

Non-Functionals

Projectnummer: I.000930

Status: Definitief



Boek 6

Non-Functionals

Projectnummer: I.000930

Status: Definitief

© Copyright 2016, Havenbedrijf Rotterdam N.V.

Niets uit deze uitgave mag worden verveelvoudigd en / of openbaar gemaakt door middel van druk, fotokopie, microfilm of op welke andere wijze dan ook zonder voorafgaande schriftelijke toestemming van Havenbedrijf Rotterdam N.V.

Non-Functionals

Projectnummer: I.000930

Status: Definitief

Inhoudsopgave

1	Inleiding	4
2	Prestaties	5
3	Bruikbaarheid	6
4	Beheersbaarheid	7
5	Beveiligbaarheid algemeen	8
6	Beveiligbaarheid IoT	11
7	Onderhoudbaarheid	12

1 Inleiding

Dit document beschrijft de non-functionele requirements die op moment van delen gespecificeerd zijn. Het dient als leidraad en richtlijn om tijdens de dialoogfase op te kunnen beoordelen. De requirements hebben betrekking op de uiteindelijke oplossing en zijn niet geprioriteerd.

Non-Functionals

Projectnummer: I.000930

Status: Definitief

2 Prestaties

2.1	Gegevensverwerking mag geen negatieve invloed hebben op andere functionele delen van de oplossing. Bijvoorbeeld het draaien van een rapportage, backup en daarnaast gebruik.
2.2	De sensordata moet real-time vanaf het ontvangstmoment binnen de applicatie klaar zijn voor verdere verwerking.
2.3	De sensordata moet real-time vanaf het verstuurmoment van de sensor beschikbaar zijn voor eindgebruikers.
2.4	Schermwisselingen binnen de applicatie mogen maximaal 2 seconden duren, van klik tot volledig laden van nieuw scherm. Uitzondering bij zware rapportages en/of berekeningen.
2.5	De oplossing is ongeacht werklocatie (bijvoorbeeld thuis of op kantoor) en/of device (HbR laptop, Citrix, mobile) in staat aan de performance eisen te voldoen.
2.6	Wanneer de werklast op de oplossing toeneemt mag dit niet van invloed zijn op de dataverwerking en de prestaties die eindgebruikers ervaren.
2.7	De oplossing is geschikt om op grote schaal (>1000 sensoren) metingen in te winnen.
2.8	De oplossing is geschikt om hoog frequente (> 1 meting/seconde) metingen te verwerken.
2.9	De oplossing is geschikt om minimaal 50 gelijktijdige gebruikers van de data (eindgebruikers en interfaces) aan te kunnen.

Non-Functionals

Projectnummer: I.000930

Status: Definitief

3 Bruikbaarheid

3.1	De oplossing werkt conform prestatie-eisen op de standaard HbR werkplek en is compatibel met Internet Explorer 11.
3.2	De oplossing moet zodanig zijn (eenvoudig, logische werkvolgorde) dat een uitgebreide opleiding NIET nodig is. Denk aan herkenbare standaarden afkomstig uit de consumentenelektronica en -software.
3.3	De oplossing moet gebruikers ondersteunen bij hun werkzaamheden - met een minimum aan handelingen - door een duidelijke structuur van de oplossing - intuïtief bruikbaar
3.4	De oplossing moet het gebruik van persoonlijke systeeminstellingen ondersteunen op het gebied van lettertype, lettergrootte, schermindeling, schermgrootte en begin- / hoofdscherm.
3.5	De functioneel beheerder van de oplossing moet de systeeminstellingen voor groepen gebruikers in kunnen stellen.
3.6	Er moet een handleiding van de standaard functionaliteit aanwezig zijn in de Nederlandse taal.
3.7	Gebruikers mogen niet in staat zijn om de resultaten of data van andere gebruikers te beïnvloeden binnen de oplossing.
3.8	De oplossing geeft duidelijke feedback voor applicatiehandelingen zoals het laden van nieuwe schermen, ophalen van data, begrijpbare foutmeldingen.

