Nota van Inlichtingen 1
Koninklijke Bibliotheek Ondersteuning publieksdiensten

Begin Nota van Inlichtingen:

Nr.	Pag.	§	Vraag:	Antwoord:
Beschrijvend document				
1.		Algemeen	In het bestek staat beschreven dat alles wat uitgevraagd wordt aan functionaliteit al in de huidige versie van inschrijver aanwezig moet zijn. Dit is volgens inschrijver niet redelijk, omdat er opmaat functionaliteit en koppelingen worden uitgevraagd die nog niet bestaan voor inschrijvers anders dan uw huidige leverancier. Graag deze eis daarom laten vervallen.	De KB verwacht een proven concept. De koppelingen en op maat gemaakte functionaliteiten zijn hier geen onderdeel van. Deze dienen door de opdrachtnemer te worden geleverd.
2.	12	2.1.4	Op pagina 12 van 'Beschrijvend document' onder hoofdstuk 2.1.4 punt 4 zeggen jullie dat een Azure VPN benodigd is. Deze VPN is niet benodigd bij een zero trust Cloud client. Wil de KB met die reden dit als optioneel opnemen?	Het betreft nu het opslaan van bestanden in de cloud, en in het huidige geval is het een onderdeel van de beveiliging van het huidige aangeboden product. VPN Azure is niet benodigd. Deze eis komt te vervallen.
3.	12	2.1.4	Om de continuïteit, veiligheid, privacy en beschikbaarheid te garanderen adviseren wij de KB om minimum een volledige Cloud omgeving te eisen. Bent u daartoe bereid?	Neen, de eisen hieromtrent zijn opgenomen in het Programma van Eisen. Het kan zijn dat de KB in de toekomst hierover een ander besluit neemt.
4.	12	2.1.4	Dient de aangeboden oplossing het internetverkeer te filteren op basis van inlogstatus of abonnementsvorm, of is er altijd een algemeen internetfilter actief (bijvoorbeeld op basis van DNS)? We gaan ervan uit dat een eventueel algemeen filter door de opdrachtgever wordt verzorgd.	Een filter voor het internetverkeer is niet aan de orde, ook niet op basis van abonnementsvorm of inlogstatus.
5.	32	4.4.3	Wat is volgens opdrachtgever een geldig alternatief voor een ISO 27001 certificering? Opdrachtnemer heeft een veiligheidsplan geënt op ISO 27001, valt dit onder een geldig alternatief?	Een dergelijk veiligheidsplan of een vergelijkbaar alternatief is door de KB op voorhand niet te beoordelen. Inschrijver dient, indien geen gevraagd geldig certificaat overlegd kan worden, haar veiligheidsplan of vergelijkbare alternatief aan ISO 27001 bij haar Inschrijving in te dienen. Het veiligheidsplan of een vergelijkbaar alternatief voor de gevraagde ISO 27001 zal door de KB op inhoud worden beoordeeld. Indien het niet voldoet zal de Inschrijving niet beoordeeld worden en wordt de inschrijving ter zijde gelegd.
6.			Wie is verantwoordelijk voor het hosten van de Wi-Fi omgeving?	Voor het netwerk gebruikt de KB overal Extreme Networks. De access point die gebruikt worden zijn: AP4000 met VX9000 Extreme Networks controllers. Deze zijn 2 jaar oud. Deze worden door KB (IT infra) beheerd.

Nr.	Pag.	§	Vraag:	Antwoord:
7.			Wie is verantwoordelijke voor het maken van de captive portal van de Wi-Fi?	Voor het gebruik van het KB wifi wordt door de opdrachtnemer een captive portal ontworpen (met KB look & feel), toegang hiertoe (KB wifi) geschiedt via de IAM authenticatie (AV) en autorisatie op basis van KB KRS. Zie PvE 71. Samenwerking met KB is uiteraard mogelijk qua look & feel.
8.			Is er een samenwerkingsmogelijkheid tussen de KB en de opdrachtnemer op het gebied van Wi-Fi?	Zie ook antwoord vraag 6. Het beheer wordt uitgevoerd door de KB zelf. Samenwerking met de opdrachtnemer is in deze is een vereiste.
Bijlage A. Programma van Eisen				
9.	6	3.13	Licht toe welke diensten/dienstverlening jullie bedoelen.	De eis is: *Het gebruik van de huidige KB (lidmaatschap)pas met NXP MIFARE Classic® EV1 S50 1 KB pas (4NUID) is mogelijk voor alle diensten/dienstverlening waar dit vereist/ingesteld is.* Voorbeelden hiervan kunnen zijn: Toegangspoortjes, Opwaarderen van KB pas (kassa/oplaadstation), printen-kopiëren-scannen MFC, scannen (flatbed of bookscanner), Werkstations (inlog & gebruik), (toekomstig) Wifi, Biebprinten (printen via byod), Inlog gebruik gelicentieerde bestanden.
10.	6	3.14	Licht toe welke diensten/dienstverlening jullie bedoelen.	De eis is: *Voor het gebruik van veel diensten en/of faciliteiten is door de KB een inlog vereist gesteld aan eindgebruikers (KB pashouders), door middel van de KB gehanteerde authenticatie voorziening én autorisatie op basis van het KB Klantregistratiesysteem [KRS] wordt toegang verleend [mits aan de gestelde voorwaarden wordt voldaan].* De KB ontwikkelt doorlopend of verbetert op bestaande/nieuwe diensten/dienstverlening, welke gebruikt kunnen worden na authenticatie/autorisatie. Hier wordt flexibiliteit en meedenkend vermogen verwacht van opdrachtnemer, mede in het kader van de toekomstige tijdelijke- & nieuwe huisvesting van de KB. Recentelijk is er een verkenning geweest en zijn er ontwikkelingen voor aanpassingen aan het 'KB lidmaatschap'. Zie ook: antwoord vraag 6.

