



Bijlage 2: Concept Programma van eisen

Inhoudelijke eisen		
Normering:		
		De aanbieding moet vergezeld gaan van de volgende bijlagen: - Geldig ISO 9001 certificaat van de Inschrijver. - Geldig ISO 27001 of gelijkwaardig certificaat van de Inschrijver. - Inschrijver dient medewerking te verlenen voor de verplichte BIO compliance test die uitgevoerd wordt door RWS.
Software assurance:		
		Inschrijver voorziet RWS van een native app om sleutels via bluetooth tenminste 4.1 ble (bluetooth low energy) om te pentesten op security level.
		Het is vereist dat de inschrijver een ESCROW-overeenkomst afsluit met aanbestedende dienst die waarborgt dat de broncode en de benodigde toegangsrechten aan de aanbestedende dienst worden overgedragen in het geval van faillissement, surseance van betaling of een vijandige overname van de inschrijver. De nadere voorwaarden voor de kwalificatie van een "vijandige overname" zullen door de aanbestedende dienst op een later moment worden vastgesteld.
		De inschrijver dient te beschikken over een programma waarmee de applicatie en het onderliggende besturingssysteem continu "up to standard" worden gehouden op het gebied van cyberveiligheid en marktconformiteit. Tevens dient de inschrijver in staat te zijn ontwikkelingen binnen het veiligheidsdomein, marktveranderingen en functionele innovaties tijdig te volgen en waar nodig door te voeren. Daarnaast wordt van de inschrijver verwacht dat noodzakelijke aanpassingen voortvloeiend uit wet- en regelgeving en de geldende certificeringsvereisten tijdig en correct worden geïmplementeerd.
Systeemtechnische vereisten:		
		Het systeem dient te beschikken over een gescheiden test- en acceptatieomgeving die fysiek en logisch is gescheiden van de productieomgeving, maar qua configuratie, functionaliteit en inrichting volledig identiek is aan de productieomgeving. Deze omgeving moet functioneren als een volwaardige OTAP-omgeving.
		Het systeem dient zo ingericht te zijn dat data en applicatie gescheiden kunnen worden beheerd en opgeslagen.
		Er moet een centrale database zijn voor alle gebruikers en personen. - Aan elke persoon moeten verschillende telefoon- en mobiele telefoonnummers, een adres en een e-mailadres kunnen worden toegewezen.
		Het systeem moet over een updatemanager beschikken. Programma-updates van de fabrikant worden geleverd als handmatige upload of internetdownload. De sleutelmanagementserver van aanbestedende dienst moet deze updates voorbereiden voor installatie en deze tegelijkertijd op de achtergrond distribueren naar alle eventuele andere servers en werkstations. De update moet beperkt blijven tot het opnieuw opstarten van het programma zonder handmatig te herladen en interactie op servers en werkstations.
		Het systeem dient te beschikken over een functiemodule die voorziet in kalenderfunctionaliteit, inclusief de weergave en verwerking van feestdagen, roosters en planningen. Deze module moet geïntegreerd werken binnen de totale oplossing en



	de kalendergegevens consistent en actueel beschikbaar stellen voor alle relevante processen.
	Het Sleutelmanagementsysteem moet zelfstandig toezicht kunnen houden op zijn diensten en lopende programma's. Bij een storing moeten de betreffende componenten automatisch opnieuw worden opgestart. De beschikbaarheid en het gebruik van de hardware omgeving van het Sleutelmanagementsysteem (CPU, RAM, HDD, LAN etc.) en de systeeminterfaces moeten onafhankelijk worden bewaakt. Bij overschrijding van grenswaarden of bij het optreden van storingen moeten passende meldingen worden gegenereerd binnen de applicatie met de mogelijkheid om deze te exporteren naar het SMS systeem van aanbestedende dienst.
	Het Sleutelmanagementsysteem moet beschikken over multi-tenancy en datasegmentatie. Er moet worden gezorgd voor de mogelijkheid om het systeem te beheren; replicatie door middel van gebruikersautorisaties is niet toegestaan. Met behulp van datasegmentatie (het opdelen van de data in logische subsets) moet er bovendien voor worden gezorgd dat alleen de data van de toegewezen onderdelen fysiek beschikbaar zijn op en bij de beheer werkplekken, gebaseerd op de inlog van de gebruiker.