4 Beheersbaarheid

4.1	De oplossing wordt gezien als missie-kritisch met als belangrijke eigenschap dat gebruikers 24 uur per dag, 7 dagen per week vertrouwen op beschikbaarheid en betrouwbaarheid van data ter ondersteuning van operationele processen.
4.2	De leverancier heeft een ingerichte (skilled) servicedesk met ticketregistratiesysteem die binnen het servicewindow telefonisch en elektronisch bereikbaar is, deze servicedesk communiceert via de HBR servicedesk. Servicedesk van de leverancier is conform ITIL proces ingericht met onder andere incident-, change-, problem- en configuratiemanagement.
4.3	Leverancier is service en system integrator over de partijen die mede verantwoordelijk zijn voor de correcte inwinning van de data (Meetnet Rotterdam, RWS, OSR, VRR, etc.)
4.4	De oplossing moet gebaseerd zijn op proven technology, gebruik maken van open of wereldstandaarden. Koppelbaar op basis van standaard interfaces (webservices, REST, SOAP, XML, etc.) met diverse HBR oplossings zoals bijvoorbeeld Portmaps, Hadoop en HaMis.
4.5	Leverancier biedt 24*7 support op elke applicatie/component/koppeling die onderdeel is van de geboden oplossing.
4.6	Aantoonbare beschikbaarheid van >99% van de keten, gedurende het servicewindow, vanuit het perspectief van de eindgebruiker.
4.7	De leverancier van de oplossing moet voorzien in een maandelijkse rapportage over de beheer-KPI's: het behaalde beschikbaarheids-percentage, aantallen incidenten, wijzigingen en oplostijden.
4.8	Het uitvallen van een component, door storing of regulier onderhoud, mag geen invloed hebben op de beschikbaarheid van andere componenten.
4.9	Er dient een uitwijkmogelijkheid te zijn indien er een calamiteit in het datacenter plaatsvindt (inclusief procedure) met een disaster recovery bij calamiteit binnen 4 uur.
4.10	De oplossing is redundant uitgevoerd in twee verschillende datacenters met een tussenliggende afstand van minimaal 100 kilometer.
4.11	De leverancier van de oplossing dient de volgende oplostijden voor incidenten aan te houden: urgente incidenten binnen 4 uur, incidenten met hoge prioriteit binnen 8 uur en incidenten met lage prioriteit binnen 48 uur.
4.12	Ieder wijzigingsverzoek dient te worden goedgekeurd in de change advisory board van het HbR. Onderhoud mag plaatsvinden binnen kantoortijden, maar niet leiden tot onbeschikbaarheid van de oplossing voor de eindgebruiker.
4.13	Maatwerkprogrammatuur moet onderhoudbaar zijn, en voldoende op kunnen worden doorontwikkeld. Bijvoorbeeld conform SIG 4* (incl geautomatiseerde testen en deployment).
4.14	De datacenters zijn duurzaam ofwel CO2 neutraal.

