real-time reageren op wijzigingen in de identity-provider. Op het moment dat een gebruiker in Entra wordt uitgeschakeld, mag er nergens vertraging of caching ontstaan waardoor fysieke toegang nog mogelijk is. Er mag dus geen lokale kopie van rechten blijven bestaan binnen het toegangscontroleplatform die pas later wordt bijgewerkt. De deactivatie moet direct zichtbaar zijn voor het toegangscontrolesysteem en onmiddellijk leiden tot het intrekken van alle autorisaties zoals deurprofielen, zones, rollen en eventuele tijdelijke rechten.

Bijlage 1. Programma van Eisen				
14.	1	Eis 4	Bij toevoeging “onder dezelfde condities” en kosteloos verwijderen: wilt u een volumecorridor (±20%) en prijsherijking/afkoopsom opnemen bij substantiële scope-wijziging i.v.m. vaste kosten, SROI-last en licentiecommitments?	De wijzigingen dienen binnen de kaders van de wezenlijke wijziging te blijven.
15.	1	Eis 5	Veel werkzaamheden kunnen onder eigen beheer uitgevoerd worden, maar het infrezen o.i.d. van elektrische sloten e.d. niet. Er zijn echter zeer weinig bouwkundige bedrijven die een ISO27001 certificaat hebben. Hoe gaan wij hier mee om?	De ISO27001-eis geldt alleen voor de inschrijver en de digitale keten van het toegangscontrolesysteem. Bouwkundige partijen die uitsluitend fysieke werkzaamheden uitvoeren vallen buiten deze verplichting. De inschrijver blijft daarbij volledig verantwoordelijk als hoofdaannemer voor beveiliging, coördinatie en correcte uitvoering van alle werkzaamheden, ook die van ingeschakelde onderaannemers.
16.	1	Eis 7	Personeel dient in bezit te zijn van een geldige VOG. Kunt u bevestigen dat een VOG zoals hier benoemd maximaal 4 jaar oud mag zijn?	Dit wordt niet bevestigd. Het gaat om dat de VOG geldend moet zijn. Opdrachtnemer is verantwoordelijk om deze periodiek controleren en opnieuw opvragen.
17.	2	Eis 10	Welke hardware wordt er bedeld bij eis 10? Kunnen we ervan uit gaan dat hiermee de server bedoeld wordt?	Indien een fysieke appliance wordt geplaatst die via een beveiligde VPN-tunnel bijvoorbeeld toegangsdeuren ontsluit en beheerbaar maakt binnen het SaaS-portaal, wordt deze appliance als zelfstandig component geplaatst in een technische ruimte van Opdrachtgever, en centraal beheerd door Inschrijver. Hierbij zal geen installatie van software op lokale servers toe worden gestaan.
18.	2	Eis 10	Kan de opdrachtgever bevestigen dat voor de prijsvorming alle bestaande hardware voor toegangscontrole (deurcontrollers) op dit moment reeds in afgeschermde ruimtes is geplaatst of dient dit te worden gerealiseerd als dusdanig?	Alle bekabeling gaat naar de serverruimte. Op dit moment zijn er geen draadloze oplossingen binnen de organisatie. Mogelijk kan dit anders zijn in de toekomst.
19.	2	Eis 10	Kan de opdrachtgever bevestigen dat eventueel netwerkvoorzieningen (incl. bekabeling) door de opdrachtgever worden verzorgd en buiten scope van de opdrachtnemer liggen?	Binnen dit traject mag worden uitgegaan van het uitgangspunt dat de benodigde fysieke netwerkaansluitingen door de opdrachtgever worden verzorgd. Indien specifieke situaties vragen om aanvullende netwerkapparatuur die niet door de opdrachtgever wordt geleverd, kan de Inschrijver deze

				componenten onder vooraf overeengekomen technische en functionele voorwaarden zelf leveren.
20.	2	Eis 14	Dienen deze kritieke ruimtes te worden goedgekeurd door het aanbieden van de fysieke pas van de groepsmanager of dient dit in de software uitgevoerd te worden door de groepsmanager?	Het systeem ondersteunt een volledig configureerbare autorisatieflow voor toegang tot kritieke zones. Bij iedere aanvraag voor ruimtes met verhoogde beveiligingsklasse, zoals server- en technische ruimtes, wordt het vier-ogen-principe afgedwongen. Dit betekent dat aangevraagde rechten niet automatisch of direct worden doorgevoerd. In plaats daarvan wordt eerst een autorisatiestroom gestart waarin een bevoegde rol, zoals de groepsmanager IT Beheer, de aanvraag expliciet moet valideren. Pas na deze goedkeuring worden de betreffende toegangsrechten geactiveerd binnen het toegangscontrolesysteem.
21.	2	Eis 14	Kunt u duiden wat u verstaat onder “aanvraag”?	Het systeem ondersteunt een volledig configureerbare autorisatieflow voor toegang tot kritieke zones. Bij iedere aanvraag voor ruimtes met verhoogde beveiligingsklasse, zoals server- en technische ruimtes, wordt het vier-ogen-principe afgedwongen. Dit betekent dat aangevraagde rechten niet automatisch of direct worden doorgevoerd. In plaats daarvan wordt eerst een autorisatiestroom gestart waarin een bevoegde rol, zoals de groepsmanager IT Beheer, de aanvraag expliciet moet valideren. Pas na deze goedkeuring worden de betreffende toegangsrechten geactiveerd binnen het toegangscontrolesysteem.
22.	2	Eis 16	Er wordt gesproken over SKG normen, welke normen worden er geëist (ook vanuit de verzekering)	OG gaat 1 op 1 over met de gebruikte sloten. Bij vervanging, wat niet van toepassing is op de huidige sloten, geldt dat voor de buitendeuren 3 sterren SKG normen gehanteerd moet worden.
23.	2	Eis 19	Opdrachtnemer dient opdrachtgever na afloop van de werkzaamheden te informeren over de uitgevoerde werkzaamheden. Niet vermeld staat op welke wijze dit plaats dient te vinden en of hiervoor ook getekend moet worden. Hoe wordt deze afstemming gewaarborgd?	Dit wordt na gunning afgestemd, en OG ontvangt dan ook graag een voorstel over wat ON werkbaar vindt.