Nr.	Pag.	§	Vraag:	Antwoord:
11.	6	14	Eis 14. Hoe ziet deze koppeling er volgens opdrachtgever uit (specificaties)?	Inloggen gebeurt met OAuth 2 of Open ID Connect, autorisatie gebruikt een REST API van KRS.
12.	6	14	Eis 14. Sip2 is de standaard koppeling voor aansluiten op bibliotheeksystemen in Nederland. Aanvullend: Opdrachtnemer heeft deze Sip2 koppeling standaard beschikbaar, mag/kan het KRS ook via Sip2 worden gekoppeld?	Neen, KRS is bedoeld als generieke klantenadministratie, niet als bibliotheeksysteem en heeft (daarom) geen Sip2 koppelmogelijkheid.
13.	7	3.21	De KB is gebaat bij de kwaliteit en de veiligheid van de oplossing. Met die reden adviseren we jullie om de printopdrachten/scanopdrachten ook mee te nemen binnen deze eis. Dit resulteert erin dat bestanden dan niet lokaal worden opgeslagen maar in één veilige centrale Cloud omgeving. Zo zorgt de KB ervoor dat de client altijd schoon blijft en dit resulteert in een waarborging van de privacy.	De eis is: *Een klant heeft de mogelijk op het werkstation bestanden tijdelijk op te slaan, deze opslag is persoonlijk (na inlog) en wordt dus niet gedeeld met anderen. Het is ook mogelijk bestanden op een extern medium van de eindgebruiker op te slaan. Het tijdelijke bestand wordt automatisch gewist via een ingestelde tijd dezelfde dag.* De KB heeft geen bezwaar tegen de voorgestelde implementatie, maar wil deze niet eisen.
14.	7	3.25	We zijn benieuwd hoe de KB deze functionaliteit voor zich ziet. Hoe wordt bijvoorbeeld dit pauze scherm weer vrijgegeven op een veilige manier?	De eis is: *Een klant kan de sessie in 'pauze' zetten (afhankelijkheid welke dienst/faciliteit gebruikt wordt). Zodat de klant voor een korte tijd deze bezet kan houden zonder hiervoor hoeft uit te loggen. Deze pauze tijd is instelbaar (d.m.v. invoer zoals bij 1e keer inloggen, kan de klant het werkstation weer vrij geven en in gebruik nemen.* Dit is aan de opdrachtnemer.

Nr.	Pag.	§	Vraag:	Antwoord:
15.	8	3.27	Is het wenselijk om bij het inloggen van een leeszaalpashouder specifieke content te laten zien voor deze leeszaalpas houder? Dat wil zeggen een gepersonaliseerd profiel na inlog.	De eis is: *Om een werkstation te kunnen gebruiken waar een inlog is bepaald/ingesteld, geschiedt dit door invoering van het geldende gebruikersnaam en wachtwoord, koppeling via de authenticatievoorziening van Opdrachtgever, dit is niet noodzakelijk voor werkstations waar geen inlog is bepaald/ingesteld.* Neen, dit is niet wenselijk. De leeszaalpashouder is alleen geautoriseerd om de website Delpher (volledig, inclusief de 'verboden content', welke alleen intramuraal (in de KB) ingezien mag worden) te raadplegen. De profielpagina kan qua opbouw hetzelfde zijn als de KB jaarpashouder.
16.	8	3.29	Kan de KB toelichten wat een leeszaalprofiel en registratie profiel precies inhoud en welke functionaliteiten deze profielen moeten hebben?	De eis is: *Het is mogelijk om werkstations in te stellen zonder een (beveiligde) inlog, maar met een speciaal thema/profiel als startpagina*. De KB wil graag klanten laten kennis maken en/of toegang geven tot haar (online/fysieke) collecties, hiervoor moet de mogelijkheid bestaan om het werkstation beperkte functionaliteit (kioskmodus) toe te wijzen, dit kan ook bijvoorbeeld een ingesteld webadres/website zijn. Voorbeelden zijn o.a. het gebruik van DBNL, Delpher, maar ook lid worden via een registratieproces (onderdeel KB website).
17.	9 en 15	3.35/3.74	De KB heeft op dit moment een lopend contract bij de huidige MFC leverancier. Echter is het wenselijk voor de KB dat er gekozen wordt voor een vendor neutrale oplossing. Dit is omdat er binnen dit bestek gevraagd wordt om een koppeling aan deze MFC leverancier. Dit zorgt ervoor dat de KB over de looptijd van 12 jaar niet gebonden is aan één MFC leverancier.	De eis is: *De bestaande MFC Ricoh IM C3000 blijft gehandhaafd, dus een koppeling dient verzorgt te worden met kopieer/printbeheer & het betaalverkeer. Momenteel verloopt dit via de payment provider Equens.* Deze eis blijft gehandhaafd. Mogelijk dat in de toekomst een andere keuze voor MFC leverancier wordt gemaakt en dan wordt e.e.a. opnieuw beoordeeld.

