Appendix 1 - Programma van Eisen

Bij de Europese aanbesteding volgens de openbare procedure

Bancaire dienstverlening

Gemeente Eindhoven

Uitgave
Gemeente Eindhoven

Datum
Mei 2025

EINDHOVEN

Inhoud

EINDHOVEN

1. Algemene Eisen

1. Inschrijver voldoet aan alle in het Beschrijvend document en daarbij behorende Appendices genoemde voorwaarden en eisen die aan de Opdracht zijn gesteld.
2. Tijdens de uitvoering van de Raamovereenkomst hanteert Opdrachtnemer als voertaal het Nederlands in woord en geschrift.
3. De inschrijver is op de hoogte van de bepalingen in het treasurystatuut van de gemeente Eindhoven, te raadplegen via de website van de gemeente Eindhoven, en houdt zowel in de offerteronde als in de contacten nadien, rekening met de bepalingen en voorwaarden die in het treasurystatuut zijn opgenomen.
4. Inschrijver voldoet aan de vereisten uit de wet Financiering Decentrale overheden (Fido) en de hieruit voortvloeiende ministeriële regelingen en algemene maatregelen van bestuur. Een wijziging in wet- en regelgeving kan leiden tot noodzakelijke aanpassingen in de overeenkomst.

2. Eisen t.a.v. Electronic Banking / Internetbankieren

5. Inschrijver biedt een volledig geautomatiseerde en gebruiksvriendelijke toepassing aan voor online banking. De beschikbaarheid, betrouwbaarheid en de veiligheid van de applicatie is maximaal gegarandeerd en voldoet aan de hoogste eisen.
6. Electronic Banking toepassing is webbased en benaderbaar vanaf meerdere locaties via verschillende devices.
7. Electronic Banking toepassing dient door meerdere gebruikers tegelijk benaderd en gemuteerd te kunnen worden.
8. Het moet voor gebruikers met administrator-rechten mogelijk zijn om in het pakket functieprofielen, tekenbevoegdheden en tekenstructuren toe te kennen met daarbij de mogelijkheid om per rekening combinaties van bevoegdheden en limieten voor gebruikers vast te leggen.
9. Voor het fiatteren van opdrachten zijn twee handtekeningen vereist; hierbij moet onderscheid gemaakt kunnen worden in autorisatieniveau tussen een eerste en tweede handtekening.
10. Electronic Banking toepassing is in staat om elke dag (7 dagen per week) geautomatiseerd dagafschriften in bestandsformaat CAMT.053 (vereist voor ons financieel pakket ERPx) aan te bieden via FTP op een netwerkschijf en via API.
11. Electronic Banking toepassing is in staat betaalbatches en incassobestanden met een omvang van minimaal 75.000 posten te verwerken. Batches worden aangemaakt in ERPx en Gouw-IT. Ingelezen en/of verwerkte betaal- en of incassobestanden in de bankapplicatie moeten in Pdf-formaat kunnen worden gedownload met weergave van hashtotal, totaalbedrag, batchnummer en autorisaties.
12. Electronic Banking toepassing biedt de mogelijkheid om aangekondigde SEPA incasseringen ten laste van gemeentelijke bankrekeningen in te zien, evenals af te keuren, en reeds geïncasseerde bedragen eenvoudig terug te laten boeken.
13. Electronic banking geeft dagelijks, zowel per rekening als geconsolideerd, het saldo weer. Van het geconsolideerd saldo zowel het boeksaldo als kladsaldo. Intradag informatie moet eenvoudig opvraagbaar en actueel beschikbaar zijn in het systeem.
14. Het is mogelijk om betalingen met een uitvoerdatum in de toekomst tot minimaal 3 maanden voor deze uitvoerdatum op te kunnen voeren in de Electronic Banking toepassing.
15. Electronic Banking toepassing dient te beschikken over uitgebreide zoek- en sorteermogelijkheden op bedrag, rekeningnummer, naam, datum, omschrijving en autorisatie informatie. Deze informatie dient minimaal 12 maanden beschikbaar te zijn. Tevens dient deze informatie eenvoudig geprint en geëxporteerd te kunnen worden naar Excel- en Pdf-formaat.
16. Inschrijver biedt de mogelijkheid om PIN-terminals of betaalautomaten te koppelen aan bankrekeningen en de ontvangsten hiervan te verwerken voor betaalmethoden onder andere V PAY, MAESTRO en Creditcards.

Pinbetalingen moeten rechtstreeks bij de huisbank op de rekening worden bijgeschreven. De individuele mutaties moeten per automaat opgevraagd kunnen worden bij de huisbankier.

17. Electronic Banking toepassing is in staat de ontvangst van iDeal-betalingen te verwerken.
18. Electronic Banking toepassing biedt de mogelijkheid tot uitvoering van verdichte salarisbetalingen.
19. Inschrijver biedt de mogelijkheid om bankrekeningnummers met een Nederlandse IBAN te leveren (beginnend met NL).

