Nota van inlichtingen 1 - Sleutelkasten - Amsterdam UMC - d.d. 23-9-2026			
Ref. Nr.	**Onderwerp**	**Vraag**	**Antwoord**
1	Punt ICT.28.005 - Verduidelijkingsvraag – testomgeving en testkast	In het Programma van Eisen is opgenomen: “Na een update/aanpassing aan het systeem kan het systeem worden gecontroleerd d.m.v. vooraf opgestelde testprocedure.” Om wijzigingen, updates en aanpassingen gecontroleerd te kunnen testen zonder directe impact op de productieomgeving, vragen wij de opdrachtgever nader te specificeren of hiervoor een afzonderlijke testomgeving dient te worden ingericht. Kan de opdrachtgever bevestigen of wordt verlangd dat de opdrachtnemer een testomgeving beschikbaar stelt, inclusief minimaal één fysieke sleutelkast, waarin updates, configuratiewijzigingen en/of nieuwe functionaliteiten voorafgaand aan implementatie in de productieomgeving kunnen worden getest? Wij ontvangen daarbij graag duidelijkheid over: - of een fysieke testkast onderdeel dient te zijn van de testomgeving; - of deze testkast representatief moet zijn voor het binnen Amsterdam UMC toegepaste type/configuratie; - of de testomgeving ook gekoppeld dient te kunnen worden aan relevante systemen, zoals het centrale IAM-systeem, intercom/video en overige koppelingen; - of de testomgeving permanent beschikbaar dient te zijn gedurende de contractperiode, of uitsluitend tijdens implementaties en updates; - wie verantwoordelijk is voor het beheer, onderhoud en actualiseren van de testomgeving; - wie verantwoordelijk is voor de benodigde hardware, software, licenties en koppelingen; - of updates en wijzigingen eerst in deze testomgeving moeten worden gevalideerd voordat deze in de productieomgeving mogen worden geïmplementeerd; - welke test- en acceptatiecriteria hierbij van toepassing zijn. Kan de opdrachtgever tevens aangeven of het beschikbaar hebben van een dergelijke afzonderlijke testomgeving met fysieke sleutelkast als contractuele verplichting gedurende de gehele looptijd van de overeenkomst wordt beschouwd?	Voor het testen van updates van de applicatie is naast een productieomgeving een acceptatieomgeving vereist. Hierdoor kunnen wijzigingen gecontroleerd worden getest voordat deze in productie worden doorgevoerd. Dit is met name van belang voor de koppelingen met andere systemen, zodat de correcte werking en gegevensuitwisseling gewaarborgd blijven. De acceptatieomgeving dient gekoppeld te zijn aan de relevante systemen. Deze omgeving moet gedurende de contractperiode continu beschikbaar zijn, aangezien niet alleen het aangeboden systeem wijzigingen kan ondergaan, maar ook gekoppelde systemen waarvan de werking regelmatig getest moet kunnen worden. Een fysieke testkast maakt uitsluitend gedurende de pilotfase onderdeel uit van de acceptatieomgeving. Deze testkast dient representatief te zijn voor het binnen Amsterdam UMC toegepaste type en de gebruikte configuratie. De leverancier is verantwoordelijk voor het beheer van de acceptatieomgeving, evenals voor de benodigde hardware, software, licenties en koppelingen. Updates en wijzigingen dienen eerst in de acceptatieomgeving te worden gevalideerd voordat deze in de productieomgeving worden geïmplementeerd. Als acceptatiecriterium geldt dat alle functionaliteiten na validatie minimaal gelijkwaardig moeten functioneren aan de situatie voorafgaand aan de wijziging. Na oplevering van het systeem is een afzonderlijke testkast niet langer benodigd.
2	Punt ICT.17.002 - Verduidelijkingsvraag – recht op vergetelheid	In het Programma van Eisen is opgenomen dat het aangeboden Systeem functionaliteit dient te bieden waarmee Amsterdam UMC invulling kan geven aan het “recht op vergetelheid” conform de betreffende richtlijnen van de Autoriteit Persoonsgegevens. Kan de opdrachtgever nader specificeren welke functionaliteit het aangeboden Systeem hiervoor minimaal dient te bieden? Wij ontvangen daarbij graag duidelijkheid over: - welke categorieën persoonsgegevens binnen het aangeboden Systeem onder deze eis vallen; - of van het aangeboden Systeem wordt verwacht dat persoonsgegevens van een gebruiker volledig kunnen worden verwijderd; - hoe dient te worden omgegaan met persoonsgegevens die onderdeel zijn van historische transacties, auditregistraties en/of logging; - of anonimisering of pseudonimisering van historische gegevens als alternatief voor volledige verwijdering wordt geaccepteerd wanneer volledige verwijdering niet verenigbaar is met wettelijke, beveiligings- of auditvereisten; - of het systeem bewaartermijnen voor persoonsgegevens en/of loggegevens moet kunnen ondersteunen; - of verwijdering of anonimisering ook moet worden doorgevoerd in gekoppelde systemen en/of databases; - welke functionaliteit en rapportage de opdrachtgever verwacht om een uitgevoerde verwijdering aantoonbaar te maken; - op welke wijze deze functionaliteit tijdens FAT en/of SAT zal worden getoetst. Kan de opdrachtgever tevens bevestigen dat het aangeboden Systeem wordt geacht functionaliteit te bieden waarmee persoonsgegevens conform het toepasselijke wettelijke kader kunnen worden verwijderd of geanonimiseerd, waarbij rekening wordt gehouden met eventuele wettelijke bewaarplichten, gerechtvaardigde beveiligings- en auditbelangen en andere toepasselijke uitzonderingen op het recht op gegevenswissing?	Met betrekking tot het recht op vergetelheid dient het aangeboden systeem te voldoen aan de toepasselijke wet- en regelgeving inzake gegevensbescherming. De bij deze Nota van Inlichtingen toegevoegde Verwerkersovereenkomst geeft hiervoor de benodigde kaders en nadere invulling.
3	Punt ICT.16.008 - Verduidelijkingsvraag – Single Sign-On (SSO)	In het Programma van Eisen is opgenomen dat het aangeboden Systeem Single Sign-On (SSO) dient te kunnen faciliteren door middel van inlogprocedures die gebruikmaken van federatie op basis van Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML), FIDO2 of gelijkwaardige protocollen. Kan de opdrachtgever nader specificeren welke SSO-functionaliteit en welke federatieve authenticatiestandaard(en) minimaal worden vereist? Wij ontvangen daarbij graag duidelijkheid over: - of het aangeboden Systeem rechtstreeks dient te kunnen integreren met de centrale Identity Provider (IdP) van Amsterdam UMC; - welke protocollen daadwerkelijk minimaal moeten worden ondersteund (bijvoorbeeld SAML 2.0, OpenID Connect, ADFS of FIDO2); - of met “FIDO2” wordt bedoeld dat FIDO2 als authenticatiemethode binnen de centrale Identity Provider moet kunnen worden gebruikt, of dat het aangeboden Systeem FIDO2 rechtstreeks moet ondersteunen; - of gebruikers na authenticatie bij de centrale Identity Provider zonder afzonderlijke login in het aangeboden Systeem toegang moeten krijgen; - of SSO uitsluitend voor de webapplicatie geldt of ook voor beheerfuncties en/of andere componenten van het aangeboden Systeem; - hoe de koppeling met het centrale IAM/Identity Provider-omgeving van Amsterdam UMC tot stand moet worden gebracht; - welke gegevens en/of claims vanuit de Identity Provider aan het aangeboden Systeem worden verstrekt; - of naast authenticatie via SSO ook de gebruikersrechten en autorisaties vanuit het centrale IAM-systeem moeten worden beheerd; - welke technische en functionele eisen tijdens FAT en SAT worden gehanteerd om de SSO-koppeling te accepteren. Kan de opdrachtgever tevens bevestigen dat een oplossing die SSO faciliteert via een door Amsterdam UMC ondersteunde federatieve standaard, zoals SAML 2.0 of OpenID Connect, als gelijkwaardige oplossing wordt beschouwd wanneer deze functioneel hetzelfde resultaat biedt?	ADFS is de door Amsterdam UMC geprefereerde methode voor federatieve authenticatie. Het aangeboden systeem dient hiervoor rechtstreeks gekoppeld te kunnen worden aan de Identity Provider (IdP) van Amsterdam UMC. FIDO2 wordt momenteel niet ingezet voor Single Sign-On. Na succesvolle authenticatie via SSO mag geen aanvullende gebruikersnaam- en wachtwoordcombinatie meer vereist zijn voor toegang tot het systeem. SSO dient in ieder geval van toepassing te zijn op de beheerfuncties van het systeem. Indien de oplossing aanvullende voorzieningen bevat waarvoor toegang via een webapplicatie noodzakelijk is, zal tijdens de implementatiefase worden bepaald op welke wijze authenticatie hiervoor wordt ingericht. De wijze waarop de koppeling met het IAM-systeem wordt gerealiseerd, evenals de gegevens en claims die worden uitgewisseld, wordt nader uitgewerkt tijdens het project. Het beheren van autorisaties via het IAM-systeem heeft de voorkeur. Hiervoor worden bedrijfsrollen ingericht of gebruikt. De test- en acceptatiecriteria voor de FAT en SAT kunnen op dit moment nog niet nader worden gespecificeerd, aangezien deze afhankelijk zijn van de door de opdrachtnemer ondersteunde koppelingsmethode. Voor de gewenste wijze van koppelen wordt verwezen naar het uitgangspunt dat ADFS de geprefereerde authenticatiemethode is.
4	Punt ICT.16.007 - Verduidelijkingsvraag – Multi-Factor Authenticatie (MFA)	In het Programma van Eisen is opgenomen dat bij Multi-Factor Authenticatie (MFA) de inlogprocedure gebruikmaakt van federatie op basis van Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML), FIDO2 of gelijkwaardige protocollen. Kan de opdrachtgever nader specificeren hoe MFA binnen de aangeboden oplossing dient te worden gerealiseerd? Wij ontvangen daarbij graag duidelijkheid over: - of MFA via de centrale Identity Provider (IdP) van Amsterdam UMC dient te worden afgedwongen; - of het aangeboden Systeem uitsluitend een federatieve authenticatiekoppeling met de centrale IdP hoeft te ondersteunen, waarbij de MFA door de IdP wordt uitgevoerd; - welke federatieve protocollen minimaal moeten worden ondersteund, bijvoorbeeld SAML 2.0 of OpenID Connect; - of FIDO2 als authenticatiemethode binnen de centrale Identity Provider mag worden toegepast, zonder dat het aangeboden Systeem FIDO2 rechtstreeks hoeft te ondersteunen; - of MFA verplicht moet zijn voor alle gebruikers of uitsluitend voor specifieke gebruikersgroepen en/of beheerders; - welke MFA-methoden door Amsterdam UMC worden voorgeschreven; - op welke wijze de werking van MFA tijdens FAT en SAT wordt getoetst. Kan de opdrachtgever tevens bevestigen dat wordt voldaan aan deze eis wanneer het aangeboden Systeem via een ondersteunde federatieve standaard, zoals SAML 2.0, integreert met de centrale Identity Provider van Amsterdam UMC en de daadwerkelijke MFA-authenticatie door deze centrale Identity Provider wordt uitgevoerd?	De Multi-Factor Authenticatie (MFA) wordt door Amsterdam UMC verzorgd.