Nr.	Pag.	§	Vraag:	Antwoord:
18.	9	3.38	Is het wenselijk om een pinterminal te monteren in de printzuil zodat er bij te weinig tegoed het resterende bedrag erbij gepind kan worden?	De eis is: *Er kan uitsluitend worden gekopieerd/geprint bij voldoende saldo (op de RFID chip) en/of bij een directw betaling/betaalmogelijkheid.* De eis blijft gehandhaafd, echter de KB staat in de toekomst open voor een alternatieve betaalmogelijkheid, deze staat omschreven in 3.41.
19.	10	3.45	Het is wenselijk om een fysieke transactie bon aan te bieden bij betalen van een printopdracht bij de betaalzuil.	De eis is: *De klant ontvangt een transactie bon van het saldo op de KB pas is opgewaardeerd. De klantgegevens & gegevens organisatie zijn in overleg met Opdrachtgever bepaald.* Het 'aanbieden' hiervan is een eis, de klant kan bepalen om 'geen' transactie bon te willen. Een toekomstig alternatief zou een digitale transactie bon kunnen zijn.
20.	11/12	3.53/54	Het is wenselijk om de omgeving van de KB geautomatiseerd te kunnen beheren met een agenda functie. Binnen deze functie kan bijvoorbeeld een pc automatisch opstarten, afsluiten, wisselen van profiel/windowsgebruikers of berichten sturen naar de klant. Bijvoorbeeld het versturen van 'we sluiten over 15 minuten'. Dit kan zonder tussenkomst van een medewerker.	Eis 53 is: *Alle ingestelde profielen, plattegronden etc. van de werkstations en randapparatuur kunnen hieruit beheerd, bewerkt worden.* Eis 54 is: *Er kunnen tekstuele berichten naar alle pc's (ad hoc en ingestelde), naar een groep en deel van een groep of naar een individueel werkstation gestuurd worden. De ontvanger/ontvangers zien dit bericht in de vorm van een pop-up.* Neen, dit is voor nu niet wenselijk. Eis 53 en 54 zijn van toepassing.
21.	12	58	Eis 58. Opdrachtnemer kan niet zonder meer het huidige kassa systeem beheren, dit kassa systeem is immers geleverd door een andere aanbieder (huidige leverancier). Gaat de huidige leverancier akkoord dat opdrachtnemer het kassasysteem gaat beheren? Waarom is de directe vervanging van het kassasysteem geen onderdeel van deze aanbesteding?	De eis is: *De Opdrachtnemer kan het kassasysteem van Opdrachtgever beheren, het ontvangen van betalingen verloopt via de payment provider Equens (huidige situatie).* De directe vervanging van het kassa systeem is onderdeel van de uitvraag. Zie het PvE (deel 3) en ook het Prijzenblad regel 17.