	Het systeem moet zo ingericht kunnen worden dat op centraal en lokaal niveau beheer kan worden uitgevoerd maar wel dusdanig dat er nooit overlap van cilinders en sleutels mogelijk is binnen het RWS-domein, dus geen dubbele unieke benaming van cilinders en/of sleutels.
	Het Sleutelmanagementsysteem moet beveiligd zijn tegen wijzigingen door onbevoegden. Er moet voor worden gezorgd dat, naast het beheerrecht, wijzigingen alleen kunnen worden doorgevoerd op werkplekken die uitdrukkelijk voor dit doel zijn bestemd. Deze functie moet worden gewaarborgd.
	Het Sleutelmanagementsysteem moet beschikken over een geïntegreerde webserver die alle functies van het Sleutelmanagementsysteem beschikbaar maakt voor web clients. De webserver moet direct de autorisaties van alle gebruikers van de Sleutelmanagementsysteem-server overnemen. Afzonderlijk rechtenbeheer op de webserver is niet toegestaan.
	Er moet op applicatieniveau een back-up van het Sleutelmanagementsysteem kunnen worden gemaakt door 2 extra hot stand-by redundantieservers. Er moet aan de volgende must-have-criteria worden voldaan: - Op de hot stand-by servers wordt het Sleutelmanagementsysteem gestart met een identieke configuratie/projectplanning en wordt een storing van de actieve server automatisch gedetecteerd op applicatieniveau. - De actieve server zorgt voor realtime gegevensvergelijking (inclusief alle logbestanden) met de redundantieservers op de achtergrond. - Bij een storing neemt de hot-stand-by server het over zonder hulp van scripts of handmatige interactie en voert een volledige statusvergelijking uit met de gekoppelde systemen. Het gevraagde aantal heeft betrekking op het aantal in bedrijf te stellen redundantieservers.
	Workflows dienen dusdanig geconfigureerd te kunnen worden dat deze op basis van omstandigheden zoals systeem statussen, additionele events etc. geautomatiseerd worden aangepast conform de dan geldende situatie
	Het Sleutelmanagementsysteem dient integratie en of koppelingen te kunnen maken met externe systemen waarbij het Sleutelmanagementsysteem informatie verstuurt en ontvangt van en naar subsystemen.
	Het systeem moet met extra bedieningsstations en modules kunnen worden uitgebreid. De Sleutelmanagementsysteem-server moet in een virtuele omgeving (VM) worden



	geïmplementeerd en als Windows-service kunnen worden uitgevoerd. Architectuur: 64-bit Besturingssysteem: Windows Server 2019 / 2022 Prestatiekenmerken (must-have criteria): - Rolgebaseerd gebruikersbeheer voor een willekeurig aantal gebruikers. - Met wachtwoord beveiligde toegang voor alle beheerders. - Alle wijzigingen aan het systeem (bijvoorbeeld nieuwe sleutels, cilinders, locaties, enz.) moeten op elk moment kunnen worden uitgevoerd zonder de productieve werking te beïnvloeden.
	Het intelligente sleutelsysteem dient onderdelen te bevatten die OSS4GOV compatibel zijn.
	Voor toekomstige uitbreidingen of maatwerkfunctionaliteit in de software dient de inschrijver op verzoek van de aanbestedende dienst een transparant gespecificeerde offerte uit te brengen, gebaseerd op marktconforme tarieven en prijsstellingen. De aanbestedende dienst behoudt zich het recht voor om de marktconformiteit van de offerte te toetsen, dan wel de opdracht niet te verstrekken indien deze niet marktconform wordt geacht.
