

Bijlage 11

Software eisen registratie uitrukpakken en instructeurspakken

Datum: 25 oktober 2024

Versie: 1.0

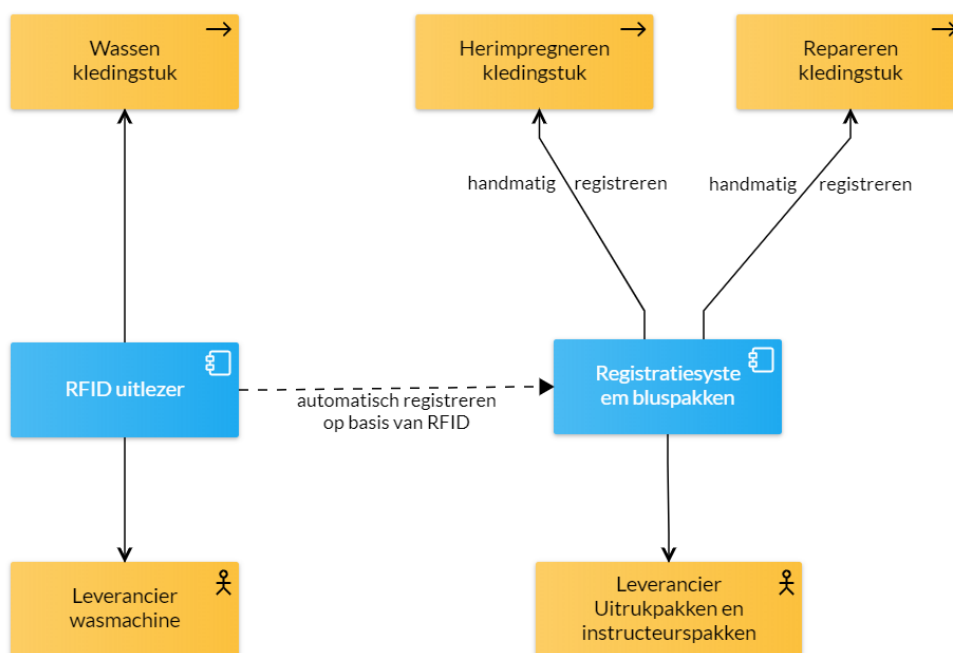
Auteur: Martijn Veurink

Organisatieonderdeel: Team Informatie

Inleiding

In dit document staan de eisen die van toepassing zijn voor het registratiesysteem uitrukpakken en instructeurspakken zoals benoemd in de opties OE.01, ~~OE.02 en OE.03~~ van het Programma van Eisen Uitrustpakken en instructeurspakken.

In onderstaand schema de opzet van het uitgevraagde systeem.



Algemene eisen

AE.1.	De applicatie betreft een SaaS oplossing.
AE.2.	De applicatie dient minimaal te voldoen aan de wet- en regelgeving op het gebied van informatiebeveiliging, vertrouwelijkheid en privacy (denk aan de Algemene verordening gegevensbescherming, de Wet beveiliging netwerk- en informatiesystemen en/of de NIS2-richtlijn).
AE.3.	De applicatie past binnen de kaders van Veiligheidsregio Referentiearchitectuur (VeRA). Deze toetsing vindt plaats middels de bij het project op te stellen PSA.
AE.4.	De data, gegevens van de VNOG, bevindt zich alleen in datacenters in de Europese Economische Ruimte (EER) of in een door Europese Unie erkent "veilig land". Indien er bedrijven betrokken zijn die onder de Amerikaanse wetgeving vallen dan moet dit bedrijf een actieve EU-U.S. Privacy Shield Framework hebben.
AE.5.	De applicatie (alsmede de data) is redundant over meerdere datacenters op verschillende locaties met een minimale onderlinge afstand van 25km.
AE.6.	De datacenters zijn ISO 27001 en ISO 27017 gecertificeerd (of vergelijkbaar).
AE.7.	De applicatie ondersteunt single sign-on (middels een koppeling met het AD van de VNOG).
AE.8.	De verbinding is beveiligd met een certificaat van een vertrouwde certificerings instantie (https).
AE.9.	Twee of meer nameservers van de domeinnaam hebben een IPv6-adres.
AE.10.	De domeinnaam is ondertekend met een geldige handtekening (DNSSEC).
AE.11.	De website/webapplicatie is beveiligd met HTTP Security headers (HTTP Strict Transport Security HSTS, X-Frame options, X-Content type option, Content Security Policy (CSP), Security Header (CT) en/of Feature-Policy).
AE.12.	Security.txt is geïmplementeerd (https://www.digitaltrustcenter.nl/securitytxt)
AE.13.	Resource Public Key Infrastructure (RPKI) is toegepast.
AE.14.	De leverancier zorgt ervoor dat beveiligingsadviezen van het NSCS (indien van toepassing) worden opgevolgd (zie https://www.ncsc.nl/actueel/beveiligingsadviezen).
AE.15.	De applicatie maakt gebruik van open standaarden (https://www.forumstandaardisatie.nl/open-standaarden)
AE.16.	De applicatie biedt de mogelijkheid tot verschillende autorisatie rollen (minimaal beheerder en gebruiker).