Nr.	Pag.	§	Vraag:	Antwoord:
22.	14	3.69	Kunnen jullie toelichten welke oplossingen jullie bedoelen?	De eis is: *Voor de onderdelen van de oplossing waar de klant zichzelf identificeert met de KB-pas, wordt, gebruikt de oplossing de autorisatie-API van Opdrachtgever om te bepalen of de dienst verleend mag worden.* Voorbeelden zijn het verkrijgen van toegang tot de leeszaal en het afdrukken van een printopdracht.
23.	14	3.71	We gaan hierbij uit dat er een samenwerking is tussen netwerk leverancier en opdrachtnemer. Er moet een API beschikbaar zijn zodat de captive portal een signaal kan sturen met als resultaat dat een geautoriseerde gebruiker toegang krijgt tot het Wi-Fi netwerk. Kunnen jullie die API aanleveren? Zo nee, licht dit nader toe.	De eis is: *Voor het gebruik van het KB wifi wordt door de Opdrachtnemer een captive portal ontworpen (met KB look & feel), toegang hiertoe (KB wifi) geschiedt via de IAM authenticatie (AV) en autorisatie op basis van KB KRS.* De captive portal wordt aangesloten op onze Extreme Networks controller.
24.	14	3.72	De KB is gebaat bij een flexibele oplossing en met die reden adviseren wij de KB om als minimum eis toe te voegen dat de KB zonder tussenkomst van opdrachtgever profielen kan wisselen.	De eis is: *De Opdrachtnemer heeft kennis om verschillende profielen (web UI) voor werkstations te maken en toe te passen (met KB look & feel) op diensten van Opdrachtgever, specifieke websites, in de leeszaal opgestelde collecties en/of databanken.* De KB verwacht de werkstations een profiel (Web-UI) toe te kunnen wijzen via de beheermodule. Zie ook 3.53.
25.	14	3.72	De KB is gebaat bij één huisstijl en interface voor het gebruiksgemak van alle portalen. Met die reden verzoeken wij de KB dat alle geleverde oplossingen een white label van de KB moeten zijn. Is de KB bereid om dit mee te nemen in de minimum eisen?	Neen, de KB staat open voor een oplossing die uit onderdelen van verschillende herkomst bestaat en vindt dit voorstel daarom te zwaar als minimumeis.
26.	14	3.73	Deze vraag is te breed interpreteerbaar kunnen jullie met die reden deze nader toelichten?	De eis is: *De oplossing heeft een Web-UI voor eenvoudige toegang tot diensten voor de wifi-gebruikers (zoals bijvoorbeeld printen).* Deze eis dient gelezen te worden als vervolg op 3.72. De vaste werkstations hebben een profiel (Web UI) nodig, maar de gebruikers met een byod ook, hierbij is het mogelijk om via een inlog printopdrachten te versturen naar de opgestelde MFC's.

Nr.	Pag.	§	Vraag:	Antwoord:
27.	16	84	Eis 84. Wat moet er na de bewaartermijn worden verwijderd?	De eis is: *De Oplossing biedt de mogelijkheid om bewaartermijnen te definiëren en deze aan gegevens te koppelen*. De bewaartermijn is afhankelijk van het doel waarvoor het dient, denk hierbij aan gebruik werkstation, klantgegevens toegang, verkoopgegevens kassa, printfiles-logging. Na gunning wordt hier verder invulling aan gegeven
28.	16	4.84	De KB is gebaat bij een gebruiksvriendelijke omgeving voor zijn/haar leden. Een van de onderdelen om dit te realiseren is de mogelijkheid om op een veilige manier bestanden op te slaan op de werkstations. Daarnaast is de KB gebaat bij een splitsing tussen gebruikersbestanden en printopdrachten. Opdrachtnemer adviseert met die reden de KB om dit mee te nemen in de aanbesteding.	De KB neemt dit advies niet over, niet akkoord dus.

Nr.	Pag.	§	Vraag:	Antwoord:
29.	17	6.91/6.92	Om deze kwaliteit te bij de opdrachtnemers te waarborgen zodat iedereen hieraan voldoet. Adviseren wij de KB om als minimum eis niet afhankelijk te zijn van de performance van andere klanten binnen één zelfde Cloud.	Eis 91 is: *Het minimale beschikbaarheidspercentage exclusief tijd voor onderhoud is 99,5% per maand. In de Supportdocumentatie wordt uitgewerkt hoe wordt omgegaan met geplande en ongeplande (bijvoorbeeld bij een security incident) onderhoudsvensters. De beschikbaarheid van de werkstations en aanverwante apparatuur is gekoppeld aan een uur vóór openingstijden leeszaal KB en een kwartier na sluitingstijd, de beschikbaarheidsuren zijn ten allen tijde aanpasbaar. In ieder geval meldt Opdrachtnemer geplande downtime, bijvoorbeeld als gevolg van onderhoudswerkzaamheden of het installeren van een nieuwe release, minimaal 48 uur van tevoren bij Opdrachtgever. Wanneer werkzaamheden binnen werkuren van Opdrachtgever plaatsvinden die downtime met zich meebrengen, vraagt Opdrachtnemer eerst instemming van Opdrachtgever voordat de werkzaamheden worden uitgevoerd.* Eis 92 is: *Opdrachtnemer zorgt voor monitoring van de beschikbaarheid en performance van de Oplossing en dat Opdrachtgever direct gealarmeerd wordt bij onder andere (niet uitputtend): uitval, performanceproblemen, (D)DOS-aanvallen, onverklaarbare toename in verkeer naar internet, verlopen van beveiligingscertificaten, ongeautoriseerde wijzigingen aan configuratiebestanden, ongeautoriseerde wijzigingen aan systeembestanden etc. De Oplossing omvat een Intrusion Detection of Intrusion Prevention Systeem.* De KB gaat niet akkoord met dit advies. Het is aan de opdrachtnemer om te bepalen hoe de eisen en wensen van de KB het beste ingevuld kunnen worden. De KB wil op deze punten geen oplossing voorschrijven.