Integriteit data:	
	Het Sleutelmanagementsysteem moet alle processen (berichten, operatoracties, interfacecommunicatie) auditproof archiveren. - Toegang tot het archief moet mogelijk zijn via variabele filters waarmee Opdrachtgever zelf selecties kan maken op de database. - Berichten niet ouder dan 5 jaar moeten op ieder moment uit het archief kunnen worden weergegeven met alle informatie, dus zoals op het moment dat het bericht werd verwerkt, beschermd tegen wijzigingen. - Toegang tot de logs moet mogelijk zijn via variabele filters.
Back-up:	
	Alle systeemgegevens, inclusief het besturingssysteem, moeten cyclisch op een externe schijf in het netwerk van aanbestedende dienst worden opgeslagen. De hiervoor benodigde back-upsoftware is onderdeel van de levering.
	Installatie van de software op de server / hot stand-by server / interface server en het instellen van de automatische back-upfunctie voor alle server componenten - via een dagelijkse, week en maand back-up.
	Het systeem dient de mogelijkheid te bieden om data extern op te slaan via een cold-storage-methode. Deze opslagmethode moet geschikt zijn voor het langdurig en veilig bewaren van gegevens die niet frequent hoeven te worden geraadpleegd, met behoud van integriteit en toegankelijkheid indien nodig.
Mobiele bereikbaarheid:	
	Het Sleutelmanagementsysteem moet toegang verlenen via een mobiele app (Android en iOS). - De mobiele client biedt overzichtelijke en compacte toegang tot de statussen en berichten van het Sleutelmanagementsysteem. - Berichtverwerkings- en controlefuncties moeten beschikbaar zijn. - Het moet mogelijk zijn om sleutels tijdsgebonden toegang te geven tot cilinders.
Hardware technische vereisten:	
	De cilinders en sleutels moeten voldoen aan de betreffende NEN normen, minstens SKG ** hebben, maar als risicoanalyse het vereist dan moet SKG *** ook mogelijk zijn.
	De cilinders en sleutels moeten voldoende beschermen tegen weerelementen zoals wind, vorst, regen, hitte, zout water, -20 tot +50 zoals benoemd in EN 15684.



	- De cilinders en sleutels moeten voldoende beschermen tegen weerslementen zoals wind, vorst, regen, hitte, zout water, -20 tot +50 zoals benoemd in EN 15684. - o Klasse 3 (binnenruimten en overdekte/halfopen technische ruimten) Toepassingsgebied: schakelruimten, MCC-ruimten, kantoor- en kantinedelen en overige inpandige ruimten van bruggen, sluizen, gemalen en bedieningsgebouwen, waar geen directe blootstelling aan neerslag, zoutnevel of stuifzand plaatsvindt. Klasse 4 (volledig buitenopgestelde en agressieve omgevingen) Toepassingsgebied: toegangsdeuren, hekwerkpoorten, kabelkasten, pompputten, sluis- en stuwbedieningskasten, gemaalafsluiters en overige buiten opgestelde op terreinen waar reiniging met hogedrukstralen plaatsvindt, en op locaties met zoute, brakke of zandige condities
	Inbraakwerendheid conform NEN 5089 (manuele beproeving) - Het aan te bieden elektromechanische sluitsysteem voldoet aanvullend op NEN-EN 14846 en NEN-EN 15684 aan de eisen voor manuele beproeving zoals vastgelegd in NEN 5089 (Hang- en sluitwerk — Inbraakwerendheid — Eisen, classificatie en beproevingsmethoden). - De opdrachtnemer toont aan dat het aangeboden product is opgenomen op de actuele productlijst van SKG-IKOB onder beoordelingsrichtlijn BRL 3104 en de bijbehorende AE 3104 (Aanvullende Eisen elektromechanisch hang- en sluitwerk). Het SKG-certificaat wordt bij de inschrijving overgelegd en is op het moment van gunning geldig. - De manuele beproeving heeft betrekking op het complete sluitsysteem in samenhang — cilinder, slot, sluitplaat, koppelvlakken en eventuele beveiligingsrozetten/-beslag — zodat de gemeten weerstand de feitelijke situatie aan de deur representeert. Losse componentcertificaten zonder systeemcertificering worden niet geaccepteerd. - De combinatie van componenten (cilinder-slot-beslag) komt voor op de SKG-lijst van goedgekeurde combinaties dan wel beschikt over een aanvullende systeemverklaring van SKG-IKOB. Bij ontbreken hiervan wordt een aanvullende projectspecifieke beproeving door een geaccrediteerd onderzoeksinstituut uitgevoerd, op kosten van de opdrachtnemer, vóór oplevering. - De opdrachtnemer levert bij oplevering een bewijslastdossier aan met daarin: het SKG-certificaat, de testrapporten van NEN 5089-beproeving, de EN 14846- en EN 15684-classificatiebladen, en een verklaring van conformiteit waarin de samenhang tussen de componenten expliciet is bevestigd. Toelichting voor inschrijvers: - NEN 5089 is in Nederland gehandhaafd als nationale aanvulling op de Europese productnormen, omdat deze laatste geen manuele aanvalsbeproeving kennen. Voor objecten die vallen onder de Wet weerbaarheid kritieke entiteiten (Wwke) is deze aanvullende beproeving van wezenlijk belang om aantoonbaar te voldoen aan de zorgplicht voor fysieke weerbaarheid van kritieke entiteiten.