5 Beveiligbaarheid algemeen

5.1	Alle centrale ICT systemen, servers en services moeten zich fysiek bevinden binnen de Europese Unie en vallen onder Nederlandse of Europese wetgeving.
5.2	De leverancier moet ten aanzien van de geleverde ICT diensten en beheerprocessen voldoen en zijn gecertificeerd conform de ISO 27001 norm voor informatiebeveiliging.
5.3	De verbinding tussen HbR en een clouddienst is ten allen tijden versleuteld over HTTPS (TLS, SSL).
5.4	Gegevens worden versleuteld opgeslagen op basis van AES256.
5.5	De gegevens worden versleuteld opgeslagen. Het Havenbedrijf blijft ten allen tijde verantwoordelijk voor sleutelbeheer.
5.6	Autorisaties en encryptie schermen de gegevens van het Havenbedrijf af tegen andere gebruikers van uw clouddienst (bescherming tegen multi-tenant fouten).
5.7	De autorisaties van gebruikers t.b.v. het systeem worden binnen de het software pakket vastgelegd. Hiertoeworden alle rechten (CRUD) in het systeem gekoppeld aan rollen. Rollen zijn door functioneel beheerders v geheel zelfstandig, zonder dat daarvoor geavanceerde programmeerkennis nodig is (zero coding), vrij te definiëren en kunnen gekoppeld worden aan één of meer groepen in de directory server van het HbR die hiertoe realtime ingelezen worden in het systeem.
5.8	Naast door functioneel beheer vooraf gedefinieerde rollen zijn tevens ad-hoc rechten uit te geven door daartoe voor de betreffende workflow geautoriseerde personen
5.9	Er moet functiescheiding ingericht kunnen worden om het risico van vergissingen, nalatigheid en opzettelijk misbruik van systemen te verminderen. Bij het beheer van de informatiemiddelen wordt zeker voor de kritieke omgevingen onderscheid aangebracht in functies voor ontwikkeling, beheer en productie.
5.10	Applicatietaken voor het opvoeren van stamgegevens en het opvoeren van mutatiegegevens zijn gescheiden.
5.11	Applicaties worden ontwikkeld en getest op basis van landelijke richtlijnen voor beveiliging, zoals de richtlijnen voor webapplicaties van het NCSC. Er wordt tenminste getest op bekende kwetsbaarheden zoals vastgelegd in de OWASP top10.
5.12	Applicaties worden voor de in productie name onder andere getest op invoer van gegevens (grenswaarden, format, inconsistentie, SQL injectie, cross site scripting, etc.)
5.13	De uitvoerfuncties van programma's maken het mogelijk om de volledigheid en juistheid van gegevens te kunnen vaststellen.
5.14	Toegang tot de broncode is beperkt tot de werknemers, die deze code onderhouden of installeren.
5.15	Wanneer de ontwikkeling van software wordt uitbesteed, zijn er afspraken gemaakt met de leverancier ten aanzien van licentie- en eigendomsrechten van de software. Tevens zijn de kwaliteits- en informatiebeveiligingseisen contractueel vastgelegd en wordt er op toegezien dat de software voldoet aan deze eisen.
5.16	Er wordt alleen gebruik gemaakt van actuele versies van software die nog door de leverancier ondersteund worden.
5.17	Bij iedere module of gegevensstroom is bekend of en welke persoonsgegevens zij omvat en per gegevenselement wat de risicoklasse daarvan is en wat de verwerkingsgrond is.
5.18	Gegevensuitwisseling vindt versleuteld plaats, via onversleutelde kanalen gaat enkel ongevoelige informatie zoals een attenderingsbericht.
5.19	Het pakket bevat specifieke functies om wijzigingen in data aan te brengen, zoals 'toevoegen', 'wijzigen' en 'verwijderen'.