5	Punt ICT.13.001 - Verduidelijkingsvraag – harmonisatieslag	In het Programma van Eisen is opgenomen dat het aangeboden Systeem ondersteuning biedt bij het uitvoeren van een harmonisatieslag. Hierbij wordt aangegeven dat een harmonisatieslag ten minste het samenvoegen van afdelingen met hun processen, werkwijzen en inrichting van systemen en datasets omvat. Kan de opdrachtgever nader specificeren welke concrete functionaliteiten van het aangeboden Systeem hierbij worden verwacht? Wij ontvangen daarbij graag duidelijkheid over: - welke afdelingen, processen, werkwijzen, systemen en datasets binnen de harmonisatieslag moeten worden samengevoegd; - of wordt verwacht dat bestaande gebruikers, autorisaties, sleutelgroepen en overige gegevens uit verschillende omgevingen kunnen worden samengevoegd; - of bestaande datasets moeten kunnen worden geïmporteerd en/of gemigreerd naar het aangeboden Systeem; - of het aangeboden Systeem verschillen en/of doublures tussen bestaande datasets, gebruikers en autorisaties moet kunnen signaleren; - of de harmonisatieslag volledig binnen het aangeboden Systeem moet kunnen worden uitgevoerd, of dat hierbij ook gebruik mag worden gemaakt van externe tooling of migratiemiddelen; - welke concrete functionaliteiten en resultaten de opdrachtgever bij oplevering als bewijs voor het voldoen aan deze eis beschouwt. Kan de opdrachtgever tevens aangeven op welke wijze deze eis tijdens de beoordeling, FAT en/of SAT objectief zal worden getoetst?	De harmonisatieslag heeft betrekking op het samenvoegen van de gegevens uit de twee bestaande Traka-omgevingen (AMC en VUmc) naar één nieuwe omgeving binnen Amsterdam UMC. Het systeem dient gebruikers, rollen, autorisaties, sleutelgroepen en datasets uit beide omgevingen te kunnen samenvoegen, importeren en migreren met behoud van integriteit en zonder ongewenste wijziging van toegangsrechten. Daarnaast moet het systeem verschillen en doublures kunnen signaleren en inzichtelijk maken. Het gebruik van externe tooling voor de migratie is toegestaan, mits de daarin verwerkte gegevens na succesvolle import en goedkeuring worden vernietigd. De concrete FAT- en SAT-criteria worden gedurende het project vastgesteld. Van de geselecteerde leverancier wordt verwacht dat deze als deskundige partij voorstellen doet voor de inrichting en toetsing van de harmonisatie.
6	Punt ICT.4.001 - Verduidelijkingsvraag – Security by Design en Security by Default	In het Programma van Eisen is opgenomen dat het aangeboden Systeem dient te voldoen aan de security-aspecten Security by Design en Security by Default, waarbij onder andere wordt aangegeven dat security-aspecten bij het ontwerp worden meegenomen en dat alle standaardinstellingen default op secure (veilig) zijn ingesteld. Kan de opdrachtgever nader specificeren aan welke concrete beveiligingsmaatregelen en/of normen het aangeboden Systeem minimaal dient te voldoen om aan deze eisen te voldoen? Wij ontvangen daarbij graag duidelijkheid over: - welke concrete securitymaatregelen onder Security by Design worden verstaan; - welke instellingen bij oplevering minimaal veilig/default secure dienen te zijn; - of hierbij specifieke eisen gelden ten aanzien van bijvoorbeeld authenticatie, autorisatie, wachtwoordbeleid, logging, netwerkcommunicatie, versleuteling en toegangsrechten; - of specifieke normen, richtlijnen of beveiligingsstandaarden van toepassing zijn; - hoe de opdrachtgever de naleving van deze eisen tijdens de beoordeling en/of acceptatie zal toetsen; - welke documentatie of bewijsstukken de opdrachtnemer hiervoor dient aan te leveren. Kan de opdrachtgever tevens bevestigen dat de beoordeling van deze eisen plaatsvindt aan de hand van vooraf vastgestelde en objectief toetsbare beveiligingscriteria?	Onder Security by Design verstaat de opdrachtgever in ieder geval: een risicogebaseerd ontwerp; integratie van informatiebeveiliging in de ontwikkel- en wijzigingscyclus; toepassing van de principes least privilege en need-to-know; een veilige architectuur en passende hardeningmaatregelen; invoervalidatie en bescherming tegen bekende kwetsbaarheden; logging en monitoring als integraal onderdeel van het ontwerp. Onder Security by Default verstaat de opdrachtgever dat bij oplevering van het systeem: standaardinstellingen geen onnodige beveiligingsrisico's introduceren; authenticatie standaard beveiligd is ingericht; autorisaties standaard beperkt zijn toegekend; logging standaard is ingeschakeld; netwerkcommunicatie standaard versleuteld plaatsvindt; gevoelige gegevens worden versleuteld; configuratie- en toegangsrechten veilig zijn ingericht. Er worden geen aanvullende beveiligingsstandaarden voorgeschreven, mits aan de genoemde uitgangspunten wordt voldaan. Wel dienen de relevante eisen uit ISO 27001 en NEN 7510 te worden gevolgd. De naleving van deze eisen wordt beoordeeld aan de hand van beschikbare en relevante certificeringen.
7	Punt ICT.3.002 - Verduidelijkingsvraag – gegevensvalidatie en toegestane tekens	In het Programma van Eisen is opgenomen: "De applicatie van het aangeboden Systeem voorziet in gegevensvalidatie en ondersteunt uitsluitend de benodigde tekens voor de invoer van gegevens t.b.v. optimale gegevensregistratie." Kan de opdrachtgever nader specificeren wat onder "gegevensvalidatie" en "uitsluitend de benodigde tekens" wordt verstaan? Wij ontvangen daarbij graag duidelijkheid over: - welke gegevens bij invoer moeten worden gevalideerd; - welke validatieregels minimaal van toepassing zijn, bijvoorbeeld ten aanzien van formaat, lengte, verplichte velden en uniciteit; - welke tekens voor de verschillende gegevensvelden zijn toegestaan; - of het gebruik van speciale tekens en diakritische tekens, zoals é, ë en ö, moet worden ondersteund; - of voor gebruikersnamen, identifiers en overige gegevens verschillende teken- en validatieregels gelden; - of de eisen ten aanzien van gegevensvalidatie mede betrekking hebben op gegevens die via koppelingen met andere systemen, zoals One Identity Manager, worden aangeleverd. Kan de opdrachtgever hiervoor een overzicht van de minimaal vereiste validatieregels en toegestane tekens beschikbaar stellen?	Met gegevensvalidatie wordt bedoeld dat de applicatie invoer controleert op basis van de uitgangspunten die voortvloeien uit de eisen rondom Security by Design. Daarbij geldt dat uitsluitend die tekens worden toegestaan die noodzakelijk zijn voor een correcte en veilige gegevensregistratie. Het systeem dient tevens ondersteuning te bieden voor diakritische tekens, zoals accenten en andere taalgebonden karakters.
8	Punt 8.12 - Verduidelijkingsvraag – Ultimo uploadlijst	In het Programma van Eisen is opgenomen dat de Ultimo uploadlijst (Bijlage 3.4) bij oplevering volledig door de opdrachtnemer dient te worden ingevuld. Kan de opdrachtgever nader specificeren welke gegevens door de opdrachtnemer dienen te worden aangeleverd en welke gegevens door de opdrachtgever beschikbaar worden gesteld? Daarnaast verzoeken wij de opdrachtgever te verduidelijken: - welke gegevensvelden uit Bijlage 3.4 door de opdrachtnemer dienen te worden ingevuld; - of de opdrachtnemer uitsluitend verantwoordelijk is voor het invullen en aanleveren van de uploadlijst, of dat de gegevens ook rechtstreeks in Ultimo moeten worden ingevoerd; - wie verantwoordelijk is voor het aanleveren van gegevens die niet door de opdrachtnemer zelfstandig kunnen worden vastgesteld; - wie verantwoordelijk is voor de controle en validatie van de aangeleverde gegevens; - wat onder een "volledig ingevulde" uploadlijst wordt verstaan; Kan de opdrachtgever tevens bevestigen dat de opdrachtnemer uitsluitend verantwoordelijk is voor het aanleveren van de gegevens waarover hij vanuit de uitvoering van de opdracht redelijkerwijs kan beschikken, en dat ontbrekende gegevens tijdig door de opdrachtgever worden aangeleverd?	Voor het invullen van de Ultimo-uploadlijst wordt verwezen naar Bijlage 3.4. De door de opdrachtnemer in te vullen velden zijn daarin grijs gemarkeerd vanaf kolom 10. De exacte invulling wordt gedurende het project nader afgestemd. Het doel is dat de opdrachtnemer de installatie-specifieke gegevens aanlevert in een format dat door het onderhoudsmanagementsysteem van de opdrachtgever kan worden ingelezen.