24.	2	Eis 21/22	Bevestigt u dat preventief onderhoud dat storingsgevoelig is buiten het productievenster (22:00–06:00) mag plaatsvinden mét beperkte, vooraf afgestemde impact, en dat “geen hinder” overdag redelijkerwijs wordt geïnterpreteerd (geen zero-impact garantie)?	Dit hangt af van de (mate) van hinder. Dit is naar oordeel van OG. Waar mogelijk wordt onderhoud overdag uitgevoerd binnen de productievensters.
25.	3	Eis 25-29	Worden service credits als exclusieve financiële remedie bij SLA-onderprestatie geïntroduceerd (met maand/jaar-cap), en wordt cumulatie met boetes/schade voor hetzelfde feit uitgesloten?	Nee, als de SLA afspraken niet gehaald worden komt ON met een verbeterplan. Dit laat de werking van de algemene voorwaarden onverlet.
26.	3	Eis 26	Klopt het dat de KPI gemeten wordt door het houden van audits door de Opdrachtgever bij de Opdrachtnemer?	Nee, het is aan ON om de prestatie van de KPI's aantoonbaar te maken.
27.	4	Eis 37	Wij verzoeken u de voorgestelde betalingsstructuur te herzien, aangezien de huidige verdeling (30% vooraf en 70% na volledige oplevering) leidt tot een disproportionele financiële belasting aan het einde van het traject/contractjaar. Deze opzet sluit bovendien onvoldoende aan op de feitelijke fasering van het werk. Om tot een evenwichtiger en conforme betalingsregeling te komen, stellen wij de volgende structuur voor: • 40% bij het sluiten van de overeenkomst • 30% na het verstrijken van 30% van de tijdsduur van het werk • 25% na het verstrijken van 60% van de tijdsduur van het werk • 5% bij bedrijfsklare oplevering Hierbij de vraag of bovenstaande betaling structuur akkoord is?	Dit is niet akkoord.
28.	4	Eis 38	Vanaf welk moment mogen we deze maandelijkse kosten factureren? Vanaf 01-05-2026 of na acceptatie van de pilot zoals genoemd in eis 37?	Na acceptatie.
29.	4	Eis 38	Heeft deze eis alleen betrekking op Software of ook op (preventief en correctief) onderhoud aan hardware	Op beide.
30.	4	Eis 39	U geeft bij deze eis aan “Opdrachtnemer factureert na uitvoering van het werk de kosten voor het correctieve onderhoud”. Echter u vraagt all-in prijzen voor onderhoud	Dat is correct. Eis 39 vervalt. Dit wordt geëvalueerd tijdens het jaarlijks contractgesprek.

			die we per maand moeten afprijzen. Hoe verhoudt zich dat tot deze eis? Deze eis lijkt dan niet van toepassing	
31.	4	Eis 40	Aangegeven wordt dat op de factuur de WBS code van opdrachtgever per locatie moet worden vermeld. Kunt u bevestigen dat deze WBS code voorafgaand aan uitvoering van het werk aan opdrachtnemer ter beschikking is gesteld en wilt u dan ook aangeven op welke manier?	Ja per mail tijdens de implementatie.
32.	4	Eis 40	Aangegeven wordt dat de factuuradresgegevens zijn opgenomen in de Overeenkomst, bijlage 2A. Daarin staan echter geen adresgegevens vermeld, graag bijlage 2A nog verder aanvullen met gegevens.	Dit volgt na gunning, dit wordt verstrekt via het Inkoopnummer (PO).
33.	5	Eis 41	In de huidige bepaling wordt aangegeven dat de indexatie pas vanaf 2028 kan worden toegepast. Gezien de aard van het werk en de marktontwikkelingen achten wij het wenselijk om de indexatie reeds vanaf 2027 te laten ingaan. Dit draagt bij aan een nauwkeuriger en marktconforme inschrijving en voorkomt dat inschrijvers een aanvullende risicopost moeten opnemen voor de periode waarin nog geen indexatie kan worden doorgevoerd, hetgeen de transparantie en vergelijkbaarheid van de inschrijvingen bevordert. Kunt u aangeven of een eerdere ingangsdatum van de indexatie, namelijk per 2027, binnen de kaders van deze tender is toegestaan.	Niet akkoord. Er kan pas geïndexeerd worden nadat een contract minimaal een jaar in werking is.
34.	5	Eis 41	In de huidige bepaling wordt verwezen naar het CBS-prijsindexcijfer voor “Financiële en zakelijke diensten” binnen de branche “IT en informatiedienstverlening”. Deze index sluit niet aan op de aard van de werkzaamheden zoals omschreven in het ontwerp. Gezien de technische inhoud en uitvoeringskarakteristieken van het werk achten wij het passender om te indexeren op basis van de CAO-lonen, contractuele loonkosten en arbeidsduur (index 2020=100) voor Bedrijfstak 24–30, 33 Metaal & Elektro (contractuele	Niet akkoord.