Non-Functionals

Projectnummer: I.000930

Status: Definitief

5.20	De oplossing biedt invoercontroles voor waarden die buiten een vooraf gedefinieerd bereik vallen, ongeldige tekens in invoervelden, ontbrekende of onvolledige gegevens en ongeautoriseerde of inconsistente beheergegevens.
5.21	Afwijkende invoer op grond van relatie- en redelijkheidscontrole wordt aan de gebruiker gesignaleerd voordat de invoer in het softwarepakket wordt verwerkt (bv vreemde Hydrometeo gegevens zoals waterstanden).
5.22	Gegevenselementen die kritisch zijn voor de toepassing moeten verplicht ingevuld worden voordat verdere gegevensverwerking plaats kan vinden.
5.23	In geval van massale invoer wordt de volledigheid gecontroleerd door middel van hash- en batchtotals.
5.24	Bij (geautomatiseerde) ontvangst van data moet het softwarepakket de authenticiteit van de verzender kunnen vaststellen.
5.25	Het gebruik van ICT-diensten en informatiebronnen is vastgelegd (logging) om vast te kunnen stellen of is voldaan aan het toegangsbeleid.
5.26	Het gebruik van speciale bevoegdheden wordt gecontroleerd door alle daaraan gerelateerde acties en handelingen te loggen (audit trail). De verantwoordelijke systeemeigenaar beoordeelt periodiek het gebruik van de speciale bevoegdheden door middel van de audit trail.
5.27	Het softwarepakket bevat geen mogelijkheid om een logfile aan te passen of te verwijderen.
5.28	Om toegang te krijgen tot het softwarepakket moet iedere gebruiker zich kunnen identificeren.
5.29	De oplossing geeft de mogelijkheid om de toegang te blokkeren na een vooraf vastgesteld (5 keer) aantal inlogpogingen.
5.30	De oplossing geeft de mogelijkheid om uit te loggen.
5.31	De oplossing slaat de wachtwoorden in beschermde vorm op, bijvoorbeeld met behulp van hash voorzien van salt mechanisme.
5.32	De oplossing biedt zodanige functionaliteit m.b.t. authenticatie en autorisatie, zowel voor gebruikers als voor applicaties, dat alle functionaliteiten van en gegevens in (c.q. te benaderen via) zodanig aan autorisaties onderworpen zijn dat zij zonder de juiste autorisaties niet te benaderen zijn.
5.33	Voor alle registraties en gegevensuitwisselingen geldt dat de systemen alleen op basis van geautoriseerde toegang kunnen worden gebruikt
5.34	De oplossing voorziet in de mogelijkheid van logische toegangsbeveiliging op basis van een rollenstructuur (bewarende, registrerende, uitvoerende, controlerende en beschikkende taken) en daarbij behorende rechten (lezen, schrijven, verwijderen, exporteren)
5.35	De eisen die worden gesteld aan wachtwoorden, zijn in overeenstemming met de waarde (classificatie) van de te benaderen informatie met het wachtwoord (min. 9 tekens, complex en max. 90 dagen geldig)
5.36	Standaard leverancieraccounts en wachtwoorden in software of voor het beheer van informatiemiddelen zijn verwijderd of ontoegankelijk gemaakt. De accountgegevens worden apart opgeborgen en alleen in geval van nood gebruikt, na toestemming van de systeemeigenaar.
5.37	Er is alleen toegang tot de applicatie door geautoriseerde gebruikers.
5.38	Authenticatie vindt plaats tegen de Active Directory.
5.39	Toegang tot webomgevingen verloopt via een beveiligde omgeving (HTTPS)
5.40	De toegang tot webomgevingen is te beperken door middel van whitelisting van IP adressen
5.41	Toekomstige oplossing moet Single Sign-on ondersteunen; een gebruiker hoeft na authenticatie tot het HbR netwerk niet opnieuw in te loggen

Non-Functionals

Projectnummer: I.000930

Status: Definitief

5.42	Voor webapplicaties geldt dat twee-factor authenticatie wordt toegepast voor alle gebruikers.
5.43	Het platform moet ingericht zijn volgens de NCSC 'ICT-Beveiligingsrichtlijnen voor Webapplicaties'.
5.44	Gebruikers van een API moeten geauthentiseerd zijn.
5.45	Toegang tot een API moet state-of-the-art bescherming gebruiken zoals HTTPS TLS 1.2 of hoger en ingericht volgens de NCSC 'ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)'.
5.46	De oplossing moet minimaal jaarlijks een beveiligingstest (zoals een penetratietest) ondergaan.
5.47	De oplossing moet beschermd zijn tegen DDoS aanvallen.
5.48	Wachtwoorden moeten gehasht en gesalt opgeslagen zijn.
5.49	Een sensor API zou IP gefilterd moeten zijn op bekende sensor IP adressen.
5.50	Berichten tussen cliënt en server moeten wederzijds geauthentiseerd zijn.
5.51	Berichten moeten integriteits-beschermd zijn (HMAC)
5.52	Geïnjecteerde berichten mogen niet geaccepteerd worden.
5.53	Gebruik standaard en open encryptie algoritmes en modes, bij voorkeur uit standaard libraries.
5.54	Er dient gebruik te worden gemaakt van certificate pinning.