9	Punt 8.8 - Verduidelijkingsvraag – ontwikkeling koppeling One Identity Manager	In het Programma van Eisen is aangegeven dat één van de partijen waarmee afstemming moet plaatsvinden Intragen is, ten behoeve van de ontwikkeling van de koppeling met One Identity Manager (de PIAM-applicatie). Kan de opdrachtgever nader specificeren welke werkzaamheden en verantwoordelijkheden met betrekking tot deze koppeling tot de scope van de opdrachtnemer behoren? Wij ontvangen daarbij graag duidelijkheid over: - welke functionaliteit en gegevens tussen de sleutelkastoplossing en One Identity Manager moeten worden uitgewisseld; - welke bestaande interfaces, API's of andere koppelmogelijkheden binnen One Identity Manager beschikbaar zijn; - welke partij verantwoordelijk is voor de ontwikkeling van het betreffende deel van de koppeling; - welke werkzaamheden van Intragen worden verwacht en welke werkzaamheden van de opdrachtnemer worden verwacht; - of de kosten voor de werkzaamheden van Intragen door de opdrachtgever worden gedragen of onderdeel zijn van de aanbieding van de opdrachtnemer; - wie verantwoordelijk is voor het technisch beheer en onderhoud van de koppeling na oplevering; - wie verantwoordelijk is voor wijzigingen aan de koppeling als gevolg van toekomstige updates of wijzigingen in One Identity Manager; - welke test- en acceptatiecriteria voor de koppeling gelden binnen de FAT en SAT. Kan de opdrachtgever tevens bevestigen dat de verantwoordelijkheden en eventuele kosten voor de ontwikkeling en instandhouding van de koppeling voorafgaand aan opdrachtverlening eenduidig tussen opdrachtgever, Intragen en opdrachtnemer worden vastgesteld?	Nadere afspraken over de koppelingen worden gedurende het project uitgewerkt. Via de koppeling worden minimaal naamgegevens, pasgegevens en autorisaties uitgewisseld. Autorisaties worden in OIM bepaald op basis van bedrijfsrollen en doorgegeven aan de sleutelkastsoftware. Deze gegevensset kan in overleg worden uitgebreid. Amsterdam UMC heeft een voorkeur voor een REST API op basis van SCIM. Voor de koppeling met de sleutelkastoplossing heeft Amsterdam UMC de voorkeur dat de leverancier verantwoordelijk is voor de ontwikkeling, het testen en het werkend opleveren van de koppeling. Eventuele kosten van Intragen hoeven niet in de aanbieding te worden opgenomen. De leverancier is verantwoordelijk voor het beheer, onderhoud en toekomstige wijzigingen van de koppeling. De FAT- en SAT-criteria kunnen op dit moment nog niet worden vastgesteld, omdat deze afhankelijk zijn van de door de opdrachtnemer aangeboden koppelingsmethode.

10	Punt 8.5 - Verduidelijkingsvraag – sleutelbeheer, migratie en projectimplementatie	In het Programma van Eisen wordt aangegeven dat de leverancier in het projectimplementatieplan onder andere rekening dient te houden met het overzetten van bestaande sleutelbossen naar nieuwe ringen en identifiers, een tijdelijke handmatige uitgifte en bewaking van sleutelbossen, opleiding en training, communicatie en een duidelijke demarcatie van taken tussen leverancier en opdrachtgever. Wij begrijpen hieruit dat de leverancier naast de levering en installatie van de nieuwe sleutelkasten ook verantwoordelijk wordt gesteld voor een belangrijk deel van de operationele transitie van het bestaande sleutelbeheer naar de nieuwe situatie. Vraag: Kan de opdrachtgever nader specificeren welke werkzaamheden met betrekking tot het overzetten en tijdelijk beheren van de bestaande sleutelbossen precies tot de scope van de leverancier behoren? Daarbij ontvangen wij graag duidelijkheid over: - het totale aantal sleutelbossen dat moet worden overgezet; - of de opdrachtgever ervoor zorgdraagt dat alle over te zetten sleutelbossen op het moment van de migratie beschikbaar zijn; - wie verantwoordelijk is voor het fysiek overzetten en registreren van de sleutelbossen; - de verwachte duur en omvang van de tijdelijke handmatige uitgifte; - wat wordt verstaan onder het “bewaken” van tijdelijk uitgegeven sleutelbossen en welke registratie hierbij wordt verwacht; - wie verantwoordelijk is voor eventuele vermissing, beschadiging of foutieve registratie tijdens de migratie; - welke communicatiemomenten en rapportages gedurende de implementatie worden verwacht; - of de opdrachtgever kan bevestigen dat de demarcatiematrix door de opdrachtnemer wordt opgesteld, waarbij per activiteit expliciet wordt vastgelegd welke partij verantwoordelijk is voor de uitvoering daarvan: de opdrachtnemer of de opdrachtgever. Tot slot verzoeken wij de opdrachtgever te bevestigen dat werkzaamheden die in de demarcatiematrix niet aan de opdrachtnemer worden toegewezen, door de opdrachtgever worden uitgevoerd. Dit betreft onder andere het beschikbaar stellen van personeel voor de tijdelijke handmatige sleuteluitgifte en het beschikbaar stellen van medewerkers voor het controleren en registreren van sleutelbossen.	Het fysiek overzetten en tijdelijk beheren van de bestaande sleutelbossen behoort niet tot de scope van de leverancier. Deze werkzaamheden worden uitgevoerd door de opdrachtgever. De leverancier is verantwoordelijk voor de levering, installatie, configuratie en technische ingebruikname van het sleutelkastsysteem. Daarnaast verzorgt de leverancier de benodigde sleutelhangers of tags, de inrichting van het systeem, trainingen voor beheerders en technische ondersteuning tijdens de implementatie. Het inventariseren, labelen en overzetten van sleutels en sleutelbossen, het tijdelijke sleutelbeheer en de inhoudelijke toekenning van autorisaties vallen onder de verantwoordelijkheid van de opdrachtgever.
11	Punt 8.4 - Verduidelijkingsvraag – projectimplementatie, FAT, SAT en Proof of Concept	In het Programma van Eisen wordt voorgeschreven dat de leverancier een projectimplementatieplan opstelt, waarin onder andere een FAT, SAT, een Proof of Concept met één kast en een periode voor het verwerken van lessons learned zijn opgenomen. Tevens wordt aangegeven dat de overige kasten vervolgens volgens een vastgestelde watervalplanning worden uitgerold. Wij begrijpen hieruit dat de leverancier verantwoordelijk is voor het beheerst en bedrijfszeker realiseren van de volledige oplossing, inclusief de verschillende systeemkoppelingen. Vraag: Kan de opdrachtgever nader specificeren welke acceptatiecriteria en testvereisten gelden voor de FAT, de SAT en de Proof of Concept, en welke systemen en koppelingen minimaal onderdeel moeten zijn van deze testen? Daarnaast verzoeken wij de opdrachtgever te verduidelijken: - wie verantwoordelijk is voor het beschikbaar stellen en configureren van de benodigde 230V- en data-aansluitingen; - welke bestaande systemen en koppelingen tijdens de Proof of Concept en SAT aantoonbaar werkend moeten zijn; - wie verantwoordelijk is voor het beschikbaar stellen van benodigde licenties, configuraties, netwerkvoorzieningen en toegang tot bestaande systemen; - hoe wordt omgegaan met eventuele gebreken in bestaande apparatuur of infrastructuur die noodzakelijk is voor het functioneren van de koppelingen; - of de genoemde herstelperiode van bijvoorbeeld twee weken uitsluitend betrekking heeft op de Proof of Concept of ook op eventuele tekortkomingen in de bestaande systemen/koppelingen; - of de opdrachtgever een standaard format of protocol voor FAT en SAT beschikbaar stelt. Tot slot verzoeken wij de opdrachtgever te bevestigen dat de leverancier na een succesvol afgeronde Proof of Concept en verwerking van de lessons learned kan starten met de uitrol van de overige kasten volgens de vastgestelde planning.	Het doel van de FAT, SAT en Proof of Concept is het waarborgen van een beheerst implementatieproces en het aantonen van de functionaliteit van de oplossing. Van de leverancier wordt verwacht dat deze hiervoor zijn eigen kwaliteitssysteem, documentatie en testmethodiek toepast. Amsterdam UMC stelt hiervoor geen standaard protocollen of formats beschikbaar. De bestaande 230V- en data-aansluitingen worden door de opdrachtgever beschikbaar gesteld. Van de leverancier wordt verwacht dat vooraf wordt getoetst of deze voorzieningen voldoen aan de eisen van de aangeboden oplossing. De opdrachtgever zorgt, op aangeven van de leverancier, voor de benodigde toegang, configuraties en voorzieningen binnen de bestaande omgeving. Eventuele gebreken in de bestaande infrastructuur of systemen vallen onder de verantwoordelijkheid van de opdrachtgever. De periode van twee weken na de Proof of Concept is bedoeld om eventuele bevindingen en noodzakelijke optimalisaties te verwerken zonder de verdere uitrol in gevaar te brengen. Na een succesvolle Proof of Concept en verwerking van de lessons learned kan worden gestart met de uitrol van de overige kasten volgens de vastgestelde planning.
12	Punt 8.2 - Verduidelijkingsvraag – gecombineerde levering en CO_2-footprint	In het Programma van Eisen is opgenomen: “Bulkleveringen voorafgaand aan de installatie zijn niet toegestaan. Levering van de kasten vindt plaats per kast, rond de montagedatum van de betreffende kast.” Wij begrijpen dat hiermee wordt beoogd te voorkomen dat kasten gedurende langere tijd voorafgaand aan de installatie op locatie worden opgeslagen. Vanuit het oogpunt van duurzaamheid, beperking van het aantal transportbewegingen en reductie van de CO_2-footprint kan het echter efficiënter zijn om meerdere kasten die op dezelfde locatie en binnen een beperkte periode worden geïnstalleerd, gecombineerd te leveren. Vraag: Kan de eis worden aangepast zodat gecombineerde leveringen van meerdere kasten voor dezelfde locatie zijn toegestaan, mits deze plaatsvinden binnen een nader af te stemmen termijn voorafgaand aan de geplande installatiedatum? Hiermee kan het aantal transportbewegingen worden beperkt en kan de CO_2-footprint van de logistiek worden gereduceerd, terwijl tegelijkertijd wordt voorkomen dat de kasten onnodig lang voorafgaand aan de installatie op locatie worden opgeslagen.	Vanwege beperkte opslagmogelijkheden op de AMC-locatie is het niet wenselijk om materialen langdurig voorafgaand aan de installatie op locatie op te slaan. Opslag brengt bovendien risico's met zich mee op schade en diefstal. Gecombineerde leveringen zijn toegestaan, mits de geleverde materialen binnen één week worden verwerkt. Opslag vindt plaats op een nader te bepalen locatie en is voor risico van de opdrachtnemer. Uitgangspunt hierbij is levering in maximaal drie delen.