Nr.	Pag.	§	Vraag:	Antwoord:
30.	19	7.97/7.98	Conform scope van de opdracht of zien jullie alle modules buiten de scope die ontwikkeld worden ook als inclusief?	Eis 97 is: *Opdrachtnemer verstrekt zonder meerkosten updates en upgrades van de Oplossing. Dit is onderdeel van de licentieprijs en/of beheerkosten. Opdrachtgever wil voorkomen dat voor vernieuwde functionaliteiten additionele kosten worden gevraagd. Ook wil Opdrachtgever voorkomen dat oplossingen voor incidenten en wijzigingen niet doorgevoerd kunnen worden omdat er een betaalde update of upgrade niet is afgenomen.* Eis 98 is: *Opdrachtnemer dient een technische beschrijving van alle gerealiseerde koppelingen, integraties en de daarbij toegepaste configuraties aan te leveren voor afronding van de implementatie en deze vervolgens te onderhouden. De beschrijving omvat minimaal een specificatie van de uitgewisselde gegevens en de wijze waarop dit gebeurt.* De eisen zijn conform de scope van de opdracht uit te voeren.
31.	19	8.101	Het uitsluiten van de acceptatie omgeving brengt de continuïteit van de omgeving van de KB in gevaar. Met die reden adviseren wij om een acceptatie omgeving wel als minimum eis op te nemen	De eis is: *Een acceptatie-omgeving is niet nodig, aangezien wijzigingen eenvoudig buiten de openingstijden van de leeszalen getest kunnen worden op de productie-omgeving.* Niet akkoord, de keuze van de KB om geen acceptatie omgeving te eisen is weloverwogen.

Nr.	Pag.	§	Vraag:	Antwoord:
32.	20	8.103	We maken hier een aanname maar wij gaan ervan uit van onze eigen infrastructuur en niet de infrastructuur van derden.	De eis is: *De afspraken met betrekking tot het technisch beheer en applicatiebeheer worden nader uitgewerkt in Supportdocumentatie (SLA of soortgelijk document waarin procedures en dienstverleningsniveau 's zijn vastgelegd). Opdrachtnemer is, ten aanzien van de Oplossing, minimaal verantwoordelijk voor:* *- Installatie van aanbevolen updates en upgrades van de Oplossing. Ook de onderliggende componenten zoals het operating systeem, eventueel gebruikte middleware en het basic input/output system;* *- Informatiebeveiliging;* *- Bewaken en controleren van de infrastructuur;* *- Configuratiemanagement op het Cloud platform;* *- Beheer van opslagcapaciteit.* De KB bedoelt hier primair de infrastructuur van de opdrachtnemer, maar waar die gebruik maakt van infrastructuur van derden, verwachten we dat de opdrachtnemer waarborgt dat die volgens dezelfde normen beheerd worden.
33.			De KB stelt hoge eisen aan hun opdrachtnemers op het gebeid van privacy en security. Met die reden is de KB gebaat bij de kwaliteit van zijn/haar inschrijvers qua privacy en security. Daarom vragen wij de KB om als minimum eis een zero trust private Cloud omgeving op te nemen in de standaard eisen. Hiermee is de KB zelf eigenaar van de Cloud en wordt dit niet gedeeld met andere klanten. Bent u daartoe bereid? Zo niet, waarom niet?	Gezien de aard van de gevraagde oplossing en de verwerkte gegevens ziet de KB dit niet als noodzaak en ook te beperkend voor aanbieders van SAAS diensten.