			loonkosten per maand – totale CAO-sector; peildatum september–september). Bent u akkoord met deze indexatie?	
35.	5	Eis 41	Is de aanname juist dat deze index toegepast mag/moet worden op alle maandelijkse kosten die we moeten afprijzen in Bijlage 4? Dus ook de maandelijkse licentiekosten, preventief en correctief onderhoud?	Dit is correct.
36.	5	Eis 45	Geldt de samenwerking als gezamenlijke inkoop, maar losstaande domeinen en SaaS-omgevingen? Of wordt er gezamenlijk gebruik gemaakt van één en dezelfde SaaS-omgeving?	De samenwerking betreft een gezamenlijke inkoop, waarbij de opdrachtgever één centraal SaaS-portaal wil voor alle DOWR-gemeenten. Binnen dit portaal moeten de gemeenten afzonderlijk én overstijgend beheerd kunnen worden, zodat zowel beheer per gemeente als DOWR-brede autorisaties mogelijk zijn. Tags/passen moeten daarbij rechten kunnen krijgen die over meerdere gemeenten gelden. De volledige DOWR-omgeving, inclusief de IDP-koppeling, moet fysiek of logisch gescheiden zijn van andere klanten van de Inschrijver.
37.	5	Eis 45	U beschrijft de toegangscontrolesysteem als een SaaS-oplossing af te willen nemen. Het concept SaaS wordt in de markt op 2 verschillende manieren geïnterpreteerd/aangeboden aan eindgebruikers. Hoewel het beide technisch als een SaaS dienst omgeschreven zou kunnen worden, is het kwaliteitsniveau van de dienst totaal verschillend door de toegepaste technologie; Optie 1; Hosted oplossing van een on-premise applicatie waarbij een traditionele applicatie (ontwikkelt voor on-premise deployments) wordt gehost in een extern datacenter en als dienst wordt aangeboden aan de eindgebruiker. Optie 2; Hosted oplossing o.b.v. een Cloudprovider i.c.m. een applicatie/platform ontwikkelt vanuit een Cloud Service/Continous Delivery. Oplossing waarbij o.b.v. Cloud technologie van een Cloud Provider (b.v. Microsoft Azure, AWS of Google) een SaaS oplossing wordt geleverd van een speciaal voor Cloud ontwikkeld software platform.	De opdrachtgever staat niet beide modellen toe. Zoals tevens beschreven in eis 64 moet de SaaS-oplossing volledig webnative en webresponsive zijn, toegankelijk via moderne webbrowsers en zonder afhankelijkheid van een traditionele applicatie. Hierdoor past alleen het cloud-native SaaS-model (Optie 2) binnen de gevraagde architectuur en kwaliteitseisen. Een gehoste on-premise applicatie (Optie 1) sluit hier niet op aan.

			Staat de opdrachtgever een SaaS oplossing toe op basis van beide modellen? Zo niet, welk model heeft de voorkeur en op welke wijze wordt de kwaliteit en wijze van exploitatie van de SaaS dienst meegenomen in de beoordeling?	
38.	5	Eis 51	Dienen we uit te gaan van 1 Identity provider of meerdere?	Er wordt uitgegaan van één centrale Identity Provider: Microsoft Entra ID. Alle deelnemende gemeenten werken binnen dezelfde gedeelde Entra-omgeving, waarbij de scheiding tussen gemeenten binnen deze IdP-structuur is ingericht. Het toegangscontrolesysteem koppelt daarom met deze ene centrale IdP voor productie. Indien de inschrijver een test- of acceptatieomgeving aanbiedt, dan moet de oplossing bij voorkeur kunnen koppelen met de test-tenant van de opdrachtgever zodat functionaliteit buiten productie gevalideerd kan worden.
39.	5	Eis 51	Wat zijn de uitgangspunten voor RBAC? Dienen we bijvoorbeeld uit te gaan van 1 HR-koppeling (Alleen Youforce) of meerdere (per gemeente een andere HR-koppeling). Kunt u schematische weergave aanleveren van de gewenste situatie?	De uitgangspunten voor RBAC zijn dat het toegangscontrolesysteem aansluit op Microsoft Entra ID als centrale bron voor identiteit. De IdP-koppeling levert gebruikersinformatie inclusief groepslidmaatschappen mee in de claim richting de software voor toegangscontrole. Deze groepen kunnen, indien gewenst en in overleg, worden gebruikt voor de toekenning van rollen en functies binnen de software. Dit kan echter leiden tot een omvangrijke set Entra-groepen die gekoppeld worden aan de IdP-koppeling. Een alternatief is om slechts enkele Entra-groepen te gebruiken voor de basisautorisatie en binnen de toegangscontrole-software zelf verder te differentiëren op rol- of functieniveau. De RBAC-structuur wordt daarmee gevoed vanuit Entra, maar binnen de toegangscontrole vertaald naar de juiste toegangsniveaus.
40.	6	Eis 59	Wat is de reden dat de logging minimaal 3 jaar bewaart moet worden in plaats van bijvoorbeeld 1 jaar. Bent u bereid de eis aan te passen naar 1 jaar aangezien logging van 3 jaar kostenverhogend werkt?	De retentieperiode van drie jaar is noodzakelijk om beveiligingsincidenten technisch volledig en aantoonbaar te kunnen analyseren. Incidenten rondom ongeautoriseerde toegang worden in de praktijk vaak pas later zichtbaar, waardoor langere historische logdata nodig is voor reconstructie, correlatie en verificatie. Deze termijn sluit direct aan op de wettelijke zorgplicht rond