13	Punt 7.2 - Verduidelijkingsvraag – Intercom- en videovoorzieningen	In het PVE wordt aangegeven dat bestaande kasten zijn voorzien van een intercom met video per bedienpaneel en dat deze voorzieningen bij de migratie naar de nieuwe kasten moeten worden overgezet en hergebruikt. Tevens wordt aangegeven dat de intercom- en videostream op locatie AMC binnenkomen op het bestaande Commend-platform en op locatie VUmc op het bestaande Alphacom-stentafon-platform. Kunt u nader toelichten wat wordt bedoeld met de passage: “Aan de zijde van VUmc zijn deze posten niet aanwezig.” Daarnaast verzoeken wij u te verduidelijken: 1. Welke bestaande intercom-, camera- en overige communicatiecomponenten exact moeten worden hergebruikt; 2. Of de inschrijver verantwoordelijk is voor het demonteren, overzetten, aansluiten, programmeren en testen van deze voorzieningen; 3. Of bestaande intercom- en cameracomponenten eigendom zijn van de opdrachtgever en ter beschikking worden gesteld; 4. Of vervanging van defecte of tijdens demontage onbruikbaar gebleken bestaande componenten onderdeel is van de opdracht; 5. Welke interfaces/protocollen beschikbaar zijn voor de koppeling met het bestaande Commend-platform en het Alphacom-stentafon-platform; 6. Of de benodigde licenties, configuraties en aansluitingen op beide bestaande platformen door de opdrachtgever worden aangeleverd dan wel door de opdrachtnemer moeten worden verzorgd; 7. Welke concrete “posten” aan de VUmc-zijde niet aanwezig zijn en welke voorzieningen de opdrachtnemer daar eventueel nieuw dient te realiseren. Tot slot verzoeken wij u aan te geven of de bestaande netwerkaansluitingen per nieuwe kast/bediendeel reeds beschikbaar zijn en of hiervoor uitsluitend gebruik mag worden gemaakt van de bestaande infrastructuur.	Op de AMC-locatie is bij vrijwel iedere bestaande sleutelkast een Commend-intercom aanwezig. Deze intercoms dienen te worden hergebruikt. De leverancier verzorgt, indien nodig, het herplaatsen van deze intercoms, maar is niet verantwoordelijk voor de programmering ervan. De bestaande intercomcomponenten zijn eigendom van de opdrachtgever. Het vervangen van defecte componenten valt niet binnen de scope van de opdracht. Herplaatsing vindt plaats op verzoek en onder verantwoordelijkheid van de opdrachtgever. Er bestaat geen technische koppeling tussen de intercoms en de sleutelkasten. De intercom wordt uitsluitend gebruikt voor communicatie met de meldkamer van de beveiliging. Op de AMC-locatie zijn geen aanvullende licenties of configuratiewijzigingen nodig. Op de VUmc-locatie maakt het (her)plaatsen van intercomvoorzieningen geen onderdeel uit van deze opdracht. De bestaande netwerkaansluitingen van de huidige sleutelkasten worden hergebruikt. Hiervoor dient de leverancier vooraf de MAC-adressen van de nieuwe kasten aan te leveren, zodat deze door de opdrachtgever kunnen worden geregistreerd binnen de ICT-omgeving.

14	Punt 2.5 - Verduidelijkingsvraag – Certificering slot	In het Programma van Eisen wordt gesteld: “Het slot waarmee de kast elektronisch en handmatig ontgrendeld wordt dient voorzien te zijn van een passende certificering, zoals SKG***.” Kunt u verduidelijken welke certificering en welk beveiligingsniveau minimaal wordt verlangd? Wij constateren dat in de eis wordt gesproken over een “passende certificering, zoals SKG***”. Wij begrijpen hieruit dat naast SKG*** ook een andere certificering kan worden geaccepteerd, mits deze aantoonbaar een gelijkwaardig beveiligingsniveau biedt. Kunt u bevestigen: of SKG* als minimaal vereist beveiligingsniveau** moet worden beschouwd; of een aantoonbaar gelijkwaardige certificering eveneens wordt geaccepteerd; of de certificering betrekking moet hebben op het complete toegepaste slotmechanisme, inclusief de elektronische en handmatige ontgrendeling; welke documentatie als bewijs wordt geaccepteerd, bijvoorbeeld een officieel certificaat of testrapport van een geaccrediteerde onafhankelijke instantie; of de certificering specifiek betrekking moet hebben op de toepassing in een elektronische sleutelkast. Deze verduidelijking is noodzakelijk om de eis voor alle inschrijvers op een objectieve en gelijkwaardige wijze te kunnen beoordelen.	De eis heeft betrekking op een minimale inbraakwerendheid die vergelijkbaar is met EN 14450 klasse S1. Een hogere classificatie, zoals EN 14450 klasse S2, heeft de voorkeur en wordt positief gewaardeerd bij de beoordeling, maar is geen minimumeis. Ook oplossingen zonder formele EN 14450-certificering worden geaccepteerd, mits objectief kan worden aangetoond dat zij een gelijkwaardig of hoger beveiligingsniveau bieden dan EN 14450 klasse S1. Wij zullen dit aanpassen in de documenten bij de Nota van Inlichtingen II
15	Punt 2.4 - Verduidelijkingsvraag – Inbraakwerendheid conform EN 14450	In het Programma van Eisen wordt gesteld: “De aangeboden apparatuur voldoet minimaal aan lichte mate van inbraakwerendheid vergelijkbaar met de norm EN 14450.” Kunt u nader specificeren welk beveiligingsniveau hiermee wordt bedoeld? EN 14450 kent onder meer de classificaties S1 en S2. In de betreffende eis wordt echter gesproken over een “lichte mate van inbraakwerendheid” en wordt verwezen naar een niveau dat “vergelijkbaar” is met EN 14450. Wij verzoeken u daarom te verduidelijken: of minimaal EN 14450 S1 wordt verlangd; of ook een aantoonbaar gelijkwaardig niveau wordt geaccepteerd wanneer het aangeboden product niet formeel volgens EN 14450 is gecertificeerd; welke documentatie als bewijs van gelijkwaardigheid wordt geaccepteerd, bijvoorbeeld een testrapport, fabrikantverklaring of technische documentatie; of de verwijzing naar EN 14450 uitsluitend bedoeld is als referentieniveau voor de gewenste inbraakwerendheid, en niet als vereiste dat de aangeboden apparatuur formeel volgens EN 14450 moet zijn gecertificeerd. Deze verduidelijking is noodzakelijk om de eis op een objectieve en voor alle inschrijvers gelijkwaardige wijze te kunnen beoordelen.	Het minimaal vereiste beveiligingsniveau is vergelijkbaar met EN 14450 klasse S1. EN 14450 klasse S2 of hoger wordt positief gewaardeerd, maar is geen knock-outeis. Een aantoonbaar gelijkwaardige oplossing zonder formele EN 14450-certificering wordt eveneens geaccepteerd, mits objectief kan worden aangetoond dat het beveiligingsniveau minimaal gelijkwaardig is aan EN 14450 klasse S1.
16	Punt 3.2 - Verduidelijkingsvraag – nader te bepalen RAL-kleur	In het Programma van Eisen is opgenomen: “Het systeem wordt uitgevoerd in één nader te bepalen RAL-kleur en voorzien van een dichte of transparante deur, zoals per sleutelkast aangegeven, zie bijlage 4 en 4.1.” Kunt u aangeven op welk moment de definitieve RAL-kleur wordt vastgesteld en gecommuniceerd? Indien deze kleur bij inschrijving nog niet bekend is, mogen wij voor de prijsstelling uitgaan van een standaard RAL-kleur, waarbij eventuele meerkosten als gevolg van een later gekozen afwijkende RAL-kleur afzonderlijk kunnen worden verrekend?	Hier komt de aanbestedende dienst graag op terug in de Nota van Inlichtingen II.
17	Certificering	Is het benodigd/verplicht dat sleutelkasten SKG of anders gecertificeerd zijn? Voor binnen sleutelkasten die alleen voor sleutels en keytags gehanteerd worden zien wij bij soortgelijke omgevingen een brandwerendheid of brandpreventie certificering niet terug als eis.	Nee, een specifieke SKG-certificering wordt niet verplicht voorgeschreven. De aangeboden oplossing dient minimaal te voldoen aan een inbraakwerendheid die vergelijkbaar is met EN 14450 klasse S1. Een aantoonbaar gelijkwaardige of hogere beveiligingsoplossing wordt eveneens geaccepteerd.
18	Data exit strategie	•Er staat bij hoofdstuk 7 Data exit strategie binnen Bijlage 3 Programma van Eisen de wens om de data op leesbaar en machine formaat te exporteren en daarna te importeren. Wordt hier alle data beschikbaar binnen de sleutelkast software mee bedoeld of alleen specifieke data?	Met de data-exitstrategie wordt specifiek bedoeld dat gegevens met betrekking tot passen en pashouders op een leesbaar en machineleesbaar formaat kunnen worden geëxporteerd. Deze gegevens moeten als basis kunnen dienen voor dienstverlening door een eventuele opvolgende leverancier.
19	Te hanteren marge(s)	Ter verificatie: de 25% marge voor toe- en afname aan gebruikers, geldt dit alleen voor het aantal gebruikers binnen de software of wilt het Stichting Amsterdam UMC ook 25% extra marge aan sleutelposities binnen de sleutelkluizen hanteren?	De genoemde marge van 25% heeft betrekking op zowel het aantal gebruikers als de schaalbaarheid van de oplossing. De oplossing moet ondersteunen dat in de toekomst circa 25% meer pashouders gebruik kunnen maken van het systeem. Daarnaast moet ook uitbreiding van het aantal sleutelposities mogelijk zijn.
20	PIAM	Moet de koppeling met de toekomstige PIAM oplossing ook al afgeprijsd worden binnen de aanbieding of hoeft binnen de eerste fase alleen de koppeling met de EAL & Nedap omgeving gerealiseerd te worden?	Binnen de opdracht dient een koppeling met de OIM/PIAM-omgeving te worden gerealiseerd. Hiervoor wordt een prijs uitgevraagd. Een koppeling met de EAL- en AEOS-omgeving maakt geen onderdeel uit van de opdracht. Het toepassen van Nedap- en/of EAL-paslezers is een keuze van de leverancier.
21	Toekomstige leveringen	Wat is de omvang van de twee sleutelkluizen die in de aankomende twee jaar geplaatst zullen worden? Deze moeten binnen de eerste aanbieding afgeprijsd worden, echter is het niet bekend wat de omvang van deze kasten betreft.	De exacte omvang van deze optionele kasten is op dit moment nog niet bekend. Om die reden is in het prijsopgaveformulier uitgegaan van een referentie- of gemiddelde kast. Inschrijver hoeft hiervoor geen eigen inschatting te maken; de prijs van de referentiekast wordt gebruikt voor de berekening van de totale vergelijkingsprijs (TCO). Op deze wijze kan Aanbestedende dienst de inschrijvingen onderling op een objectieve en vergelijkbare manier beoordelen. In aanvulling hierop merkt Aanbestedende dienst op dat in de aanbestedingsleidraad momenteel wordt verwezen naar een gemiddelde prijs van de optionele kasten. Dit is niet correct. De beoordeling vindt plaats op basis van de prijs van de opgenomen referentiekast. Aanbestedende dienst zal dit punt verduidelijken en corrigeren in Nota van Inlichtingen II.