3. Eisen t.a.v. Service en Ondersteuning

20. Inschrijver garandeert een beschikbaarheid van uw bancair systeem op werkdagen tussen 7.30 en minimaal 18.00 uur.
21. Inschrijver beschikt over een Nederlandstalige helpdesk die op werkdagen tussen 8.30 en 17.00 uur bereikbaar is.
22. Uw accountorganisatie dient binnen 1 uur actie te ondernemen bij calamiteiten. Hieronder wordt verstaan gebeurtenissen waardoor de normale bedrijfsvoering verstoord is of kan worden.
23. In geval van storingen van de Electronic Banking toepassing moet binnen 24 uur een uitwijkmogelijkheid beschikbaar zijn om betalingen te kunnen verrichten en informatie te kunnen opvragen.
24. Communicatie tussen Opdrachtnemer en Opdrachtgever vindt op de volgende niveaus plaats:
    • Operationeel;
    • Tactisch;
    • Strategisch.
    De vaste overleggen worden door de contractmanager van Opdrachtgever gepland. Twee (2) dagen voor het geplande operationeel overleg wordt de agenda aan betrokkenen toegestuurd. De agenda voor het strategisch en tactisch overleg wordt uiterlijk één (1) week voor het overleg door aan betrokkenen toegestuurd. De Opdrachtgever is verantwoordelijk voor de verslaglegging en het (digitaal) aanleveren hiervan aan alle deelnemers van het overleg.

4. Eisen t.a.v. Security

25. Informatiebeveiliging wordt integraal meegenomen bij het ontwerp en de inrichting van applicatie en infrastructuur. Dit dient te worden aangetoond door middel van het certificaat ISO27001 of vergelijkbaar.
26. Opdrachtnemer toont op verzoek van Opdrachtgever aan hoe zij de Responsible Disclosure procedure heeft ingericht. Zie Coordinated Vulnerability Disclosure (CVD) | Rijkswebsites | CommunicatieRijk.
27. Opdrachtnemer draagt zorg voor een erkende en recente TPM-verklaring, afgegeven door een geregistreerde EDP/ Norea auditor.
28. De wijze waarop inschrijver afnemer in staat stelt om te voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en aan de Baseline Informatiebeveiliging Overheid (BIO) is als volgt: Indien inschrijver in aanmerking komt voor gunning dient een kopie van het geldige certificaat/de geldige certificaten en verklaringen te uploaden. Bij het ontbreken van een geldig certificaat dient inschrijver een alternatief te overleggen dat voldoet aan bovenstaande criteria.
29. Inschrijver laat jaarlijks een PEN-test uitvoeren door een onafhankelijke gecertificeerde partij en geeft inzage in de uitkomsten van de PEN-Testen, op kosten van de Inschrijver/Opdrachtnemer. Leverancier werkt mee aan audits en pentesten op verzoek van de gemeente Eindhoven (right to audit). De leverancier laat, bij hosting, periodiek (minimaal 1x per jaar en/of op verzoek) een White box pen-test uitvoeren, waarbij een kwetsbaarheids-scan onderdeel vormt van de pen-test, op zijn systemen binnen de scope van de dienstverlening. De resultaten van deze pen-test, de opvolging van de testresultaten en de oplossingsmogelijkheden conform het risicoprofiel worden gerapporteerd aan de gemeente Eindhoven. Daarbij is vereist dat alle high-risk bevindingen binnen een nader overeen te komen tijd worden opgelost.
30. Sessies dienen na een bepaalde tijd te verlopen afhankelijk van de kriticiteit van de applicatie.
31. Software libraries mogen niet EOL (End-of-life) zijn. Update mag N-1 zijn.
32. Security scorecard >80%
33. Network>70%, DNS>70%, Patching >70%.

34. Datacenterklasse is Tier 1 bij BBN1, Tier 2 bij BBN2 en Tier 3 bij BBN2+.
35. Inschrijver dient een oplossing te hebben geïmplementeerd tegen DDOS aanvallen.
36. Inschrijver beschikt over een exit-strategie.
37. Medewerkers en externen die de aanbieder ten behoeve van Opdrachtgever inzet dienen te beschikken over een VOG en een geheimhoudingsverklaring te ondertekenen, conform artikel 4.4.3 in het Beschrijvend Document.
38. Van iedere applicatie dient door Opdrachtnemer een autorisatie-matrix te worden opgesteld.