6 Beveiligbaarheid IoT

6.1	IoT sensoren moeten veilig beheerd kunnen worden: * uitsluitend versleutelde en geauthenticeerde verbindingen * HTTPS voor webinterface * geen plain-text beheer (geen telnet, ftp, snmpv1) * geen onveilige services (zoals telnet, ftp, ...) * bij voorkeur geen passwords maar keys (en eventueel 2FA)
6.2	IoT sensoren moeten regelmatig geupdate kunnen worden: * maandelijkse updates * updates moeten geauthenticeerd en versleuteld zijn * de public key voor deze authenticatie moet gepind zijn op het device
6.3	IoT sensoren moeten kunnen worden gemonitord via een centrale voorziening: * beschikbaarheid * performance * security status (patches)
6.4	IoT sensoren moeten security events kunnen loggen naar een centrale log server: * minstens login events * tamper-events van de fysieke enclosure
6.5	IoT sensoren moeten fysiek beveiligd zijn: * tegen ongeautoriseerde toegang * tegen ongeautoriseerde manipulatie * de netwerk aansluiting mag niet misbruikt kunnen worden door een andere device
6.6	IoT sensoren zouden een host-based firewall moeten draaien: * die alleen toegang vanuit vooraf gedefinieerde management stations en het centrale platform toestaat * zodat hij niet bereikbaar is voor andere devices op of buiten het netwerk
6.7	IoT sensoren moet voldoende entropie hebben voor goed sleutelmateriaal: * let op first boot (installatie), certificaten genereren! * met name van belang voor asymmetrische sleutels
6.8	IoT sensoren mogen geen automatische configuratie gebruiken, maar handmatige provisioning: * geen standaard username / password * veilige configuratie out-of-the-box, geen defaults die lekken
6.9	IoT sensoren moeten gehardened zijn, geen ongebruikte services hebben draaien
6.10	IoT sensoren mogen (op netwerk-niveau) uitsluitend bereikbaar zijn vanaf management stations * niet bereikbaar zijn vanaf het publieke internet * IP-whitelist voor API / platform richting IoT netwerk
6.11	IoT sensoren moeten zich authenticeren tegen het netwerk.
6.12	Het netwerk moet zich authenticeren tegen IoT sensoren.
6.13	Het netwerk moet minimaal jaarlijks een security test ondergaan zoals een penetratietest.

Non-Functionals

Projectnummer: I.000930

Status: Definitief

7 Onderhoudbaarheid

7.1	Bij de oplossing moet documentatie ten behoeve van beheer en configuratie beschikbaar zijn.
7.2	Herstarten van één van de componenten van de oplossing leidt niet tot de verplichting dat de andere componenten herstart moeten worden.
7.3	De verschillende componenten binnen de oplossing moeten run-time autonoom van elkaar kunnen functioneren.
7.4	Het moet mogelijk zijn een nieuwe versie van een component te installeren, zonder dat er aanpassingen noodzakelijk zijn in de andere componenten.
7.5	Er moet van standaard functionaliteit (commercial off-the-shelf) gebruik gemaakt worden.
7.6	Het is gewenst dat de presentatielaag zoveel mogelijk los van de applicatielaag is.
7.7	Componenten uit de oplossing zijn onafhankelijk en schaalbaar. Dat wil zeggen dat het vervangen van een component niet tot het noodzakelijk vervangen van een andere component leidt.
7.8	De oplossing beschikt over afzonderlijke test-, acceptatie-, en productieomgeving.
7.9	Lokaal te installeren applicatiecomponenten kunnen geautomatiseerd worden uitgerold en aangeboden binnen concept het concept van de huidige werkplekleverancier.
7.10	Lokaal te installeren applicatiecomponenten worden gevirtualiseerd aan de werkplek aangeboden en niet lokaal geïnstalleerd.
7.11	Lokaal te installeren applicatiecomponenten zijn ook bruikbaar in de HbR thuiswerkomgeving (Citrix).
7.12	De oplossing moet beschikken over een exitstrategie in kader van vervangbaarheid.