22	Optimalisatie selutelkasten	Is het toegestaan om de bestaande samenstelling zoals deze nu is in de sleutelkasten te optimaliseren? Op sommige locatie's zijn twee losse sleutelkasten per één terminal gebruikt terwijl deze samengevoegd zouden kunnen worden binnen één sleutelkast. Echter neemt het formaat van de sleutelkast dan wel iets toe of worden de panelen binnen de sleutelkast compacter.	Het optimaliseren van de huidige kastindeling is toegestaan, mits de benodigde bouwkundige aanpassingen zoveel mogelijk worden beperkt. Daarnaast dient rekening te worden gehouden met de afmetingen van de bestaande sleutelbossen, zodat deze passend blijven binnen de aangeboden oplossing.
23	Bijlage 3 Programma van Eisen, art.2 producteisen 2.4	De norm kent daarbij twee verschillende klassen: S1 en S2. Welke klase bedoeld opdrachtgever?	Het minimaal vereiste beveiligingsniveau is vergelijkbaar met EN 14450 klasse S1. EN 14450 klasse S2 of hoger wordt positief gewaardeerd, maar is geen minimumeis. Gelijkwaardige oplossingen worden geaccepteerd, mits het beveiligingsniveau objectief aantoonbaar minimaal gelijkwaardig is aan klasse S1.
24	Bijlage 3 Programma van Eisen, art.2 producteisen 2.4	In hoeverre is deze norm van toepassing op de bestaande sleutelbeheersystemen? Er bestaan naar ons inzicht momenteel geen sleutelbeheersystemen (sleutelkasten) die voldoen aan deze norm (Zowel klasse 1 als klasse 2. Hoe ziet opdrachtgever dit?	De verwijzing naar EN 14450 dient als referentie voor het gewenste niveau van inbraakwerendheid. Het is niet vereist dat de aangeboden oplossing formeel volgens deze norm is gecertificeerd. Oplossingen die aantoonbaar een gelijkwaardig of hoger beveiligingsniveau bieden dan EN 14450 klasse S1 worden eveneens geaccepteerd.
25	Bijlage 3 Programma van Eisen, art.2 producteisen 2.5	Opdrachtnemer verzoekt opdrachtgever het doel van eis 2.5 nader toe te lichten. Indien deze eis is opgenomen vanuit het oogpunt van inbraakwerendheid, merken wij op dat de inbraakwerendheid van een sleutelbeheersysteem wordt bepaald door de totale constructie van kast, deur, verankering en sluitmechanisme, en niet uitsluitend door het toegepaste slot. Daarnaast wordt de gewenste mate van inbraakwerendheid reeds afgedekt in eis 2.4. Vrijwel alle professionele sleutelmanagementsystemen maken gebruik van speciaal voor kasten ontwikkelde mechanische of elektronische meubelsloten, waarvoor een SKG***-certificering veelal niet beschikbaar is. De eis lijkt daardoor marktbeperkend zonder dat dit aantoonbaar leidt tot een hoger beveiligingsniveau van het totale systeem. Daarbij worden de sleutelkasten toegepast in gecontroleerde binnenruimten en zijn deze voorzien van elektronische autorisatie, logging en alarmering bij onbevoegde toegang. Opdrachtnemer verzoekt opdrachtgever daarom eis 2.5 te wijzigen naar: "Het slot waarmee de kast elektronisch en handmatig wordt ontgrendeld dient geschikt te zijn voor professioneel sleutelbeheer en aantoonbaar passend te zijn voor de beoogde toepassing. Gelijkwaardige certificeringen of aantoonbaar gelijkwaardige beveiligingsoplossingen worden geaccepteerd." Kan opdrachtgever hiermee instemmen?	De opdrachtgever handhaaft de eis dat de aangeboden oplossing minimaal een inbraakwerendheid moet bieden die vergelijkbaar is met EN 14450 klasse S1. Een hoger beveiligingsniveau, zoals EN 14450 klasse S2, wordt positief gewaardeerd, maar is geen knock-outeis. Ook oplossingen zonder formele EN 14450-certificering komen in aanmerking, mits objectief kan worden aangetoond dat zij een gelijkwaardig of hoger beveiligingsniveau bieden dan EN 14450 klasse S1.

26	Bijlage 5 - Verklaring Russische betrokkenheid	Kan Amsterdam UMC toelichten welke eisen worden gesteld aan de herkomst van de aangeboden hardware en software? In de aanbestedingsstukken worden beperkingen gesteld ten aanzien van producten van Russische herkomst. Wij ontvangen graag een nadere toelichting op het beleid van Amsterdam UMC ten aanzien van software, hardware en clouddiensten afkomstig uit andere landen buiten de Europese Unie, waaronder China. Tevens vernemen wij graag of hiervoor aanvullende eisen, beperkingen of beoordelingscriteria gelden.	Voor hardware, software en clouddiensten afkomstig uit andere landen geldt dat Amsterdam UMC de geldende Europese en nationale wet- en regelgeving volgt. Behoudens specifieke wettelijke beperkingen, sancties of andere dwingendrechtelijke voorschriften worden leveranciers, producten of diensten niet uitgesloten op basis van nationaliteit of land van herkomst alleen. Er gelden derhalve geen aanvullende uitsluitingsgronden, beperkingen of beoordelingscriteria die specifiek zijn gebaseerd op de herkomst van hardware, software of clouddiensten uit landen buiten de Europese Unie, zoals China. Een dergelijke beoordeling zou in strijd kunnen zijn met de aanbestedingsrechtelijke beginselen van gelijke behandeling en non-discriminatie.
27	Bijlage 3 - Programma van Eisen - Eis 1.7	Kan Amsterdam UMC aangeven binnen welke termijn de dienstverlening, hardware en software volledig dienen te voldoen aan de genoemde wet- en regelgeving (NIS2, CER/Wwke en CRA)? Uit de huidige formulering blijkt dat binnen één (1) maand na ingangsdatum van de overeenkomst dient te worden aangetoond op welke wijze aan deze wet- en regelgeving wordt voldaan of zal worden voldaan. Het is echter niet duidelijk op welk moment daadwerkelijke naleving van de genoemde wet- en regelgeving wordt vereist. Graag ontvangen wij een nadere toelichting op de beoogde implementatie- en nalevingstermijnen.	Voor wet- en regelgeving die op de ingangsdatum van de overeenkomst reeds van kracht is en van toepassing is op de opdracht, dient de leverancier vanaf de ingangsdatum aantoonbaar compliant te zijn. Voor wettelijke verplichtingen die op dat moment nog niet volledig van kracht zijn, geldt dat de leverancier uiterlijk vanaf de wettelijk voorgeschreven ingangsdatum van de betreffende verplichting aantoonbaar moet voldoen aan de geldende eisen.
28	Bijlage 3 - Programma van Eisen - Eis 2.4	In eis 2.4 wordt gesteld dat de aangeboden apparatuur minimaal dient te voldoen aan een lichte mate van inbraakwerendheid vergelijkbaar met EN 14450. Voor zover ons bekend is EN 14450 primair bedoeld voor inbraakwerende kasten en sleutelkluizen. Voor elektronische sleutelbeheersystemen zijn geen gangbare certificeringen of classificaties beschikbaar die rechtstreeks op deze norm aansluiten. Kan Amsterdam UMC aangeven: - Welke objectieve en toetsbare criteria worden gehanteerd om te beoordelen of een elektronisch sleutelbeheersysteem aan deze eis voldoet; - Welke certificaten, testrapporten of andere bewijsmiddelen worden geaccepteerd; - Hoe inschrijvers zonder een specifieke EN 14450-certificering voor een sleutelbeheersysteem kunnen aantonen dat sprake is van een gelijkwaardig beveiligingsniveau? Indien dergelijke objectieve beoordelingscriteria niet beschikbaar zijn, verzoeken wij Amsterdam UMC deze eis te heroverwegen dan wel nader te concretiseren.	De eis verwijst naar een minimale inbraakwerendheid die vergelijkbaar is met EN 14450 klasse S1. Oplossingen zonder formele EN 14450-certificering worden eveneens geaccepteerd, mits met objectieve bewijsmiddelen kan worden aangetoond dat sprake is van een gelijkwaardig of hoger beveiligingsniveau. Een hoger niveau, zoals EN 14450 klasse S2, wordt positief gewaardeerd maar is niet verplicht.
29	Bijlage 3 - Programma van Eisen - Eis 2.5	Kan Amsterdam UMC toelichten waarom voor het slot van de aangeboden sleutelkast een certificering zoals SKG*** wordt verlangd? Voor zover ons bekend worden elektronische sleutelbeheersystemen en sleutelkasten niet gebruikelijk beoordeeld of gecertificeerd op basis van SKG-classificaties. Hierdoor is onduidelijk welke relatie Amsterdam UMC ziet tussen deze certificering en de beoogde toepassing binnen deze aanbesteding. Gelet hierop verzoeken wij Amsterdam UMC te motiveren waarom deze eis noodzakelijk wordt geacht en of Amsterdam UMC bereid is deze eis te heroverwegen.	De eis is bedoeld om een minimale mate van inbraakwerendheid te waarborgen die vergelijkbaar is met EN 14450 klasse S1. Een specifieke SKG-certificering is daarbij niet verplicht. Ook aantoonbaar gelijkwaardige oplossingen worden geaccepteerd, mits objectief kan worden aangetoond dat minimaal hetzelfde beveiligingsniveau wordt geboden.
30	Bijlage 3 - Programma van Eisen - Eis 5.5/5.6	In eis 5.5 en 5.6 wordt verwezen naar de "NFU-referentiearchitectuur Gegevensuitwisseling" als bijlage bij respectievelijk eis 5.6 en 5.5. Wij kunnen deze bijlage echter niet terugvinden in de aanbestedingsstukken. Kan Amsterdam UMC de betreffende referentiearchitectuur beschikbaar stellen en aangeven welke versie van toepassing is op deze aanbesteding?	De verwijzing in eis 5.5 en 5.6 is onjuist. Hier wordt verwezen naar Bijlage 2, de NFU Algemene Inkoopvoorwaarden. Dit wordt gecorrigeerd in de aanbestedingsstukken. De aangepaste versie wordt beschikbaar gesteld bij de tweede Nota van Inlichtingen.