				informatiebeveiliging en het kunnen onderbouwen van incidentonderzoek. Een jaar retentie biedt daarvoor onvoldoende historische diepgang. Drie jaar blijft daarom de minimale retentietermijn voor alle relevante toegangs- en auditlogs.
41.	6	Eis 59	Een logretentie periode van 3 jaar is bovengemiddeld lang. Is deze eis van toepassing op alle events/ transacties van het systeem (incl. toegangsbewegingen op basis van pasgebruik) of geldt de retentieperiode van 3 jaar enkel voor de audit trail (mutaties in het systeem van applicatiegebruikers)?	De retentieperiode van drie jaar is noodzakelijk om beveiligingsincidenten technisch volledig en aantoonbaar te kunnen analyseren. Incidenten rondom ongeautoriseerde toegang worden in de praktijk vaak pas later zichtbaar, waardoor langere historische logdata nodig is voor reconstructie, correlatie en verificatie. Deze termijn sluit direct aan op de wettelijke zorgplicht rond informatiebeveiliging en het kunnen onderbouwen van incidentonderzoek. Een jaar retentie biedt daarvoor onvoldoende historische diepgang. Drie jaar blijft daarom de minimale retentietermijn voor alle relevante toegangs- en auditlogs.
42.	6	Eis 65	Gebruik van wildcard certificaten is gebruikelijk in moderne (publieke) Cloud services. Is het gebruik van wildcard certificaten toegestaan als de opdrachtnemer kan aantonen dat deze oplossing op een dusdanig wijze is geïmplementeerd dat eventuele cyber security risico's aan het gebruik hiervan juist zijn gemitigeerd?	De eis blijft van kracht omdat wildcard-certificaten in een multi-tenant omgeving het risico vergroten dat één gecompromitteerde sleutel impact heeft op meerdere klanten. Het centrale toegangsportaal vormt hierop een uitzondering, omdat dit slechts één gecontroleerd entrypoint betreft en geen directe toegang biedt tot API-verkeer. Voor alle API's en achterliggende services blijven uitsluitend domein-specifieke certificaten toegestaan.
43.	6	Eis 65	Wat is de reden waarom u dit eist? Bent u bereid deze eis te laten vervallen aangezien veel gerenommeerde SaaS oplossingen met een wildcard werken	De eis blijft van kracht omdat wildcard-certificaten in een multi-tenant omgeving het risico vergroten dat één gecompromitteerde sleutel impact heeft op meerdere klanten. Het centrale toegangsportaal vormt hierop een uitzondering, omdat dit slechts één gecontroleerd entrypoint betreft en geen directe toegang biedt tot API-verkeer. Voor alle API's en achterliggende services blijven uitsluitend domein-specifieke certificaten toegestaan.

44.	7	Eis 72	Dient alleen de tag te voldoen aan Mifare Desfire EV3 en de kaartlezers, draadloos deurbeslag, ed. niet?	De eis heeft uitsluitend betrekking op de toegangstag (of pas), die gebaseerd is op MIFARE DESFire EV3. De gebruikte lezers, het draadloos deurbeslag en andere componenten binnen de toegangscontroleomgeving moeten deze EV3-tags kunnen verwerken binnen de daarvoor gebruikelijke beveiligde communicatie. Het uitgangspunt is dat dezelfde EV3-tag wordt toegepast voor zowel fysieke toegangsverlening als aanvullende voorzieningen, zoals gebruikersauthenticatie op centrale printers en andere systemen die kaart-gebaseerde identificatie gebruiken.
45.	7	Eis 77	Kunt u bevestigen dat SROI wordt berekend over de feitelijk gerealiseerde omzet per jaar, en bij substantiële scope-krimp of beëindiging pro rata wordt aangepast?	De Social Return on Investment (SROI)-verplichting wordt vastgesteld op basis van de geraamde opdrachtsom. Indien gedurende de uitvoering van de overeenkomst blijkt dat de daadwerkelijk gerealiseerde omzet substantieel afwijkt van de oorspronkelijk begrote contractwaarde, kan de SROI-verplichting evenredig worden herijkt, zowel in positieve als in negatieve zin. Dus: Indien gedurende de looptijd van de overeenkomst sprake is van een substantiële wijziging van de scope, zoals scope-krimp, of van (gedeeltelijke) beëindiging van de overeenkomst, wordt de SROI-verplichting pro rata aangepast op basis van de daadwerkelijk gerealiseerde omzet over de betreffende periode.
Bijlage 2A. Overeenkomst				
46.	2	Art. 2.2	Aanbesteder is op zoek naar een partnerschap. Het eenzijdig recht van Aanbesteder om de overeenkomst na 5 jaren te verlengen verhoudt zich daarmee slecht. In het onverhoopte geval dat de samenwerking voor Opdrachtnemer onhoudbaar is, heeft hij geen rechten om een verlenging te weigeren. Ook kan Opdrachtnemer niet over een termijn van maximaal 9 jaren overzien hoe de markt eruit ziet. Daarmee kan de aanbieding – ondanks een evenwichtige indexmogelijkheid – geen rekening houden. Een en ander zal noodgedwongen leiden tot onnodige prijsopdrijvende effecten. Kan Aanbesteder instemmen dat	Het is akkoord dat voor de tweede verlenging door beide partijen formeel akkoord moeten gaan. Mocht de samenwerking in eerder stadium voor ON onwerkbaar zijn dan is dat uiteraard bespreekbaar om het partnerschap te herstellen.