Nr.	Pag.	§	Vraag:	Antwoord:
34.	24	9.121	Kan de KB extra uitleg geven over deze vraag? Wij maken op dit moment namelijk geen gebruik van e-mails.	De eis is: *Waar in de Oplossing gebruik wordt gemaakt van e-mail die namens Opdrachtgever wordt verstuurd of ingelezen, dan wordt daarvoor bij voorkeur aangesloten op de Microsoft Graph API en vindt autorisatie plaats op basis van OpenID Connect (Oauth 2.0) om toegang te verkrijgen tot het e-mailplatform Exchange Online van Opdrachtgever voor het verzenden of uitlezen van e-mail.* *In het geval dat een e-mailvoorziening wordt toegepast die niet verloopt via het e-mailplatform van de Opdrachtgever, dan zorgt Opdrachtnemer ervoor dat de e-mail herkenbaar is, op basis van domeinnaam van Opdrachtgever, als e-mail van de Opdrachtgever.* Deze eis is alleen relevant indien de opdrachtnemer e-mails gebruikt
35.	24	9.122	Kan de KB extra uitleg geven over deze vraag? Wij maken op dit moment namelijk geen gebruik van e-mails.	De eis is: *Waar de Oplossing gebruik maakt van e-mailverkeer dat namens Opdrachtgever plaatsvindt (intern dan wel extern) voldoet de implementatie blijvend aan aanvullende beveiligingsmaatregelen als SPF, DKIM, DMARC en DANE (eventueel na implementatie door Microsoft).* Deze eis is alleen relevant indien de opdrachtnemer e-mails gebruikt

Nr.	Pag.	§	Vraag:	Antwoord:
36.	25	9.129	Is het mogelijk om dit te organiseren bij de POC. Op deze manier waarborgt de KB de veiligheid van de nieuwe omgeving.	De eis is: *Opdrachtgever heeft het recht om bij Opdrachtnemer een (onafhankelijke) audit uit te (laten) voeren naar de opzet, het bestaan en de werking van informatiebeveiligingsmaatregelen. Opdrachtnemer gaat akkoord met een audit door een medewerker van Opdrachtgever of een door Opdrachtgever ingehuurd accountants- of onderzoeksbureau. Opdrachtnemer gaat hierbij ook akkoord met het feit dat dit periodiek uitgevoerd wordt.* *Opdrachtnemer heeft de mogelijkheid om een audit rapport van een onafhankelijke 3rd-party auditor te overleggen.* Neen, is wordt geen POC ge-eist. Deze eis geldt gedurende de looptijd van het contract en dus niet alleen bij de aanvang.
37.	26	9.131	We nemen aan dat deze pentesten georganiseerd worden door de opdrachtgever. Daarbij is dit een samenwerkingsverband, dus gaan we er vanuit dat deze gegevens transparant met elkaar gedeeld wordt.	De eis is: *De Oplossing die naar productie wordt gebracht, dient ten tijde van vrijgeven en bij alle majeure wijzigingen vrij te zijn van bekende kwetsbaarheden, waaronder minimaal de kwetsbaarheden genoemd in de actuele 'OWASP top 10' en de 'SANS/CWE top 25 most dangerous software errors'. Opdrachtnemer toont dit aan door een preventieve vulnerability scan en/of een penetratietest.* Neen, niet akkoord. We vragen dit van de opdrachtnemer om de testen zelf uit te voeren.

Nr.	Pag.	§	Vraag:	Antwoord:
38.	26	9.132	Worden deze pentesten georganiseerd door de KB of moeten deze bij de prijs inbegrepen zijn.	De eis is: *Opdrachtnemer zorgt dat de digitale infrastructuur (hardware en software) van de Oplossing continu gemonitord wordt op kwetsbaarheden. Patches worden aangebracht conform de volgende criteria:* *- Binnen één week voor critical security patches (CVSS 9+),* *- Binnen twee weken voor high security patches (CVSS 7.0-8.9) en* *- Bij het eerstvolgende onderhoudswindow in andere gevallen (CVSS kleiner dan 7.0).* *Indien de toepassing extern-facing is of het de werkplek betreft gelden de volgende tijdwindows:* *- Direct en i.i.g. binnen 24 uur voor critical security patches (CVSS 9+),* *- Binnen één week voor high security patches (CVSS 7.0-8.9) en* *- Bij het eerstvolgende onderhoudswindow in andere gevallen (CVSS kleiner dan 7.0).* *Opdrachtnemer zal tenminste jaarlijks in de Oplossing gebruikte webapplicaties en API's door een onafhankelijke penetratietest laten controleren op kwetsbaarheden. Opdrachtnemer rapporteert ieder kwartaal over aangetroffen kwetsbaarheden en ondernomen acties en tenminste jaarlijks over de penetratietest en ondernomen actie dienaangaande. Opdrachtnemer stelt op verzoek van Opdrachtgever de originele rapportage van de vulnerability scan en penetratietest beschikbaar.* Deze testen moeten bij de prijs inbegrepen zijn.