AE.17.	Er mag geen data verloren gaan. Historische backup en restore moet mogelijk zijn tot minimaal 10 dagen terug.
AE.18.	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt en toegankelijk te zijn voor de functioneel beheerder van de VNOG.
AE.19.	Er is een acceptatieomgeving van de applicatie beschikbaar en toegankelijk voor de VNOG die vergelijkbaar is met de productieomgeving.
AE.20.	De applicatie is webbased (direct vanaf de browser van de gebruiker te benaderen, dus geen constructies met rdp of citrix-achtige constructies).
AE.21.	De applicatie past zich automatisch aan aan de verschillende schermgroottes en resoluties van de gebruiker (responsive)
AE.22.	De oplossing werkt platform onafhankelijk (o.a. IOS, Android, Windows).
AE.23.	De applicatie kan gebruikt worden met Microsoft Edge, Google Chrome, Mozilla Firefox en Safari.
AE.24.	De applicatie is schaalbaar (de applicatie kan meegroeien bij een groei van gebruikers zonder software aanpassingen).
AE.25.	Indien de applicatie niet beschikbaar is wordt er een alert gestuurd naar de functioneel beheerder van de VNOG.
AE.26.	De opdrachtnemer verzorgt alle updates en waarborgt dat de VNOG steeds met de nieuwste, succesvol geteste applicatie werkt, zonder dat dit ten koste gaat van de beschikbaarheid en bruikbaarheid van de applicatie.
AE.27.	De uitrol van updates wordt in afstemming met de VNOG uitgevoerd, eerst op de acceptatieomgeving daarna de uitrol naar de productieomgeving.
AE.28.	De opdrachtnemer zorgt voor het technisch beheer van de applicatie (o.a. ontwikkeling en onderhoud van de software, de hosting en de infrastructuur van de software, de beveiliging en compliance van de software).
AE.29.	De opdrachtnemer faciliteert dat de VNOG zelfstandig de verschillende omgevingen (acceptatie en productie) functioneel kan beheren.
AE.30.	Per release, upgrade of fix wordt een volledig overzicht gegeven van de inhoud van de release, upgrade of fix.
AE.31.	Opdrachtnemer dient een volledige opleiding voor functioneel beheerders en train-de-trainers te organiseren t.b.v. de applicatie.
AE.32.	Opdrachtnemer onderhoudt documentatie voor functioneel beheerders (beheerdocumentatie) en gebruikers (handleidingen) en draagt er zorg voor dat deze altijd up-to-date is met de gebruikte versie van de applicatie.
AE.33.	De applicatie hanteert de Nederlands taal.

SLA eisen

ESLA.1.	Er wordt een SLA afgesproken tussen opdrachtgever en opdrachtnemer. In de SLA wordt o.a. vastgelegd wat de responstijd is op verstoringen en worden er communicatieafspraken gemaakt.
ESLA.2.	In de SLA wordt de datalek-procedure afgesproken.
ESLA.3.	De opdrachtnemer beschikt over professionele Nederlandstalige ondersteuning minimaal van 8 - 17 uur (maandag t/m vrijdag m.u.v. feestdagen).
ESLA.4.	De interactieve respons van de applicatie bedraagt niet meer dan 2 seconden.
ESLA.5.	De applicatie is 24/7 beschikbaar voor de eindgebruikers.
ESLA.6.	De applicatie is minimaal 99 % beschikbaar (uptime). De opdrachtnemer rapporteert per maand of per kwartaal over de uptime van de applicatie.