31	Bijlage 3 - Programma van Eisen - Eis 5.5/5.6	Kan Amsterdam UMC bevestigen dat uitsluitend een koppeling met One Identity Manager (OIM) gerealiseerd dient te worden en dat OIM hierbij fungeert als bronsysteem voor de personeels- en autorisatiegegevens die worden uitgewisseld met het sleutelbeheersysteem?	Ja, uitsluitend een koppeling met One Identity Manager (OIM) dient te worden gerealiseerd. OIM fungeert daarbij als bron voor de personeels- en autorisatiegegevens die met het sleutelbeheersysteem worden uitgewisseld.
32	Bijlage 3 - Programma van Eisen - Eis 6.5	Kan Amsterdam UMC verduidelijken wat wordt bedoeld met het onbevoegd openen van een sleutelkast? Begrijpen wij correct dat hiermee een braakpoging of andere vorm van ongeautoriseerde toegang wordt bedoeld? Zo niet, welke gebeurtenissen dienen volgens Amsterdam UMC een alarmmelding richting de meldkamer te genereren?	Met onbevoegd openen wordt een inbraak(poging) of andere ongeautoriseerde toegang tot de sleutelkast bedoeld.
33	Programma van Eisen - Bijlage 3 - Eis 7.2	Kan Amsterdam UMC verduidelijken welke voorzieningen worden bedoeld met de passage "deze voorzieningen moeten worden overgezet (hergebruikt)"? Begrijpen wij correct dat hiermee uitsluitend de intercom- en videovoorzieningen worden bedoeld, of dienen tevens andere componenten te worden hergebruikt?	Met het hergebruiken van voorzieningen wordt uitsluitend het hergebruiken van de bestaande video-intercomvoorzieningen bedoeld. Voor verdere toelichting wordt verwezen naar het antwoord op vraag 13.
34	Programma van Eisen - Bijlage 3 - Eis 7.2	Dienen alle nieuw te plaatsen sleutelkasten te worden voorzien van een intercom- en videovoorziening, of geldt deze eis uitsluitend voor de locaties waar momenteel reeds een intercom- en videovoorziening aanwezig is?	Nee, niet alle nieuw te plaatsen sleutelkasten hoeven te worden voorzien van een intercom- en videovoorziening. Alleen bestaande intercomvoorzieningen worden hergebruikt. Op locaties waar momenteel geen intercom aanwezig is, hoeft geen nieuwe voorziening te worden gerealiseerd.
35	Programma van Eisen - Bijlage 3 - Eis 7.2	Kan Amsterdam UMC aangeven welke partij verantwoordelijk is voor het beheer, onderhoud en de ondersteuning van de bestaande intercom- en videovoorzieningen en de bijbehorende platformen (Commend respectievelijk Alphacom-Stentofon)?	Het beheer, onderhoud en de ondersteuning van de bestaande intercom- en videovoorzieningen en de bijbehorende platformen zijn de verantwoordelijkheid van de opdrachtgever.
36	Programma van Eisen - Bijlage 3 - Eis 7.3, 5.5, 5.6 en 8.8	Kan Amsterdam UMC verduidelijken hoe eis 7.3 zich verhoudt tot de eisen 5.5, 5.6 en 8.8? In eis 7.3 wordt gesproken over een koppeling met een nog in ontwikkeling zijnd PIAM-systeem. In de eisen 5.5 en 5.6 wordt echter verwezen naar een koppeling met One Identity Manager (OIM) en in eis 8.8 wordt One Identity Manager omschreven als de PIAM-applicatie. Begrijpen wij correct dat hierbij sprake is van hetzelfde systeem? Indien dit het geval is, vernemen wij graag of dit systeem reeds beschikbaar is of nog in ontwikkeling is. Indien het verschillende systemen betreft, ontvangen wij graag een toelichting op de vereiste koppelingen en de daarbij behorende scope.	Ja, in de genoemde eisen wordt hetzelfde systeem bedoeld. One Identity Manager (OIM) is binnen Amsterdam UMC de IAM- en PIAM-oplossing. Voor de verdere specificaties van deze koppeling wordt verwezen naar het antwoord op vraag 9.
37	Programma van Eisen - Bijlage 3 - Eis 7.4	Kan Amsterdam UMC verduidelijken hoe eis 7.4 zich verhoudt tot de gewenste inrichting van het totale sleutelbeheersysteem? Op locatie VUmc dient een koppeling met Winguard te worden gerealiseerd en op locatie AMC met Inter. Wij vernemen graag of wordt uitgegaan van één centrale beheersomgeving voor beide locaties, of dat per locatie een afzonderlijke omgeving dient te worden ingericht en beheerd. Tevens ontvangen wij graag een toelichting op de gewenste architectuur (schematische weergave) en de onderlinge samenhang van deze koppelingen.	Voor locatie AMC bestaat reeds een koppeling tussen INTER en het huidige sleutelbeheersysteem. Deze koppeling dient ongewijzigd te worden overgenomen en maakt onderdeel uit van de opdracht. Voor locatie VUmc bestaat momenteel geen koppeling tussen het bestaande sleutelbeheersysteem en Winguard. De realisatie van deze koppeling valt vooralsnog buiten de scope van de opdracht. Amsterdam UMC onderzoekt nog op welke wijze deze integratie in de toekomst wordt ingericht. De voornaamste wens is dat alarmmeldingen, zoals ongeoorloofd geopende deuren, in Winguard kunnen worden weergegeven. Het bedienen van sleutelkasten via Winguard is geen vereiste.
38	Programma van Eisen - Bijlage 3 - Eis 9.6	Kan Amsterdam UMC verduidelijken hoe de in eis 9.6 genoemde oplostijd wordt toegepast indien voor het oplossen van een storing afstemming of medewerking van derden noodzakelijk is? Wij ontvangen graag een toelichting op de wijze waarop storingen worden beoordeeld (KPI) wanneer de oorzaak geheel of gedeeltelijk buiten de invloedsfeer van Opdrachtnemer ligt.	De opgegeven respons- en hersteltijden worden als KPI gehanteerd. Indien de oorzaak van een storing buiten de invloedsfeer van de opdrachtnemer ligt, wordt in onderling overleg bepaald hoe de storing verder wordt afgehandeld en beoordeeld.
39	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - 1.6	Wanneer begint en eindigt de termijn en geldt deze per kast, locatie, fase of volledig project?	Aanbestedende dienst gaat ervan uit dat met de termijn de onderhouds- en supportperiode wordt bedoeld. Deze termijn start na oplevering van de laatste sleutelkast. Voor iedere kast geldt een minimale looptijd van vijf (5) jaar, met een maximale looptijd van tien (10) jaar. Een nadere uitwerking is opgenomen in artikel 8 van Bijlage 1, Conceptovereenkomst.
40	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - 1.6	Wordt deze niet toegerekend en leidt ze tot termijnverlenging en vergoeding van meerkosten?	Aanbestedende dienst vraagt Gegadigde om de vraag te concretiseren omdat niet duidelijk is naar welke situatie of bepaling wordt verwezen.
41	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - Prijscriterium	Is €400.000 tot €500.000 alleen puntenschaal of ook minimum, maximum of uitsluitingsgrens	€ 500.000 betreft de maximale toegestane vergelijkingsprijs. Inschrijvingen boven dit bedrag worden uitgesloten van verdere deelname aan de aanbesteding. Onder € 400.000 mag worden ingeschreven, maar hiervoor wordt het maximaal aantal van 30 punten toegekend.. Dit wordt verduidelijkt in de aangepaste aanbestedingsstukken die bij de tweede Nota van Inlichtingen worden gepubliceerd.
42	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - Prijsformule	Welke score geldt buiten de bandbreedte en wordt afgetopt op 30 en 0?	Zie het antwoord op vraag 41.
43	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - Prijsblad	Welke kostencomponenten vallen limitatief in prijs en TCO?	Opgegeven prijzen voor de levering, montage en onderhoud van de kasten zij all-in. Het is niet toegestaan om, naast de in het Prijzenblad opgegeven tarieven, andere kosten in rekening te brengen bij Opdrachtgever.
44	EA Sleutelkasten Aanbestedingsleidraad - Amsterdam UMC - Prijsblad	Welke objectieve prijsbepaling geldt bij latere afname?	Zie tevens het antwoord op vraag 21. De omvang van de optionele kasten is nog niet bekend. Daarom wordt voor de berekening van de vergelijkingsprijs uitgegaan van een referentie- of gemiddelde kast. Indien de optionele kasten daadwerkelijk worden afgenomen, worden hierover nadere prijsafspraken gemaakt die aansluiten bij de prijsverhoudingen zoals opgenomen in het prijsopgaveformulier.
45	Programma van Eisen - Bijlage 3 - Eis 9.3, Eis 14 en overeenkomst 9	Welke regeling geldt voor onderhoud, software, licenties, onderdelen en diensten?	De vraag is onvoldoende specifiek om te kunnen beantwoorden. Wij verzoeken u uw vraag ten behoeve van de tweede Nota van Inlichtingen nader te concretiseren.
46	Overeenkomst 2.3	Wanneer wordt deze gepubliceerd en krijgen inschrijvers voldoende tijd voor vragen?	Aanbestedende dienst vraagt Gegadigde om de vraag te concretiseren omdat niet duidelijk is waar met "deze" naar wordt verwezen. Voor de planning en de beschikbare termijnen voor het stellen van vragen wordt verwezen naar de planning zoals gepubliceerd op TenderNed.
47	Programma van Eisen - Bijlage 3 - Eis 5.5, 5.6, 7.3, 7.4 en 8.8	Wie is per koppeling verantwoordelijk voor ontwikkeling, test, documentatie, beveiliging en beheer?	Voor de verantwoordelijkheden ten aanzien van ontwikkeling, testen, documentatie, beveiliging en beheer van de koppelingen wordt verwezen naar het antwoord op vraag 9.

48	PvE koppelingen en oplevering	Moeten koppelingen werken of hoeft alleen de mogelijkheid te worden aangetoond en wat valt in de vaste prijs?	De benodigde koppelingen dienen bij oplevering volledig werkend te zijn. Handmatig beheer van pashouders, pasgegevens en autorisaties is niet toegestaan. Het realiseren van werkende koppelingen maakt onderdeel uit van de vaste prijs. Voor de verdeling van verantwoordelijkheden wordt verwezen naar het antwoord op vraag 9.