Oplevering:	
	Inschrijver dient, op basis van de vastgestelde servicebeschrijving en in afstemming met de aanbestedende dienst, een volledige en eenduidige specificatie op te stellen. Dit vereist regelmatige en actieve deelname aan de realisatievergaderingen. De specificatie dient ten minste de volgende onderdelen te omvatten:



		• Definitie van de gebruikersprofielen, inclusief lay-outs van de gebruikersinterfaces • Definitie van de categorie en prioriteit van de berichten voor elk vakgebied en berichttype • Definitie van de gebeurteniscontrolematrix (actieplannen, visualisatie voor elk type transactie en bericht) • Definitie van de actiematrix voor elk type transactie en bericht • Definitie van de kennisgevingsmatrix voor elk type transactie en bericht
		Inschrijver verzorgt gebruikerstrainingen op locatie over het Sleutelmanagementsysteem. De inhoud van de training omvat: Presentatie - programma-interface, concepten, interfaces, bediening - aan-/afmelden - functies - berichtverwerking - bediening, bediening, weergave - afdrukken - foutafhandeling.
		Inschrijver verzorgt training voor verantwoordelijke beheerders.
Start proces:		
		Acceptatie vindt plaats via een succesvol afgeronde site acceptance test, om dit uit te voeren zal het programma management, in samenspraak met de Inschrijver een testprotocol opzetten welke vervolgens per onderdeel beoordeeld wordt. Indien bij oplevering de gewenste testresultaten niet behaald worden krijgt de Inschrijver de mogelijkheid om dit binnen 6 weken te herstellen en om vervolgens een hertest te doen. Het testprotocol zal alle delen en diensten die uitgevraagd en geleverd zijn bevatten. Succesvol betekent dat ieder item de verwachte en benoemde waarde conform testplan heeft behaald.
Beheer:		
		Het systeem moet de gebruiker in staat stellen om met één en dezelfde sleutel alle RWS-assets te betreden waar dit sleutelsysteem toegepast is. Met andere woorden: er zijn niet langer grote sleutelbossen nodig maar dus slechts één sleutel waarvan de autorisaties in te regelen zijn zodat alleen wie toestemming heeft ook daadwerkelijk naar binnen kan.
		Handeling om sleutel te activeren op een cilinder moet binnen 1 minuut uitgevoerd kunnen worden.
		Geautoriseerde gebruikers moeten de mogelijkheid hebben om via de app hun eigen sleutel te activeren voor de aan hun toegewezen cilinders.
		Een instelbare waarde op systeemniveau is de maximale duur van een geactiveerde sleutel, dit is een systeem instelling op admin niveau.
		Een instelbare waarde op systeemniveau is de maximale duur van een geactiveerde sleutel, op basis van risico kwalificatie locatie, dit is een systeem instelling op admin niveau.
		Gebruiker krijgt in de app waarschuwing dat zijn batterij van de sleutel lager is dan X %.