			beide partijen na de initiële termijn van 5 jaren dienen in te stemmen met een verlenging?	
47.	3	Art 3.6	Betaling vindt plaats binnen 30 dagen na ontvangst en goedkeuring van de factuur. Kunt u bevestigen dat u de factuur binnen 1 week heeft goed of afgekeurd met reden?	Nee dit kan niet worden bevestigd. OG streeft uiteraard naar tijdige betaling.
48.	3	Art. 4.2	Kan Aanbesteder ondubbelzinnig opnemen op welke specifieke leveringen deze fatale termijnen van toepassing zijn. Geldt dit enkel voor de datum van het bedrijfsklaar opleveren van het toegangssysteem? Zo ja, kan - gelet op de impact - voor de overige termijnen een streefdatum worden gehanteerd?	Dit geldt voor het bedrijfsklaar opleveren. Het is niet akkoord dat de overige termijnen als streefdatums worden beschouwd. Bij het niet behalen volgt een ingebrekestelling met een hersteltermijn (door OG te bepalen). In artikel 4.1 is opgenomen dat de bepaling van de data gezamenlijk wordt overeengekomen, dus mag ook worden verwacht dat ON een reëel en haalbaar voorstel hierin doet.
49.	3	Art 4.3	Een boete is verschuldigd ter hoogte van 2,5% van “het te laat geleverde” per dag tot maximaal 20% van de waarde ervan en onverkort eventuele schade door de late levering. Indien de bepaling betrekking heeft op de gehele installatie, geldt dat deze boetebepaling de redelijkheidstoets niet doorstaat. Kan Aanbesteder specifiek maken voor welke leveringen deze exorbitante boete zou moeten gelden? Hoe verhoudt deze boete zich voorts tot artikel 8 van de concept Overeenkomst? Kan Aanbesteder de percentages fors matigen en het totaal maximaliseren tot 5% en de mogelijkheid de overige schade te verhalen schrappen OF de boete schrappen en de schade in stand houden?	Dit geldt voor de fatale termijn zoals bedoeld in antwoord 48.
50.	4	Art. 9.4	Kan Aanbesteder toelichten wat precies wordt bedoeld met “voordeel”? Bedoelt Aanbesteder dat Partijen per beëindigingsdatum afrekenen naar de stand van het werk?	Dit is correct.
51.	5	Art. 10.2	Kan Aanbesteder bepalen dat de vrijwaring wordt beperkt tot de hoogte van de tussen partijen overeengekomen aansprakelijkheid, waarbij de beperking (redelijkerwijs) niet ziet op de aansprakelijkheid zoals genoemd in de slotzin van dit lid? Dit voorkomt dat Opdrachtnemer wordt gedwongen meer aansprakelijkheid te aanvaarden dan hij wettelijk heeft.	Dit is niet akkoord.

52.	5	Art. 10.4	Aanbesteder exonereert zich voor elke aansprakelijkheid buiten zijn bewuste en opzettelijke gedragingen. Dit is niet redelijk. Indien Aanbesteder schade veroorzaakt, die aan hem is toe te rekenen, moet hij daarop kunnen worden aangesproken. Opdrachtnemer meent dat ook hier een limiet kan worden afgestemd. Kan Aanbesteder zich erin vinden dat wij over en weer eenzelfde beperking van aansprakelijkheid hanteren in overeenstemming met de eerste drie leden van het bepaalde in art. 10?	Dit is niet akkoord.
Bijlage 4. Prijzenblad				
53.		Algemeen	U geeft aan dat we qua kosten rekening moeten houden dat de oplossing 15 jaar probleemloos operationeel moet functioneren. Voor IP-gebaseerde hardware betekent dit in de praktijk dat, vanuit cybersecurity-oogpunt, vervanging binnen deze termijn noodzakelijk is vanwege het wegvallen van beveiligingsupdates, firmware-ondersteuning en compliance met actuele securitystandaarden. Technisch gezien is 15 jaar wel realiseerbaar. Kunt u aangeven hoe u naar dit aspect kijkt met betrekking	De gevraagde operationele levensduur van vijftien jaar ziet primair op de continuïteit van de oplossing als geheel, niet op het statisch in stand houden van individuele IP-componenten zonder lifecycle-beheer. Voor IP-gebaseerde hardware is het vanzelfsprekend dat gedurende deze periode regulier onderhoud, firmware-updates, componentvervanging en security-aligned lifecycle-management noodzakelijk zijn om te blijven voldoen aan actuele beveiligingsnormen en ondersteuning te behouden. Het uitgangspunt is dat de gekozen techniek en architectuur over deze volledige periode veilig en functioneel inzetbaar blijft, waarbij vervanging van hardware-onderdelen mogelijk onderdeel is van de normale exploitatie. De levensduur ziet daarmee op duurzame operationele stabiliteit en niet op het voorkomen van hardware-vervanging vanuit security- of compliance-overwegingen.
54.		Algemeen	De gevraagde eenheidsprijzen zijn niet uniform te bepalen. Om een goede vergelijking te maken tussen de inschrijvers is het vereist duidelijke uitgangspunten te benoemen en/of meer vrijheid van prijsopgave te kunnen geven. Kunt u dit aanpassen in de aanbestedingsstukken?	Dit is niet akkoord. De uitgangspunten zijn in het prijzenblad weergegeven en vormen voor partijen een gelijke opbouw van de inschrijfprijs. U dient een open calculatie bij het prijzenblad te voegen om een onderbouwing te geven van de totaalbedragen.
55.		Algemeen	Kunnen jullie op tekeningen aangeven welke deuren er draadloos dienen te worden?	Nee, op dit moment zijn er geen deuren die draadloos zijn.