5. Eisen t.a.v. Technisch Beheer

39. Indien (Seamless) Single Sign On niet mogelijk is verloopt authenticatie via onderstaande protocollen in volgorde van voorkeur:
    - Strong Customer Authentication (SCA) conform de PSD2-richtlijn voor Financiële dienstverlening
    - DigiD
    - E-herkenning
    - EiDAS
    - Username/wachtwoord o.b.v. aangewezen wachtwoordbeleid i.c.m. Multifactor authenticatie (Passkey, FIDO2, Certificaat, Biometrisch, Authenticator app, (programmable) Hard Tokens en Email protocollen zijn toegestaan. SMS en telefonische Multifactor authenticatie is niet toegestaan).
40. Alle protocollen die worden gebruikt in de ICT Prestatie en staan in de verplichte of aanbevolen standaarden van Forum Standaardisatie voldoen aan de vereiste versie of hoger. Verder blijft de ICT Prestatie, indien van toepassing, voldoen aan de meest actuele NCSC richtlijnen voor wat betreft de ICT-beveiligingsrichtlijnen voor webapplicaties, TLS, Mobile apps en HTTPS.
    https://www.ncsc.nl/
    https://www.forumstandaardisatie.nl/open-standaarden/verplicht
    https://www.forumstandaardisatie.nl/open-standaarden/aanbevolen
41. Encryptie & hashing algoritmes voldoen aan de FIPS standaard N-1 (meest recente definitieve versie of 1 versie lager). Zie https://csrc.nist.gov/publications/fips
    De SSL Cipher Suites volgorde is zo ingesteld dat deze als eerst gebruik maakt van het sterkste Cipher en zo aflopend. Hierbij gebruikt de Leverancier enkel ciphers met de status goed en/of voldoende van het NCSC (Amazon Cloudfront en Azure Frontdoor voldoen hier standaard aan).
42. Data wordt versleuteld opgeslagen.
43. De ICT Prestatie moet voorzien zijn van strikte input- en output-validatiemechanismen. Voor de input houdt dit in dat alle ontvangen gegevens, of deze nu van gebruikers, andere systemen of bestanden afkomstig zijn, gecontroleerd en gevalideerd worden op veiligheid en correctheid voordat ze worden verwerkt. Dit is essentieel om beveiligingsrisico's zoals SQL-injectie, cross-site scripting en andere potentiële aanvallen te voorkomen. Wat betreft de output, moeten alle gegevens die naar externe bestemmingen worden verzonden, zorgvuldig worden gecontroleerd en gevalideerd om te waarborgen dat er geen gevoelige informatie wordt gelekt en dat de gegevens correct worden weergegeven. De implementatie en werking van deze validatiemechanismen dienen in lijn te zijn met de richtlijnen zoals beschreven in NORA online met betrekking tot input-/output-validatie.
    Zie https://www.noraonline.nl/
44. Logging: Er wordt er een audit trail gelogd van alle transacties en wijzigingen waarbij de logging minimaal het volgende bevat (indien van toepassing):
    • Een tot een natuurlijke persoon herleidbare gebruikersnaam of ID;
    • De gebeurtenis;
    • Waar mogelijk de identiteit van het werkstation;
    • Host naam;
    • Naam van de toepassing;
    • IP-adres(sen);
    • Het object waarop de handeling werd uitgevoerd;
    • Het resultaat van de handeling;

• De datum en het tijdstip van de gebeurtenis.
Standaard wordt logging minimaal 6 maanden bewaard en bij verwerking van bijzondere persoonsgegevens (AVG) minimaal 12 maanden, de maximale bewaarperiode van de logging (zonder beveiligingsincident) is 24 maanden. Bij het voorkomen van een beveiligingsincident wordt de logging omtrent het incident 36 maanden bewaard.

45. Toegankelijkheid: De ICT Prestatie gaat om met Diakrieten en met zowel IPv4 als IPv6.
46. Web-applicaties: Indien er geen Continuous access evaluation (CAE) plaatsvindt dan zal de session time-out (Idle, Absolute, Renewal) ingesteld moeten worden voor het webbased gedeelte van de Totale ICT prestatie en is deze zo ingesteld dat de maximale tijd niet wordt overschreden.
Time-out voor inactiviteit (Idle):
• Max 1 uur of na handmatig beëindigen van de sessie
Absolute time-out:
• Max 4 uur of na handmatig beëindigen van de sessie
Verlenging Time-out (Renewal):
• Maximaal ieder uur midden in de gebruikerssessie, en onafhankelijk van de sessieactiviteit en dus van de time-out voor inactiviteit, dient er automatisch een nieuw sessie ID te worden gegenereerd welke, met een veiligheidsinterval van max 10 minuten, automatisch overgang verzorgt van het oude naar het nieuwe sessie ID en hiermee het voorgaande sessie ID ongeldig maakt.

6. Eisen t.a.v. Facturatie en Betaling

47. Facturen voldoen aan de factuureisen, conform Appendix 7 “Instructie Factuurvereisten Gemeente”.

7. Eisen t.a.v. Condities rekening courant

48. De debet- en creditrentevergoedingen zijn gebaseerd op de 1 maands -Euribor