49	Programma van Eisen - Bijlage 3 - Eis 8.4-8.6 en acceptatieprotocol	Welke criteria, procedure en termijnen gelden en wanneer geldt acceptatie?	Het uitgangspunt is dat opdrachtgever en opdrachtnemer overeenstemming bereiken over het plan van aanpak en de wijze waarop de implementatie wordt uitgevoerd. Vervolgens dient dit plan beheerst en volgens afspraak te worden gerealiseerd.
50	Overeenkomst 8.1	Start de looptijd na eerste kast, laatste kast of integrale acceptatie?	De looptijd van de overeenkomst vangt aan na de integrale acceptatie van de oplossing, na oplevering van de laatste sleutelkast. De aanbestedingsdocumenten zullen naar aanleiding van de tweede Nota van Inlichtingen hierop worden aangepast.
51	Overeenkomst 3.5	Worden materiële wijzigingen als wijziging of meerwerk behandeld?	Wijzigingen van de overeenkomst worden behandeld conform artikel 3.5 van de conceptovereenkomst. Eventuele wijzigingen zijn uitsluitend van kracht nadat deze schriftelijk door beide partijen zijn overeengekomen. Of een wijziging leidt tot een aanpassing van de overeengekomen werkzaamheden of prestaties, wordt per wijzigingsverzoek beoordeeld op basis van de aard en omvang van de betreffende wijziging. Een materiële wijziging wordt derhalve niet automatisch als meerwerk aangemerkt. Een vergoeding wordt mogelijk pas aangepast nadat het als meerwerk wordt aangemerkt
52	Bijlagen 4 en 4.1	Mogen gegevens als juist gelden en hoe worden afwijkingen behandeld?	Ja, de door Aanbestedende dienst verstrekte gegevens mogen als juist worden beschouwd. De gegunde opdrachtnemer dient voorafgaand aan levering de locaties in te meten en de maatvoering te verifiëren. Indien na deze verificatie blijkt dat geleverde kasten niet passend zijn voor de betreffende locatie, ligt het risico en de verantwoordelijkheid hiervoor bij opdrachtnemer. Deze verplichting wordt opgenomen in het Programma van Eisen in de Nota van Inlichtingen II.
53	Gunningscriterium inpasbaarheid	Wie draagt planning, coördinatie en aansprakelijkheid voor fouten of schade van de derde?	Aanbestedende dienst draagt dit. De door u genoemde werkzaamheden of verantwoordelijkheden maken geen onderdeel uit van de scope van deze opdracht.
54	Programma van Eisen - Bijlage 3 - Eis 5.3	Voldoet een oplossing die uitsluitend zes cijfers ondersteunt?	Ja, deze voldoet.
55	Programma van Eisen - Bijlage 3 - Eis 5.5/5.6	Welke objecten worden uitgewisseld, in welke richting en welk systeem initieert?	Voor een beschrijving van de uit te wisselen gegevens, de gegevensstromen en de werking van de koppelingen wordt verwezen naar het antwoord op vraag 9.
56	Programma van Eisen - Bijlage 3 - Eis 6.5	Welke meldingen, protocollen, overdrachtspunten en hardware zijn vereist?	De softwareapplicatie van het sleutelkastsysteem dient bij relevante gebeurtenissen een actieve pop-upmelding te genereren, voorzien van een bijbehorend akoestisch signaal.
57	Programma van Eisen - Bijlage 3 - Eis 7.3/7.4	Welke specificaties, testomgevingen, testdata en verantwoordelijkheden gelden?	De specificaties van de koppelingen worden gedurende het project gezamenlijk nader uitgewerkt. Voor de PIAM-koppeling dient naast een productieomgeving ook een acceptatieomgeving beschikbaar te zijn, zodat wijzigingen aan de koppeling gecontroleerd kunnen worden getest. De gegevens in de acceptatieomgeving zijn daarbij identiek aan de gegevens in de productieomgeving. Voor de koppelingen met Winguard en Barco Opspace/Control is uitsluitend een productieomgeving vereist.
58	Programma van Eisen - Bijlage 3 - Eis 8.3 en 8.6	Hoe wordt planning behandeld als specificaties of voorzieningen ontbreken?	Indien ondanks een passende planning noodzakelijke voorzieningen door overmacht niet tijdig beschikbaar zijn, treden opdrachtgever en opdrachtnemer hierover in overleg om tot een redelijke oplossing te komen. De bepalingen in hoofdstuk 8 zijn mede bedoeld om dergelijke onzekerheden zoveel mogelijk te beperken.
59	Programma van Eisen - Bijlage 3 - Eis 10.1	Moeten alle rapportages in beide formaten en wordt CSV geaccepteerd?	De in de vraag genoemde eis 10.1 over rapportages is niet teruggevonden. In het Programma van Eisen heeft eis 10.1 betrekking op garantie en onderhoud. Wij verzoeken u daarom de verwijzing naar de betreffende eis nader te specificeren.
60	Programma van Eisen - Bijlage 3 - Eis ICT.9.003-9.015	Welke brondata, mapping, rapportages, kwaliteitsregels en acceptatiecriteria gelden?	De brondata bestaat uit de gegevens die momenteel beschikbaar zijn in de twee bestaande Traka-omgevingen. Met de mapping wordt bedoeld het vertalen van de bestaande datastructuur naar de datastructuur van de aangeboden oplossing. Deze mapping is op dit moment nog niet beschikbaar. Om die reden kunnen ook de bijbehorende kwaliteitsregels nog niet nader worden gespecificeerd. Als acceptatiecriterium voor de datamigratie geldt dat minimaal 99% van de passen zonder handmatige aanpassingen correct functioneert in het nieuwe systeem. Daarnaast dient het systeem onderscheid te kunnen maken tussen identieke pasnummers van verschillende locaties. Zo moet bijvoorbeeld pasnummer 10 van locatie AMC afzonderlijk kunnen worden beheerd ten opzichte van pasnummer 10 van locatie VUmc, inclusief de daarbij behorende autorisaties.
61	Programma van Eisen - Bijlage 3 - Eis ICT.9.010-9.015	Zijn analyse, microbiologie en patiënten niet van toepassing en kan dit naar sleutelbeheer worden vertaald?	De genoemde voorbeelden met betrekking tot microbiologie en patiënten zijn niet van toepassing op deze opdracht en kunnen in deze context buiten beschouwing worden gelaten. Voor deze eis is het van belang dat de data binnen het systeem op een adequate wijze gefilterd kan worden.
62	Gunningscriterium inpasbaarheid	Wie draagt planning, coördinatie en aansprakelijkheid voor fouten of schade van de derde?	Zie het antwoord op vraag 53
63	Programma van Eisen - Bijlage 3 - Eis ICT.14.001	Tot welke omgevingen moet AUMC toegang krijgen en wordt een klantgebonden OTAP verlangd?	Amsterdam UMC dient toegang te hebben tot een acceptatieomgeving waarin wijzigingen aan koppelingen gecontroleerd kunnen worden getest. Het beschikbaar stellen van een volledige, klantgebonden OTAP-omgeving is niet vereist en valt buiten de scope van deze aanbesteding.
64	Programma van Eisen - Bijlage 3 - Eis ICT.14.007	Hoe wordt end-of-life van OS en derde componenten behandeld?	Gedurende de looptijd van de overeenkomst dienen alle onderdelen die onderdeel uitmaken van de dienstverlening te voldoen aan de gestelde eisen. Dit betekent dat zowel het besturingssysteem als eventuele derde componenten actueel, ondersteund en beveiligd moeten blijven. Indien noodzakelijk wordt van de opdrachtnemer verwacht dat gedurende de contractperiode upgrades of updates worden uitgevoerd om aan deze eis te blijven voldoen.
65	Programma van Eisen - Bijlage 3 - Eis ICT.23.001	Welke toekomstige ontwikkelingen moeten in de vaste SaaS-prijs zitten?	De vraag is onvoldoende specifiek om te kunnen beantwoorden. Wij verzoeken u nader toe te lichten op welke toekomstige ontwikkelingen u doelt.
66	Bijlage 4	a. Welke ruimte is per locatie rondom de huidige kast beschikbaar voor plaatsing, bediening en onderhoud van de nieuwe kast? b. Welke ruimte is beschikbaar om de bestaande kast tijdens de migratie tijdelijk naast de nieuwe kast te plaatsen?	Op de locaties waar de sleutelkasten zijn geplaatst, zoals gangen en hallen, is voldoende ruimte aanwezig om gedurende de migratie de bestaande en nieuwe kast tijdelijk naast elkaar op te stellen. Dit kan plaatsvinden in de directe nabijheid van de montagelocatie.
67	Algemene vragen over verankering	a. Waar kan per locatie veilig in de vloer en wand worden geboord? b. Welke vloerverwarming, leidingen, kabels, medische gassen of andere installaties bevinden zich in de vloer en wand waarmee bij verankering rekening moet worden gehouden? c. Welke technische tekeningen of veilige boorzones zijn hiervoor beschikbaar?	De nieuwe kasten dienen zoveel mogelijk op de locatie van de bestaande kasten te worden geplaatst. De huidige kasten zijn reeds op deze locaties verankerd, waardoor redelijkerwijs mag worden aangenomen dat zich achter deze posities geen kritische installaties bevinden. Voor zover bekend bevinden leidingen, bekabeling en overige kritische infrastructuur zich hoofdzakelijk boven plafonds of onder technische vloeren.
68	Punten 2.4 en 2.5	In hoeverre voldoet een elektronische sleutelkast met een constructieve kwaliteit en een sluitmechanisme van minimaal hetzelfde niveau als de huidige Traka kasten aan eisen 2.4 en 2.5?	De aangeboden oplossing dient minimaal te voldoen aan een inbraakwerendheid die vergelijkbaar is met EN 14450 klasse S1. Een hoger beveiligingsniveau, zoals EN 14450 klasse S2, wordt positief gewaardeerd maar is niet verplicht. Ook oplossingen zonder formele EN 14450-certificering worden geaccepteerd, mits objectief kan worden aangetoond dat zij een gelijkwaardig of hoger beveiligingsniveau bieden.
69	Eisen 6.1 en 6.2	a. Hoe werkt bij de huidige Traka kasten de mechanische noodvrijgave van de kastdeur? b. Hoe werkt de mechanische noodvrijgave van een individuele sleutelpositie? c. Welke deur en welke sleutelposities worden daarbij daadwerkelijk vrijgegeven? d. Kunt u dit tijdens de schouw demonstreren?	De mechanische noodvrijgave van de kastdeur vindt plaats met een fysieke sleutel. De mechanische noodvrijgave van individuele sleutelposities wordt uitgevoerd met een sleutel in combinatie met een schakelaar in de kast. Hierbij worden alle sleutelposities vrijgegeven. Een demonstratie tijdens de schouw is niet meer mogelijk, aangezien de schouw reeds heeft plaatsgevonden.

70	Programma van Eisen - Bijlage 3 - Eis 7.2	a. Wat wordt er bedoelt met "Aan de zijde van VUmc zijn deze posten niet aanwezig." b. Hoe worden de intercom, spreek, luister en videovoorzieningen momenteel gebruikt? c. Welke technische koppeling bestaat met de huidige Traka kasten? d. Kunt u de werking tijdens de schouw demonstreren? e. Welke schematische weergave is beschikbaar van de koppeling tussen de sleutelkast, de spreek, luister en videovoorzieningen en de overige betrokken systemen? f. Welke partij verzorgt momenteel het beheer, onderhoud en de ondersteuning van de intercom en videovoorzieningen? g. Hoe worden na het overzetten de verantwoordelijkheden verdeeld voor configuratie en ingebruikname? h. Hoe worden de verantwoordelijkheden verdeeld voor technische ondersteuning en storingsafhandeling?	Op de locatie VUmc zijn geen intercomvoorzieningen aanwezig. De aanwezige intercoms op locatie AMC worden uitsluitend gebruikt als communicatiemiddel met de meldkamer van de beveiliging in geval van storingen of incidenten. De intercoms hebben geen technische koppeling met de sleutelkasten. De intercomvoorzieningen vallen onder de verantwoordelijkheid van de opdrachtgever. Indien noodzakelijk verzorgt de opdrachtnemer het herplaatsen van de intercoms, onder verantwoordelijkheid van de opdrachtgever. Een demonstratie tijdens de schouw is niet meer van toepassing, aangezien deze reeds heeft plaatsgevonden.
71	Programma van Eisen - Bijlage 3 - Eis 7.4	a. Hoe zijn de huidige Traka kasten per locatie gekoppeld aan de alarm en meldkameromgeving? b. Welke overdrachtspunten en bestaande bekabeling worden daarbij gebruikt? c. Welke gebeurtenissen worden momenteel als alarm doorgemeld? d. Welke schematische weergave is beschikbaar van deze koppeling?	Op locatie VUmc verlopen alarmmeldingen momenteel uitsluitend via de applicatie van het sleutelbeheersysteem. Er is geen koppeling met het meldkamersysteem Winguard. Op locatie AMC is de applicatie van het sleutelbeheersysteem gekoppeld aan de INTER-applicatie, die als meldkamersysteem wordt gebruikt. Momenteel worden alle alarmmeldingen die door de sleutelkastapplicatie worden ondersteund, weergegeven via deze systemen. Op beide locaties wordt hiervoor gebruikgemaakt van de gebruikersinterface van de sleutelkastapplicatie.
72	Programma van Eisen - Bijlage 3 - Eis 8.4	a. Welke locatie is beoogd voor de proof of concept? b. Welke aansluitingen en voorzieningen zijn op deze locatie beschikbaar? c. Hoe kan op deze locatie de tijdelijke situatie met de bestaande en nieuwe kast worden gerealiseerd?	De definitieve locatie voor de Proof of Concept wordt nog vastgesteld. Op basis van de beschikbare ruimte is locatie V01 (energiecentrale) hiervoor de meest voor de hand liggende locatie. De opdrachtgever zorgt voor de benodigde tijdelijke voorzieningen op deze locatie.
73	Programma van Eisen - Bijlage 3 - Eis 11.2	a. Hoe wordt Sensormatic momenteel gebruikt in combinatie met de sleutelbossen en de huidige Traka kasten? b. Kunt u tijdens de schouw bij een huidige Traka kast het volledige proces demonstreren, vanaf uitname tot en met terugplaatsing?	De werking van Sensormatic in combinatie met de huidige Traka-kasten is tijdens de schouw gedemonstreerd.
74	Algemene vragen en plan van aanpak	a. Hoe moet de vervanging per locatie praktisch plaatsvinden wanneer de nieuwe kast op dezelfde positie als de bestaande kast komt? b. Waar kan de bestaande kast tijdens de migratie tijdelijk worden geplaatst? c. Welke ruimte is beschikbaar om beide kasten tijdelijk operationeel te houden? d. In hoeverre is de bestaande bekabeling lang genoeg om de tijdelijk verplaatste kast operationeel te houden? e. Welke voeding, data en alarmaansluitingen zijn op de tijdelijke positie beschikbaar? f. Is er een tijdelijke verankering nodig voor de oude kast? g. Welke partij verzorgt het loskoppelen, tijdelijk verplaatsen, aansluiten en verankeren van de bestaande kast? h. Welke partij verzorgt de definitieve verwijdering van de bestaande kast?	Van de opdrachtnemer wordt verwacht dat de praktische aanpak voor de vervanging van de kasten wordt uitgewerkt in het Plan van Aanpak, conform de uitgangspunten van paragraaf 8.5 van het Programma van Eisen. Ter ondersteuning van de uitvoering zal een beveiliger vanuit de opdrachtgever beschikbaar worden gesteld.
75	Programma van Eisen - Bijlage 3 - Eis 7.2	a. Hoe blijven de spreek, luister en videovoorzieningen tijdens de vervangingswerkzaamheden functioneren? b. Hoe wordt de werking geborgd wanneer tijdelijk twee kasten operationeel zijn en slechts één intercomvoorziening beschikbaar is? c. Op welke kast wordt de intercomvoorziening tijdens de overgang aangesloten? d. Op welk moment wordt de intercomvoorziening van de bestaande naar de nieuwe kast overgezet?	De spreek-, luister- en videovoorzieningen functioneren onafhankelijk van het sleutelbeheersysteem en beschikken over een eigen netwerkaansluiting. Hierdoor kunnen deze voorzieningen zelfstandig blijven functioneren tijdens de vervangingswerkzaamheden. Indien tijdens de migratie tijdelijk handmatige sleuteluitgifte plaatsvindt, is de intercomvoorziening hiervoor niet noodzakelijk. Daarnaast is een beveiliger beschikbaar om, indien nodig, handmatig sleutels uit te geven. De wijze waarop de intercomvoorziening gedurende de overgangsperiode wordt ingezet, behoort tot de verantwoordelijkheid van de opdrachtnemer. Het ligt daarbij voor de hand om het overzetten van de intercom als laatste stap van de migratie uit te voeren.
76	Programma van Eisen - Bijlage 3 - Eis 7.2	Algemene vragen over transport en bereikbaarheid a. Hoe verloopt per locatie de transportroute vanaf de laad en losplaats tot de kastpositie? b. Welke actuele plattegronden zijn per locatie beschikbaar? c. Welke kastposities, beschikbare ruimte, aansluitpunten en transportroutes zijn daarop aangegeven? d. Welke beperkingen gelden voor doorgangsmaten en liftmaten? e. Welke maximale gewichten zijn toegestaan? f. Met welke drempels, trappen, scherpe bochten of andere fysieke beperkingen moet rekening worden gehouden?	Alle sleutelkasten zijn bereikbaar met een palletwagen of platte kar. Daarnaast zijn goederenliften beschikbaar met een capaciteit van ruim 2.000 kg, waardoor de opdrachtgever geen beperkingen verwacht ten aanzien van transport en plaatsing. De gangen zijn toegankelijk en vrij van drempels. Actuele plattegronden van de locaties kunnen beschikbaar worden gesteld. De exacte posities van de sleutelkasten zijn hierop niet weergegeven, maar kunnen afzonderlijk worden aangewezen.
77		Is het toegestaan om de bestaande samenstelling zoals deze nu is in de sleutelkasten te optimaliseren? Op sommige locatie's zijn twee losse sleutelkasten per één terminal gebruikt terwijl deze samengevoegd zouden kunnen worden binnen één sleutelkast. Echter neemt het formaat van de sleutelkast dan wel iets toe of worden de panelen binnen de sleutelkast compacter.	Optimalisatie van de huidige kastindeling is toegestaan, mits bouwkundige aanpassingen en herstelwerkzaamheden tot een minimum worden beperkt. Daarnaast dienen de bestaande sleutelbossen zonder ingrijpende aanpassingen aan de omgeving of de kastopstelling in de nieuwe oplossing te passen. Voor verdere toelichting wordt verwezen naar het antwoord op vraag 22.
78		Wat is de omvang van de twee sleutelkluizen die in de aankomende twee jaar geplaatst zullen worden? Deze moeten binnen de eerste aanbieding afgeprijsd worden, echter is het niet bekend wat de omvang van deze kasten betreft.	Voor deze vraag wordt verwezen naar het antwoord op vraag 21.
79		Moet de koppeling met de toekomstige PIAM oplossing ook al afgeprijsd worden binnen de aanbieding of hoeft binnen de eerste fase alleen de koppeling met de EAL & Nedap omgeving gerealiseerd te worden?	Voor deze vraag wordt verwezen naar het antwoord op vraag 20.
80		Ter verificatie: de 25% marge voor toe- en afname aan gebruikers, geldt dit alleen voor het aantal gebruikers binnen de software of wilt het Stichting Amsterdam UMC ook 25% extra marge aan sleutelposities binnen de sleutelkluizen hanteren?	Voor deze vraag wordt verwezen naar het antwoord op vraag 19.
81		Er staat bij hoofdstuk 7 Data exit strategie binnen Bijlage 3 Programma van Eisen de wens om de data op leesbaar en machine formaat te exporteren en daarna te importeren. Wordt hier alle data beschikbaar binnen de sleutelkast software mee bedoeld of alleen specifieke data?	Voor deze vraag wordt verwezen naar het antwoord op vraag 18.
82		Is het benodigd/verplicht dat sleutelkasten SKG of anders gecertificeerd zijn? Voor binnen sleutelkasten die alleen voor sleutels en keytags gehanteerd worden zien wij bij soortgelijke omgevingen een brandwerendheid of brandpreventie certificering niet terug als eis.	Voor deze vraag wordt verwezen naar het antwoord op vraag 14.

	Onderwerp	Algemene mededeling AUMC	Het AUMC heeft bij deze Nota een concept Verwerkersovereenkomst als Bijlage 11 van de Aanbestedingsleidraad gepubliceerd. Deze concept Verwerkersovereenkomst dient door de (voorlopig) gegunde Inschrijver ingevuld verder ingevuld, en tegelijktijdig met de Overeenkomst ondertekend.