56.	Regel 20	Implementatiekosten	Mogen wij ervan uitgaan dat de benodigde netwerkaansluitingen door de opdrachtgever worden verzorgd?	Binnen dit traject mag worden uitgegaan van het uitgangspunt dat de benodigde fysieke netwerkaansluitingen door de opdrachtgever worden verzorgd. Indien specifieke situaties vragen om aanvullende netwerkapparatuur die niet door de opdrachtgever wordt geleverd, kan de Inschrijver deze componenten onder vooraf overeengekomen technische en functionele voorwaarden zelf leveren.
57.	Regel 23	Kaartlezers	U vraagt 160 kaartlezers. Kunt u bevestigen dat dit de bestaande kaartlezers zijn en exclusief eventuele extra nieuwe kaartlezers. Waar dienen we de extra nieuwe kaartlezers te werken qua prijs?	Het aantal kaartlezers in het prijzenblad staat op 106 i.p.v. 160. In het prijzenblad dient u een prijs per eenheid in, die geldend is voor implementatie en gedurende de looptijd.
58.	Regel 24-25	Hardware	Waar staat de afkorting PVK voor?	Dit staat voor Potentiaal Vrij Kontakt en houdt in dat dat de deur te bedienen valt, na bijv. Kortsluiting).
59.	Regel 24-25	Hardware	Waar staat de afkorting ‘PVK’ voor?	Zie antwoord 58.
60.	Regel 24	Bekabeld slot	U vraagt de prijs voor een elektronisch slot bekabeld, maar specificaties en montage-omstandigheden ontbreken in het PvE. Kunt u aangeven welk type elektronisch slot wordt bedoeld en onder welke omstandigheid (type deur/kozijn etc.) dit slot moet worden gemonteerd, zodat inschrijver een juiste prijs kan bepalen?	Uitvraag behelst een standaardoplossing met oog op uitbreidingen. Stuks prijs is incl. lokale bekabeling, montage en inbedrijfstelling. Excl. bouwkundige aanpassingen en horizontale bekabeling.
61.	Regel 25	Draadloos slot	U vraagt de prijs voor een elektronisch slot draadloos, maar specificaties en montage-omstandigheden ontbreken in het PvE. Kunt u aangeven welk type elektronisch slot wordt bedoeld en onder welke omstandigheid (type deur/kozijn etc.) dit slot moet worden gemonteerd, zodat inschrijver een juiste prijs kan bepalen?	Zie het antwoord op vraag 60.
62.	Regel 25	Draadloos slot	Kunt u meer informatie aanleveren over het gebruik van draadloos slot. Op welke locatie en op welke ruimtes moeten ze gemonteerd worden.	Zie vraag 55.

63.	Regel 26	Toegangspas/tag	Er wordt gesproken over toegangspas / tag. Beide zijn qua prijs en formaat wezenlijk anders. Kunt u aangeven wat de voorkeur heeft tag of pas. Indien de voorkeur uitgaat naar een toegangspas, kunt u dan de eisen specificeren ten aanzien van de lay-out, zoals bedrukking?	Wij willen in de nieuwe situatie gebruik maken van een toegangstag op basis van MIFARE DESFire EV3. In situaties waarin een fysieke pas gewenst of praktischer is, bijvoorbeeld voor bezoekers of specifieke doelgroepen, moet er ook een pas kunnen worden ingezet. Deze passen moeten voldoen aan precies dezelfde beveiligingseisen als de gebruikte tags. Voor passen kunnen verschillende opdrukken worden toegepast, zoals gemeentelijke huisstijlen of een bezoekersvariant, zonder concessies aan de beveiliging.
64.	Regel 28-30	Software	De meeste software licenties moeten per jaar afgenomen worden. Wij verzoeken u de maandelijkse softwarekosten te wijzigen naar jaarlijkse software kosten. Bent u daartoe bereid?	Het is ook akkoord om dit als jaarlijkse kosten af te rekenen. Dit wordt na gunning met ON bepaald. Deze software kosten kunnen vooraf worden gefactureerd.
65.	Regel 32-34	Onderhoud hardware	Wij verzoeken u de maandelijkse onderhoudskosten te wijzigen naar jaarlijkse onderhoudskosten. Bent u daartoe bereid?	Dit is ook akkoord, om jaarlijks af te rekenen. De onderhoudskosten worden achteraf gefactureerd.
66.	Regel 32-34	Maandelijkse kosten	Voor de maandelijkse kosten hanteert u een weging van 96 wat neerkomt op 8 jaar. Wat is de reden dat u 8 jaar aanhoudt terwijl de overeenkomst een duur heeft van 5 jaar met een eventuele verlening van 4 jaar?	Dit is uitsluitend om een fictieve situatie te creëren.
67.	Regel 32-34	Onderhoudskosten	Vanaf welk moment mogen we de maandelijkse kosten factureren? Vanaf 01-05-2026 of na oplevering van de implementatie	Zie het antwoord op notavraag 28.
Overige bijlagen				
68.	1	Document Blokschema	Kunt u meer informatie verschaffen op welke wijze de huidige toegangspas nu wordt gebruikt voor de printer (Follow Me)?	De huidige toegangstag wordt gebruikt voor de eerste identificatie bij het Follow-Me printen. Bij het aanbieden van de tag wordt de unieke identifier uitgelezen en gekoppeld aan het gebruikersaccount dat binnen de centrale identity-omgeving is geregistreerd. Nadat deze koppeling is bevestigd, krijgt de gebruiker toegang tot zijn eigen printopdrachten. De tag bevat zelf geen rechten of