Nr.	Pag.	§	Vraag:	Antwoord:
39.	27	9.134	Ten opzichte van ISO-27001 wat voor waarde hecht de KB aan deze certificering als opdrachtnemer een ISO certificering heeft. Bij de ISO certificering wordt beleid en maatregelen getoetst waarbij ook gekeken wordt of dit op de juiste wijze toegepast wordt. Wij zien niet waarom dit van toepassing is, graag nadere toelichting.	De eis is: *Opdrachtnemer beschikt over, dan wel levert na 1 jaar, een onafhankelijke Service Organization Control (SOC) 2 Type 2 dan wel SOC 3 rapportage of een ISAE 3402 type II verklaring om aan te tonen in control te zijn. Opdrachtnemer zorgt ervoor dat de Assurance-verklaring onderhouden wordt.* Waar bij ISO 27001 de focus op informatiebeveiliging ligt, gaan SOC 2/ISAE 3402 type 2 over het aantonen in control te zijn van risico's en beheersmaatregelen in een bredere scope. Afbakening en doel hebben zeker overlap, maar zijn niet hetzelfde. Daarom vraagt de KB beide. Zie ook antwoord vraag 5.
40.	27	9.138	Kunnen jullie uitleggen waar E22.14 voor gedefinieerd staat?	De eis is: *Waar de Oplossing gebruik maakt van Cookies of HTTP verkeer worden adequate beveiligingsinstellingen toegepast. Cookies dienen te zijn voorzien van de 'secure' en 'httponly' flags. Tevens bevatten cookies geen persoonlijke informatie en vindt de uitwisseling altijd via adequate transportbeveiliging conform E22.14 plaats. De Oplossing is vrij van tracking cookies. HTTP Secure Headers worden overeenkomstig met Best Practices (bijvoorbeeld op basis van OWASP Secure Headers Project) toegepast.* E22.14 is een schrijffout. Hier wordt een verwijzing naar eis 123 bedoeld.
41.	27	9.139	Dit is niet de verantwoordelijkheid van de opdrachtnemer? Aangezien de Opdrachtnemer geen netwerkomgeving levert? Graag nadere toelichtingen.	De eis is: *Bij wireless netwerkvoorzieningen voor gebruikers wordt verzekerd dat geen rechtstreekse verbindingen tussen gebruikers mogelijk zijn.* Deze eis is generieker bedoeld dan alleen Wifi. Ze geldt voor alle plekken of onderdelen in de aangeboden oplossing waar gebruik gemaakt wordt van draadloze netwerkvoorzieningen.

Nr.	Pag.	§	Vraag:	Antwoord:
42.	30	154 en 155	Eis 154 en 155. Deze twee eisen lijken tegenstrijdig. Kan Opdrachtgever dit toelichten?	Eis 154 is: *Opdrachtnemer voorziet in het verwijderen van alle gebruikershistorie na uitloggen door de gebruiker.* Eis 155 is: *Retentie van centraal opgeslagen bestanden van gebruikers bedraagt maximaal 24 uur.* De scope van eis 154 zijn de werkstations, die van 155 heeft betrekking op de bestandsopslag.
43.	31	10.163	Is de KB akkoord dat bij verwijdering van een gebruiker dat deze transactie data geanonimiseerd wordt. Dit ter behoeve van rapportages.	De eis is: *Als persoonsgegevens uit de Oplossing worden verwijderd, moeten deze uit alle systemen/back-ups van Opdrachtnemer worden verwijderd. Voor backups geldt dat dit mag naijlen tot maximaal de termijn waarbinnen Opdrachtnemer gehouden is nog te kunnen herstellen vanuit backups.* Akkoord indien anonimiseren inhoudt dat de persoonsgegevens niet langer te herleiden zijn tot een persoon.
44.	31	10.164	Is dit eenmalig of periodiek en wie organiseert dit?	De eis is: *Opdrachtnemer werkt mee met het uitvoeren van een Data Protection Impact Assessment (DPIA) volgens het model van Opdrachtgever.* De KB organiseert dit. Een DPIA moet onderhouden worden en kan herzien moeten worden bij veranderingen in de scope van de oplossing of de set verwerkte gegevens

Nr.	Pag.	§	Vraag:	Antwoord:
45.	31 en 32	166 en 167	Eis 166 en 167. Mag het exitplan (i.p.v. voor ingebruikname) na implementatie overlegd worden? Een compleet exitplan met daarin alle onderdelen en koppelingen beschreven kan o.i. pas na implementatie overlegd worden, graag hier akkoord op.	Eis 166: *Het exitplan beschrijft de wijze waarop de dienstverlening van Opdrachtnemer kan worden beëindigd. Als ook de wijze waarop Opdrachtnemer na beëindiging, samen met Opdrachtgever zal zorgen voor een continuering van deze dienstverlening bij Opdrachtgever of een door Opdrachtgever aan te wijzen dienstverlener. Het exitplan wordt initieel opgesteld door Opdrachtnemer voorafgaand aan de ingebruikname van de Oplossing. Het exitplan wordt periodiek herzien en indien relevant geactualiseerd. Periodiek is (minimaal) jaarlijks of wanneer de situatie daartoe aanleiding geeft.* Eis 167 *Het exitplan bevat een gedetailleerde weergave van alle uit te voeren activiteiten om de exit transitie tot een succes te maken. Dit omvat onder meer de wijze waarop Opdrachtnemer zorgdraagt dat Opdrachtgever de beschikking krijgt over de in de Oplossing opgeslagen gegevens en documenten. De doorlooptijd van de exit transitie is (maximaal) 3 maanden na de aanvang van de transitie.* Na implementatie is akkoord. Het exitplan dient uiterlijk binnen 6 maanden na implementatie te worden aangeleverd.
46.	33	12.175	Graag deze vraag verduidelijken	De eis is: *Inzake het in- en uitloggen in de wifi-omgeving ligt het in de bedoeling dat Opdrachtgever deze werkzaamheden zelf wil gaan uitvoeren. In overleg met de Opdrachtnemer zal het moment en de wijze waarop deze overgang naar het inbesteden van deze dienst worden besproken* *Vanaf het moment van inbesteden zal een minder prijs op de maandfactuur gaan gelden.* Op termijn wil de KB de captive portal voor het inloggen op de wifi zelf gaan verzorgen. Een exacte termijn hebben we daar nog niet voor.

Nr.	Pag.	§	Vraag:	Antwoord:
Bijlage B. Overeenkomst				
47.	5	4.4	Eenmalige kosten worden voor 50% bij aanvang van de implementatie in rekening gebracht. Graag zien we dit aangepast naar 70% bij aanvang en 30% na acceptatie	De KB houdt vast aan de gevraagde percentages. Dus 50% bij aanvang en 50% na acceptatie.
Bijlage C. Wachtkamerovereenkomst				
			Geen vragen	
Bijlage D. Verwerkersovereenkomst				
			Geen vragen	
Bijlage E. Arbit 2022				
			Geen vragen	
Bijlage F. Aanvullende voorschriften en voorwaarden				
			Geen vragen	
Bijlage G. Referenties				
			Geen vragen	
Bijlage H. Prijzenblad				
			Geen vragen	
Overige bijlagen				
48.	1	Aanbesteding Publieksomgeving SOLL (aanbestedingsfase)	Kunnen jullie het doel van de koppeling met Entra ID toelichten per categorie: **a) Werkplekken:** Willen jullie op de publieke werkplekken kunnen inloggen met Entra ID **b) Printoplossing:** Willen jullie doormiddel van jullie Entra ID printen, kopieren en scannen. Zo ja, hoe zien jullie dit voor je? **c) Kassa publiekszaal:** Wat is het doel van Entra ID met deze koppeling? **d) Besturing toegangspoortjes:** Hoe zien jullie deze koppeling met Entra ID voor jullie?	De toegang tot userinterfaces die bedoeld zijn voor KB-medewerkers dienen beschermd te zijn door een inlog met het KB-medewerkers-id op de entra-ID omgeving van de KB. Inloggen op de eindgebruikersfuncties van de oplossing is hoeft geen Entra-ID te ondersteunen, daar wordt -voor zover relevant- alleen ingelogd met de authenticatievoorziening (AV in de architectuurtekening) a. nee. b. nee. c. Alleen voor toegang tot de userinterfaces die bedoeld zijn voor KB-publiekszaal-medewerkers. d. Alleen voor toegang tot eventuele userinterfaces voor kb-publiekszaal-medewerkers.

Nr.	Pag.	§	Vraag:	Antwoord:
49.			Gaan jullie nog gebruik maken van de KB pas ter behoeve van autorisatie voor printoplossing, werkplek en toegangscontrole?	De eis is: *Het gebruik van de huidige KB (lidmaatschap)pas met NXP MIFARE Classic® EV1 S50 1 KB pas (4NUID) is mogelijk voor alle diensten/dienstverlening waar dit vereist/ingesteld is.* Ja, voor de toegangscontrole en printoplossing. Wellicht in de nieuwe situatie t.b.v. opwaarderen ook mogelijk bij het nieuwe kassasysteem, dit is aan de opdrachtnemer.
50.			Kan de KB toelichten wat een leeszaalprofiel en registratie profiel precies inhoud en welke functionaliteiten deze profielen moeten hebben?	De eis is: *Het is mogelijk om werkstations in te stellen zonder een (beveiligde) inlog, maar met een speciaal thema/profiel als startpagina.* De KB wil graag klanten laten kennis maken en/of toegang geven tot haar (online/fysieke) collecties, hiervoor moet de mogelijkheid bestaan om het werkstation beperkte functionaliteit (kioskmodus) toe te wijzen, dit kan ook bijvoorbeeld een ingesteld webadres/website zijn. Voorbeelden zijn o.a. het gebruik van DBNL, Delpher, maar ook lid worden via een registratieproces (onderdeel KB website).

Bijlagen: Geen

Einde Nota van Inlichtingen 1.