				aanvullende informatie; alle gebruikersgegevens en autorisaties staan centraal in de identity-omgeving.
69.	1	Document Blokschema	Kunt u meer informatie verschaffen op welke wijze de huidige toegangspas nu wordt gebruikt voor KM-registratie?	Pas is alleen voor het herkenbaar maken van de bestuurder.
70.	1	Document Blokschema	Kunt u meer informatie verschaffen op welke wijze de integratie met inbraak en sleutelkluis is geïnstalleerd en met welk functioneel dit is gerealiseerd?	Pas is alleen voor het herkenbaar maken van de persoon. Wijhe schakelt een inbraakzone middels KL.
71.	1	Document Blokschema	Moet de genoemd Systeem – Integratie inbraak sleutelkluis gehandhaafd blijven met het nieuwe systeem?	Ja.
72.	1	Document Blokschema	Bij beide gemeentewerven staat cameratoezicht vermeld. Is dit onderdeel van de uitvraag? Zo ja, kunt u hiervoor aanvullende benodigde informatie verstrekken?	Is wel een onderdeel voor werf Raalte.
73.	1	Document Blokschema	Er zijn - volgens de blokschema's - verschillende bestaande koppelingen met systemen van derden. Kunt u – wanneer deze moeten worden gehandhaafd – per koppeling aangeven hoe deze koppeling is opgebouwd?	Dit is onderdeel van de engineering van het project.
74.	1	Document Blokschema	In DOWR- TGK blokschema V01 wordt verwezen bij locatie Gemeentewerf Raalte naar 'DOWR Gemeentewerf TGK V01'. Kunt u dit document ter beschikking stellen?	Zie bijlagen.
75.	1 & 2	Document aanpassingen	Kunt u meer concrete informatie geven over dit document. Het is nu niet duidelijk voor inschrijver (ook niet na de schouw) hoeveel nieuwe kaartlezers per locatie op welke deuren geplaatst moeten worden.	Het gaat in de basis om de vervanging van de huidige situatie.
76.	1 & 2	Document aanpassingen	Voor het Stadhuis Deventer worden balies genoemd, echter is deze tijdens de schouw niet bezocht. Wat dient hier toegepast te worden?	Deze uitvraag ziet initieel op het 1 op 1 overzetten, na gunning zullen de aanpassingen zoals verstrekt in de toegestuurde bijlagen worden afgestemd met de leverancier.
77.	1 & 2	Document aanpassingen	Voor het Stadhuis Deventer wordt de kelder genoemd, echter is deze tijdens de schouw niet bezocht. Wat dient hier toegepast te worden?	Zie antwoord 76.
78.		Schouwing	Maakt de sleutelkast nabij de receptie onderdeel uit van de uitvraag?	Bestaande sleutelkasten blijven in gebruik, geen nieuwe kasten in de uitvraag.

79.		Schouwing	Maakt de doorloopsluis nabij de receptie onderdeel uit van de uitvraag?	Ja, de doorloopsluis moet zodanig worden aangepast dat de nieuwe tag werkt.
80.		Schouwing	Maakt het lockerblok op de BG rechts achterin het Stadhuis Deventer onderdeel uit van de uitvraag?	Blok hoeft niet vervangen te worden, Tag moet hier wel werken.
81.		Schouwing	Bij de locatie Gemeentewerf Olst-Wijhe was onduidelijkheid m.b.t. de bestaande situatie/materialen? Kunt u op basis van een projectietekening aangeven wat de huidige en gewenste installatieomvang is.	Zie toegestuurde bijlagen.
82.		Schouwing	Op de Gemeentewerf Raalte is geen bestaande toegangscontrole-installatie aanwezig. Kunt u op basis van een projectietekening aangeven wat de gewenste installatieomvang is.	Zie toegestuurde bijlagen.
83.		Tekeningen	Kunt u op de tekeningen vermelden waar deurcontrollers hangen, overeenkomend met de verstrekte blokschema's?	De beschikbare informatie staat op de verstrekte tekeningen.
84.		Tekeningen	Kunt u op de tekeningen vermelden hoeveel deurcontrollers er hangen per centraal punt, overeenkomend met de verstrekte blokschema's?	Er is geen aanvullende informatie beschikbaar.
85.		Tekeningen	Kunt u op de tekeningen vermelden welke deuren nieuwe toegangscontrole krijgen?	Dit wordt na gunning verstrekt.
86.		Tekeningen	Kunt u op de tekeningen vermelden welke deuren in de bestaande situatie toegangscontrole hebben?	Staat op tekening.
87.		Tekeningen	De tekeningen van het stadhuis Deventer zijn van Chubb. Kunt u deze ter gelijk speelveld ook aan de andere gegadigden in goede digitale kwaliteit aanleveren?	Alle beschikbare informatie is opvraagbaar conform par. 3.4
88.		Tekeningen	Kunt u op de tekeningen onderscheid maken per deur tussen bekabelde en onbekabelde oplossingen wat betreft de gewenste situatie?	Niet van toepassing. Zie antwoord 55.
89.		Tekeningen	Kunnen jullie aanduiden op tekening waar alle bestaande hardware zit?	Zie antwoord 83.
90.		Tekeningen	Kunnen jullie tekening aanleveren met daarop de kabelgoten trace's	Zie vraag 1.

91.		Tekeningen	Zijn er plattegronden voor werf Raalte beschikbaar met daarom de exacte locaties van de nieuwe toegangscontrole deuren	Zie bijlage.
92.			Mogen de controllers op de reeds bestaande plaatsen gemonteerd worden?	Ja.
93.			Is de netwerk bekabeling en netwerkapparatuur onderdeel van deze uitvraag?	Binnen dit traject mag worden uitgegaan van het uitgangspunt dat de benodigde fysieke netwerkaansluitingen door de opdrachtgever worden verzorgd. Indien specifieke situaties vragen om aanvullende netwerkapparatuur die niet door de opdrachtgever wordt geleverd, kan de Inschrijver deze componenten onder vooraf overeengekomen technische en functionele voorwaarden zelf leveren.
94.			Welke systeemkoppelingen dienen er te worden gemaakt per locatie?	Er dient een koppeling te worden gemaakt met de IdP gemaakt te worden waar gebruikers centraal beheerd worden en waar met één enkele tag toepasbaarheid van meerdere doeleinden naast toegangsbeheer mogelijk zijn. Het gaat dan om koppelingen met onder andere sleutelkluizen, Druppel auto's, Printer (Canon, MFP) en (Tourniquet)poorten.
95.			Is er 1 installateur bekend bij alle locaties?	Nee het gaat om verschillende installateurs
96.			Is er 1 bouwkundige leverancier voor alle locaties?	Nee het gaat om verschillende installateurs.
97.			Is er 1 ICT dienstverlener welke verantwoordelijk is voor alle locaties?	Binnen de DOWR-samenwerking is DOWR ICT de enige ICT-dienstverlener die integraal verantwoordelijk is voor alle deelnemende locaties. Alle ICT-diensten, inclusief beheer, ondersteuning en continuïteit, worden centraal geleverd vanuit DOWR ICT.
98.			Zijn alle locaties IT-technisch aan elkaar verbonden?	Alle locaties zijn IT-technisch met elkaar verbonden via de centrale netwerkvoorzieningen van DOWR. De onderlinge koppeling verloopt via één gedeelde netwerkarchitectuur waarin routing, segmentatie en beveiliging uniform zijn ingericht.
99.			Kunnen wij er vanuit gaan dat de 230V voorzieningen door de huisinstallateur voorzien worden?	Ja.

100.			Zijn er specifieke eisen voor wat betreft de noodstroom voorzieningen?	Er zijn geen specifieke eisen. De paslezers en deuren waarvan dit noodzakelijk is zijn reeds op dit net aangesloten.
101.			Er wordt gesproken over mogelijk hergebruik van huidige kaartlezers. Wij hebben tijdens de schouw te weinig gezien om in te kunnen schatten of kaartlezers hergebruikt kunnen worden.	Voor de inschrijving kunt uitgaan voor de gehele vervanging van de kaartlezers. Na gunning wordt bekeken waar hergebruik mogelijk is. (in een nulmeting). Uw aanpak voor hergebruik dient u te beschrijven in het antwoord op Open vraag 1
102.			Kunnen wij er bij de prijsvorming vanuit gaan dat van deuren welke nu toegangsgecontroleerd zijn de sluitoplossingen (sluitplaten/elektrische sloten e.d.) hergebruikt kunnen worden?	De sluitoplossing werkt op het huidige systeem, en dient de basis te zijn voor het nieuwe systeem. Hier kunt u van uitgaan voor de inschrijving. Eventuele aantoonbare afwijkingen zullen na gunning tijdens de nulmeting worden besproken.
103.			Zijn de aanwezige sleutelkasten in Deventer geïntegreerd in/gekoppeld aan het huidige toegangscontrolesysteem? En zijn er meer gegevens van de aanwezige sleutelkasten?	Ja als het gaat om de identificatie. Zie vraag 78.
104.			Op welke wijze zijn de inbraakinstallaties van Deventer en Olst-Wijhe gekoppeld? Op contactbasis of een software koppeling? En dient deze integratie gehandhaafd blijven in het nieuwe systeem?	Uitgangspunt is het vervangen van het TGK systeem waarbij koppelingen gehandhaafd zijn. Verder is het na inschatting van inschrijver.
105.	6	9	Dient het aangeboden toegangscontrolesysteem te voldoen aan de BIO (Baseline Informatiebeveiliging Overheid)? Zo ja, aan welke technische eisen dient een toegangsdeur te voldoen m.b.t. Deurconstructie & Hang- en sluitwerk?	Het systeem dient te voldoen aan alle voorwaarden waardoor een nieuw, veilig, gebruiksvriendelijk en toekomstbestendig toegangscontrolesysteem voor de DOWR-gemeenten kan worden gegarandeerd.

Einde nota van inlichtingen: