



Aansluitvoorwaarden Besturingssysteem Gemalen

Inhoudsopgave

1.0	Inleiding.....	2
1.1	Generieke Aansluitvoorwaarden.....	2
1.1.1	Eisen en wensen aan zelf te ontwikkelen additionele API's	5
2.0	Uitgangspunten SaaS ICT Prestatie	6
2.1	SaaS Aansluitvoorwaarden	7
2.1.1	Algemene SaaS aansluitvoorwaarden	7
2.1.2	Koppelingen	8
3.1	Additionele en Specifieke voorwaarden	9
4.1	Common Ground Aansluitvoorwaarden	10
4.1.1	Algemene eisen Common Ground	10
4.1.2	Aansluiten Common Ground gegevenslandschap	12
5.1	Bijlagen en Toelichting.....	14
5.1.1	Authenticatie en provisioning standaarden.....	14
5.1.2	Authenticatie en SSO	14
5.1.3	Wachtwoordbeleid	15
5.1.4	Aansluiting op mail voorziening	15
5.1.5	Toelichting common ground aansluitvoorwaarden	16
5.1.6	Verplichte standaarden.....	17

1.0 Inleiding

Dit hoofdstuk bevat de generieke aansluit voorwaarden. Deze voorwaarden dienen altijd doorlopen te worden en opgenomen te worden in het bestek. De generieke voorwaarden zijn opgesplitst in verschillende categorieën voorwaarden, deze dienen getoetst te worden aan de functionaliteit en toepassing van de ICT Prestatie.

1.1 GENERIEKE AANSLUITVOORWAARDEN

Tabel 1 Generieke aansluitvoorwaarden

Nr.	Eis – Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
		Dwingende voorwaarden		Wettelijke en/of Overheidsrichtlijnen
1.a	Eis	De ICT Prestatie ondersteunt de van toepassing zijnde standaarden uit de lijsten "pas toe of leg uit" en "aanbevolen standaarden" zoals gepubliceerd door het Forum standaardisatie. (Bijlage 5.1.6)	Verplichte standaarden	Hierbij is gebruikt gemaakt van beslisboom open standaarden
1.b	Eis	De gemeente conformeert zich aan de richtlijnen Baseline Informatiebeveiliging Overheid (BIO). De ICT Prestatie fungeert binnen de kaders van deze richtlijnen.	Normenkader overheid	Indien componenten niet binnen het normen kader functioneren dient dit duidelijk aangegeven te worden met dereden.
1.c	Eis	Alle opslag van data binnen de ICT Prestatie vindt plaats op locaties welke binnen de Europese economische ruimte bevinden (EER)	Wettelijke verplichting	Richtlijnen doorgifte en opslag van data met persoonsgegevens
1.d	Eis	De GIBIT is van toepassing voor inkoop voorwaarden conform het pas toe leg uit principe	Normenkader Utrecht	Uniforme toepassing van kwaliteitsnormen bij de inkoop van een ICT Prestatie GIBIT NG realisatie
		Overige voorwaarden		
1.e	Eis	De ICT Prestatie conformeert zich aan het domein namen beleid van de Gemeente Utrecht.	Herkenbaarheid en uitwisselbaarheid	Eenduidige herkenbaarheid van extern gepubliceerde ICT Prestaties. Volgens de richtlijn Domein naam beleid gemeente Utrecht

1.f	Eis	De ICT Prestatie ondersteunt de uitwisseling van gegevens tussen applicaties middels API (web) services of een andere Gestandaardiseerde methodiek	Standaardisatie van uitwisseling	Utrecht conformeert zich aan de NL API strategie Design Rules: KennisplatformAPI's [Geonovum]
		Authenticatie en autorisatie (Bijlage 5.1.1)		
1.g	Eis	Toegang tot de ICT Prestatie is dwingend geregeld op basis van Single-Sign-On, (SSO) middels Oauth (Bijlage 5.1)	Gebruik van Utrecht identiteit	De gebruiker kan hiermee inloggen met de Utrechtse identiteit en zijn wachtwoord
1.h	Eis	De ICT prestatie ondersteunt federatie middels de standaarden van de gemeente Utrecht (Bijlage 5.1)	Standaardisatie van aansluiten	Standaardisering van protocollen en methodieken
1.i	Eis	De ICT prestatie ondersteunt indien nodig MFA via Azure AD Multi-Factor authentication	Standaardisatie van aansluiten	Utrecht maakt gebruik van Microsoft Authenticator MFA, Deze app dient uniform toegepast te worden
1.j	Eis	Afhankelijk van de BIV-classificatie (3-3-3) wordt er gebruik gemaakt van een in de ICT prestatie aanwezige authenticatie methodiek. Deze voldoet minimaal aan het wachtwoord beleid (bijlage 5.1.3)		Afhankelijk van BIV classificatie zie beleid IAM
1.k	Eis	Indien er aansluiting op de mail omgeving van Utrecht benodigd is voldoet de ICT prestatie aan de aansluitvoorwaarden e- mail (bijlage 5.1.4)	Standaardisatie van aansluiten	Aansluiten op de mail voorziening indien functioneel benodigd voor de ICT- prestatie.
1.l	Eis	Gegevens die via het internet worden uitgewisseld dienen op een bij de data passende manier te worden beveiligd.		Bij hoog privacy gevoelige gegevens uitwisseling dienen er additionele maatregelen te worden getroffen. DPIA is niet van toepassing
1.m	Eis	Bij bericht uitwisseling met externe voorzieningen wordt authenticatie d.m.v. 2-zijdig TLS 1.2 of hoger toegepast.		Voldoen aan beveiligingsbeleid en forumstandaardisatie richtlijnen

		Releasemanagement		
1.n	Eis	De leverancier levert op aanvraag inzicht in de te verwachten ontwikkeling in de ICT prestatie		Inzicht in de roadmap van de leverancier om op toekomstige ontwikkelingen te kunnen inspelen.
		Algemeen		
1.o	Eis	De gemeente Utrecht behoudt zich het recht voor om alsnog af te zien van een opdracht als de ICT prestatie in een later stadium niet blijkt te voldoen aan de eisen of op onderdelen niet functioneert binnen het ICT-landschap van de gemeente Utrecht		
1.p	Eis	Alle in dit document genoemde versies en beschrijvingen zijn onderhevig aan verandering. De leverancier kan zich derhalve niet beroepen op onjuistheden of onvolledigheden in deze specificatie maar heeft de verantwoordelijkheid aanvullende vragen te stellen voor zover deze nodig zijn voor het uitbrengen van een juiste offerte of implementatie.		

1.1.1 Eisen en wensen aan zelf te ontwikkelen additionele API's

De onderstaande eisen en wensen betreffen de eisen en wensen als er binnen een project wordt besloten dat bepaalde informatie door API's moet worden ontsloten terwijl hier nog geen door de VNG vastgestelde standaard voor bestaat.

Tabel2 Beschrijving informatie landschap

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
1.1.a	Eis	De syntax en samenhang van de gegevens zijn in een informatiemodel gedocumenteerd. Het informatiemodel vormt de formele beschrijving van alle informatie die van belang is binnen het domein dat de ICT Prestatie ondersteunt en beschrijft het domein in termen van objecten, gegevens (attributen) en de relaties daartussen.		
1.1.b	Eis	Het informatiemodel van de ICT Prestatie wordt direct ter beschikking gesteld aan de opdrachtgever.		
1.1.c	Eis	De ICT prestatie maakt indien beschikbaar gebruik van een informatie model dat gestandaardiseerd is bij de VNG of een andere gemeentelijke-of rijks context.		
1.1.d	Eis	De API's zijn wat betreft mogelijke API- aanroepen en API-antwoorden gedocumenteerd en worden ter beschikking gesteld aan de opdrachtgever (minimaal conform OAS3).		
1.1.e	Eis	De API-documentatie met de mogelijke API- aanroepen en API-antwoorden mag de opdrachtgever met andere organisaties delen.		

Tabel 3 Technische wensen aan additioneel te ontwikkelen API's

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
1.1.f	Eis	Een nieuw te bouwen API wordt gebouwd volgens de standaarden zoals beschreven in REST-API Design Rules van Forum Standaardisatie (https://publicatie.centrumvoorstandaarden.nl/api/adr/#normative-design-rules)		
1.1.g	Eis	API's worden in de vorm van REST/JSON aangeboden		
1.1.h	Eis	API's implementeren regels t.b.v. de consistentie van de gegevens in de registratie.		

1.1.i	Eis	API's worden via een NLX gateway component (NLX-Inway) aangeboden aan andere applicaties. De leverancier verplicht zich maximaal 1 jaar na de ingangsdatum van het contract te kunnen voldoen aan deze eis.		
1.1.j	Eis	API's en registraties die door de leverancier gebouwd worden op verzoek van de gemeente, worden opensource onder een EUPL beschikbaar gesteld en het intellectueel eigendom ligt bij de opdrachtgever		
1.1.k	Eis	Indien er een API wordt gebouwd op een bestaande ICT prestatie van de leverancier, is deze API vrij van kosten door andere gemeenten te gebruiken		
1.1.l	Eis	In lijn met GIBIT Artikel 18 geldt dat de opdrachtgever eigenaar is van de gegevens Die vastgelegd worden in registratie en heeft ten alle tijden toegang tot de data		

Tabel 4 Beheer van additioneel te ontwikkelen API's

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
1.1.m	Eis	De leverancier garandeert het beschikbaar zijn van de API voor gebruik volgens de afgesproken SLA.		

2.0 UITGANGSPUNTEN SAAS ICT PRESTATIE

- Gebruikers hebben toegang tot een SaaS-ICT Prestatie via een beveiligde internet verbinding;
- Gebruikers van de SaaS-ICT Prestatie hebben uitsluitend een internetbrowser nodig voor het gebruik van een SaaS-ICT Prestatie ('zero footprint');
- Voor SaaS-ICT Prestaties wordt geen software op de infrastructuur van de gemeente Utrecht geïnstalleerd ('zero footprint');
- De aanbieder van de SaaS-ICT Prestatie verzorgt het applicatiebeheer, zoals het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates, beveiliging tegen ongeautoriseerde toegang en dergelijke.

2.1 SAAS AANSLUITVOORWAARDEN

2.1.1 Algemene SaaS aansluitvoorwaarden

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
2.1.a	Eis	Het gebruik van remote display en/of digitale workspace Software om een externe applicatie te benaderen is niet toegestaan.	Borgen vertrouwelijkheid, integriteit en beheer (zero footprint).	Voorkomen dat programmatuur op de infrastructuur van de gemeente moet worden geïnstalleerd.
2.1.b	EIS	De toegang tot de SaaS-applicatie kan worden beperk top basis van de bron.	Borgen vertrouwelijkheid	Afhankelijk van de aard van de gegevens en applicatie. Bij voorkeur i.c.m. Federatie en conditionele toegang.
2.1.c	Eis	De SaaS-applicatie maakt geen gebruik van plug-in componenten. (Bij een lokaal component geldt tevens IaaS aansluitvoorwaarden)	Borgen van interoperabiliteit En beheer van de beheerde werkplek infrastructuur van de gemeente Utrecht.	Plug-ins moeten in de standaardwerkplek worden opgenomen (compatibiliteit met werkplek en overige applicaties, beheer)
2.1.d	Eis	Voor het functioneren van de SAAS-applicatie op het client device en/of in de webbrowser zijn geen verdere instellingen en/of installaties op het client device en/of in de browser benodigd.	Borgen van interoperabiliteit En beheer van de beheerde werkplek infrastructuur van de gemeente Utrecht.	Voor het gebruik van de applicatie hoeft geen software geïnstalleerd te worden, geen aanpassingen aan de browser instellingen, de applicatie maakt geen gebruik van extensies op de browser.
2.1.e	Eis	De beschikbaarheid, responstijden van de front-end kan door de gemeente Utrecht worden gemonitord	Borgen van continuïteit	Opdrachtnemer toont aan middels een rapportage dat voldaan wordt aan de gestelde eisen in het SLA.

2.1.2 Koppelingen

De eisen en wensen zijn van toepassing op SaaS ICT Prestatie welke koppelingen hebben met andere applicaties. De eisen en wensen in deze paragraaf zijn aanvullend op de overige aansluitvoorwaarden.

Tabel 5 SaaS koppelingen

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
2.1.f	Eis	buitende infrastructuur van de gemeente Utrecht (zoals andere SaaS applicaties of landelijke voorzieningen) verlopen direct van de SaaS applicatie met de voorziening of SaaS applicatie.	Beheer alsmede efficiëntie.	Van de voorziening of SaaS applicatie. Redenen zijn (niet uitputtend): Performance ,robustheid, betrouwbaarheid, complexiteits reductie van de koppelingen en lagere beheer inspanning voor de gemeente.

3.1 ADDITIONELE EN SPECIFIEKE VOORWAARDEN

Tabel 6 Additionele aansluitvoorwaarden

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
3.1.a	Eis	Alle verbindingen worden beveiligd (VPN of APN) opgezet tussen objectlocatie en telemetriesysteem.		
3.1.b	Eis	Ook deze verbindingen worden voldoende beveiligd zodat een veilige communicatie tussen telemetriesysteem en objectlocatie tot stand wordt gebracht. Toekomstige Low Power communicatietechnieken worden ook ondersteund door de opdrachtnemer.		
3.1.c	Eis	Het telemetriesysteem beschikt over een volwaardige API waarmee gegevens tussen telemetriesysteem en andere applicaties op veilige wijze uitgewisseld kunnen worden. De API heeft geen limieten (restricties) in het opvragen van hoeveelheden data. Zowel object-, meet-, alarmdata als parameters zijn op te vragen in de API.		
3.1.d	Eis	Het telemetriesysteem maakt via een SSO aansluiting op Azure middels OAuth. (zie afb 5.1) Hiermee kunnen gebruikers op het interne netwerk makkelijk inloggen. Dit conflicteert niet met de gebruikers die niet in het AD bekend zijn of handmatig worden opgevoerd in het telemetriesysteem.		
3.1.e	Eis	Buiten het gemeentelijk netwerk wordt gebruik gemaakt van two-factor authenticatie, dan wordt na het inloggen met gebruikersnaam en wachtwoord een token verstuurd.		
3.1.f	Eis	De hoofdpst dient gehost te worden bij de opdrachtnemer. De hostingomgeving dient aantoonbaar in landen binnen de EER te zijn ondergebracht en onder de Europese regelgeving te vallen voor databescherming.		
3.1.g	Eis	De SIM kaarten zijn geschikt om een beveiligde verbinding tussen PLC besturing en telemetriesysteem te kunnen opzetten.		

4.1 COMMON GROUND AANSLUITVOORWAARDEN

Mits van toepassing bij de aanbestedingen gaan we als gemeente de markt op om een standaardpakket (geen nieuwbouw of maatwerk) af te nemen. Een leverancier kan dit product aanbieden als SaaS-dienst of de gemeente Utrecht kan zelf in de hosting en beheer van het product voorzien. Vanuit Common Ground stellen we aan standaardpakketten alleen eisen aan de koppelvlakken en randen van de applicatie. Overige infrastructuur en beveiligingseisen zijn opgenomen in de aansluitvoorwaarden van een specifieke oplossing.

Achtergrond informatie over Common Ground is opgenomen in de bijlage Toelichting Common Ground aansluitvoorwaarden.

De eisen die we stellen zitten enkel aan de koppelvlakken/randen van de applicatie. Kort gezegd komt het erop neer dat we het volgende willen bereiken:

- Een ICT Prestatie maakt gebruik van data in [het common ground / GEMMA gegevenslandschap](#). Dit kan zowel het opvragen van gegevens uit het gegevenslandschap als mede het wijzigen / opslaan van gegevens zijn
- Als een ICT Prestatie informatie aanbiedt willen we dat deze de informatie conform de [VNG API standaarden](#) aanbiedt.
- Als een ICT Prestatie door middel van een API informatie aanbiedt waar nog geen standaarden voor zijn vastgesteld, geven we een aantal eisen mee waar de implementatie van de API aan moet voldoen.

Onder het Common Ground gegevenslandschap verstaan we de implementatie van een aantal door de VNG gestandaardiseerde API's waarvan een deel bij de gemeente draait en een deel landelijk. Voor een actuele lijst verwijzen we naar bijlage Bronregistraties Common Ground gegevenslandschap.

4.1.1 Algemene eisen Common Ground

Dit hoofdstuk beschrijft de algemeengeldende eisen en wensen voor Common Ground. De tabel is van toepassing ongeacht het type ICT Prestatie.

Tabel 7 Algemene eisen Common Ground

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
4.1.a	Eis	De leverancier ¹ heeft het Groeipact Common Ground ondertekend het geen zichtbaar is op de website van CommonGround.nl bij 'Overzicht Deelnemers Groeipact CommonGround.		
4.1.b	Eis	Leverancier die een API conform de VNG-standaard implementeert, ondersteunt alle in de bijbehorende specificaties beschreven operaties met uitzondering van de in de opdracht als uitzondering benoemde operaties.		

4.1.c	Eis	Leveranciers die VNG API-standaarden implementeren, zorgen ervoor dat nieuweversies van de standaard niet later dan zes maanden na het bereiken van de status 'in gebruik' deze conform specificatie zijn geïmplementeerd. Leverancier verricht de voor implementatie benodigde werkzaamheden tegen de in de overeenkomst bepaalde tarieven en condities. Een actueel overzicht van API-standaarden en de bijbehorende statussen is te vinden op GEMMAOnline .		
4.1.d	Eis	Conform GIBIT-artikel 6.2 geldt dat voor API's die onderdeel zijn van de ICT Prestatie en VNG API-standaarden implementeren dat de bijbehorende testscenario's in het VNG API-testplatform Voorafgaand aan implementatie succesvol zijn doorlopen.		
4.1.e	Eis	In lijn met GIBIT Artikel 18 geldt dat de opdrachtgever eigenaar is van de gegevens die vastgelegd worden in de registratie en heeft ten alle tijden toegang tot de data		
4.1.f	Wens	Leverancier draagt actief bij aan de ontwikkeling van API-standaarden door suggesties voor verbeteringen, voor zover die voor een bredere groep gemeenten relevant zijn, in te dienen bij de Organisatie die de betreffende standaard beheert.		
4.1.g	Wens	De leverancier maakt bij de ICT Prestatie gebruik van software componenten uit de CommonGround-componentencatalogus (vindbaar op CommonGround.nl). Beschrijf in uw aanbod welke componenten u toepast en op welke manier deze componenten worden gebruikt.		

4.12 Aansluiting op CommonGround gegevenslandschap

ICT Prestaties sluiten aan op het CommonGround gegevenslandschap. Dit kan zijn voor het ophalen van gegevens maar ook voor het creëren en muteren van gegevens. De volgende tabel geeft de eisen en wensen weer die relevant zijn voor het aansluiten van een applicatielandschap op het gegevenslandschap.

Tabel 8 Aansluiting op gegevens landschap

Nr.	Eis - Wens	Omschrijving aansluitvoorwaarden	Waarom	Toelichting
4.1.h	Eis	De ICT Prestatie maakt, indien beschikbaar, gebruik van door andere onderdelen binnen het applicatielandschap van Opdrachtgever of door haar partners beschikbaar gemaakte gegevens in bronregisters. Opdrachtgever levert hiertoe een overzicht van (relevante) ontsloten bronnen.		Beschrijf in uw aanbod welke bronnen u gebruikten op welke manier deze bronnen worden gebruikt in de ICT Prestatie.
4.1.i	Eis	Bij het aansluiten op gemeentelijke bronregisters draagt de leverancier zorg voor het actueel houden van de informatie in de bronregistratie voor Zover dit informatie betreft die binnen de ICT-prestatie wordt beheerd.		
4.1.j	Eis	Op het moment dat de aangeboden koppelvlakken wijzigen in een major version (conform semantic versioning) van een basisregistratie of andere gestandaardiseerde registratie die door de ICT Prestatie gebruikt wordt (bijv. API's naast de eerdere StuF), zal de leverancier binnen 6 maanden haar geïmplementeerde koppelvlak conform de nieuwe specificatie aanpassen.		
4.1.k	Eis	De aanroep van een API waarin persoonsgegevens worden bevraagd, wordt vastgelegd in logbestanden conform de eisen vanuit de AVG, ongeacht of de aanroep succesvol was of niet.		

4.1.l	Eis	API-aanroepen naar andere applicaties worden via een NLX-gateway component (NLX-Outway) gedaan. De leverancier verplicht zich maximaal 1 jaar na de ingangsdatum van het contractte kunnen voldoen aan deze eis.		
4.1.m	Eis	De door de leverancier / aanbieder aangeboden API's worden via een NLX gateway component (NLX-Inway) aangeboden. De leverancier verplicht zich maximaal 1 jaar na de ingangsdatum van het contractte kunnen voldoen aan deze eis		
4.1.n	Eis	Door de ICT Prestatie worden abonnementen aan dienstenafnemers aangeboden op wijzigingen in bron gegevens die in haar ICT Prestatie zijn vastgelegd. (conform pub/sub mechanisme)		
4.1.o	Eis	De ICT Prestatie maakt voor het publiceren en afnemen van abonnementen gebruik van de gemeentelijke notificatiecomponent voor objecten uit de API's voorzaakgericht werken.		
4.1.p	Eis	Digitale informatieobjecten voldoen aan de eisen uit de Archiefwet en hebben de Daarbij benodigde metadatering.		
4.1.q	Wens	De ICT Prestatie haalt gegevens op via API's van een bronsysteem niet eerder dan dat deze nodig zijn (in plaats van vooraf een lokale kopie op te zetten). Dit geldt voor alle gevallen waar bronsystemen de daarvoor benodigde API's aanbieden.		
4.1.r	Wens	Gegevens uit externe bronnen die met API's real-time zijn te bevragen of opgeslagen, worden niet als kopie van de bron in de ICT Prestatie vastgelegd.		
4.1.s	Wens	Alle als brongegevens beschouwde gegevens die in de ICT Prestatie zijn vastgelegd, worden via API's ontsloten waarbij de API's onderdeel zijn van de ICT prestatie		
4.1.t		De specificatie van de API wordt gepubliceerd. Dit is van toepassing als de ICT Prestatie zelf de bronregistratie is voor een unieke set van gegevens die door andere toepassingen gebruikt moeten kunnen worden.		

5.1 Bijlagen en Toelichting

5.1.1 Authenticatie en Provisioning standaarden

De gemeente maakt van marktconforme protocollen en wordt standaard aangesloten op Azure Federatie. Onderstaande tabel bevat dedoor Utrechtondersteunde protocollen en toepassing daarvan. Eris een IAM loketbeschikbaar welke de federatieve koppeling samen met de leverancier realiseert

Authenticatie middelen

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloud-applicaties
1	OpenID Connect Oauthv2	Voorkeur	Azure Federatie (3)	Ja	Ja
2	SAMLv2.0	Alternatief	Azure Federatie	Ja	Ja
3	Kerberos	Alleen intern	ActiveDirectory	Ja	Nee
4	LDAPS	Niettoegestaan		n.v.t.	n.v.t.

Identity Provisioning

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/Cloudapplicaties
1	SCIMv2	Voorkeur	Azure SCIM endpoint	Ja	Ja
2	SCIMv2	Alternatief	Intern SCIM endpoint	Ja	Ja
3	Maatwerk REST API	Indienbeschikbaar	Azure SCIM	Ja	Ja
4	Maatwerk XML SOAP	Alleen bij uitzondering		Ja	Ja
5	Eigen implementatie	Alleen bij uitzondering		Ja	Ja
6	Handmatig	Afhankelijk van BIV classificatie toegestaan		Ja	Ja
7	MicrosoftLDAPS	Niettoegestaan		n.v.t.	n.v.t.
8	Bestand: XML, JSON (beveiligd)	Niettoegestaan		n.v.t.	n.v.t.

Toelichting;

1. Nummering van protocollen staat in volgorde van voorkeur
2. De mate en inrichting van identity provisioning is mede afhankelijk BIV-classificatie en het gebruik van rollen.
3. Bij Container platform met Keycloak als broker
4. Alleen bij uitzondering; na afstemming met IAM en architectuur

5.1.2 Authenticatie en SSO

Utrecht hanteert het Single Sign On beleid voor interne en externe applicaties aangevuld met een tweede factor. Medewerkers van de Gemeente Utrecht beschikken over één identiteit en een 2^e factor op basis van Microsoft MFA. Ten behoeve van SSO wordt er federatie toegepast op basis van Azure Federatie en het conditionele toegang beleid.

Identiteiten worden automatisch beheerd, applicaties worden aangesloten voor authenticatie op de Utrecht

identiteit. Hiervoor zijn aansluit voorwaarden van toepassing (zie Authenticatie en provisioning standaarden) Medewerkers van de Gemeente Utrecht beschikken over één identiteit en een 2^e factor op basis van Microsoft MFA.

5.1.3 Wachtwoord beleid

Utrecht hanteert het volgende minimale wachtwoord beleid voor de Utrecht identiteiten

Lengte; minimaal 12 karakters

1. **Complexiteit;** Een complex wachtwoord bestaat uit minimaal twaalf karakters waarin ten minste 3 van de 4 karakters gebruikt worden:

- kleine letters : a, b, c, ... z
- hoofdletters : A, B, C, ... Z
- cijfers : 0, 1, 2, ... 9
- speciaal tekens : ({}[],.<>;:'"/\`~!@#\$%^&*()_-=)

2. **Naam:** Het wachtwoord mag niet de voornaam of achternaam bevatten van de betreffende natuurlijk persoon behorende bij deze identiteit

3. **Verboden woorden / begrippen:** (delen van) wachtwoorden mogen geen woorden omvatten die opgeslagen zijn in een tabel van verboden woorden / begrippen ter voorkoming van makkelijke wachtwoorden (bijvoorbeeld 'Welkom123456')

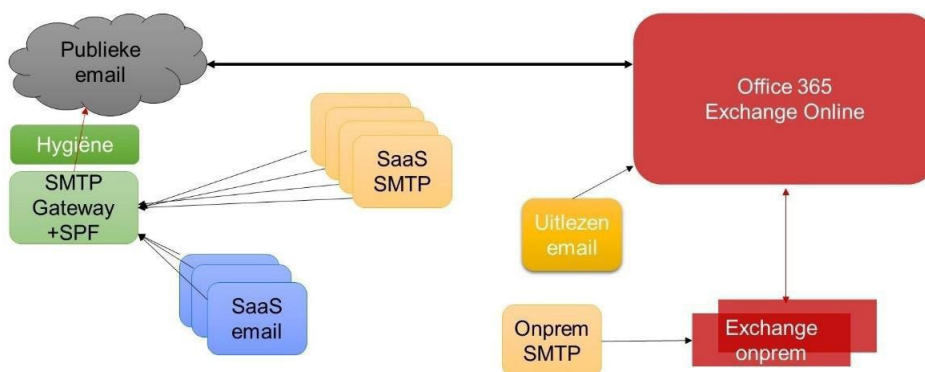
4. **Vervaltermijn;** minimaal om 60 dagen vernieuwen van het wachtwoord (BIO-beleid).

5. **Wijzigingen van wachtwoord:** Het wachtwoord kan op zijn vroegst na 7 dagen weer veranderd worden. Zes (6) recente wachtwoordwijzigingen worden onthouden en mogen niet opnieuw worden gebruikt en worden accounts automatisch geblokkeerd;

- Na 3 foutieve inlogpogingen voor minimaal 10 minuten.
- Als de geldigheidstermijn van het wachtwoord is verlopen

5.1.4 Aansluiting op mailvoorziening

Utrecht maakt voor de mail voorziening primair gebruik van Microsoft 365 Exchange Online i.c.m. een lokale Exchange installatie voor specials en interne routing. Alle applicaties welke verzending namens een Utrecht email adres nodig hebben sluiten aan op de Exchange online SMTP dienst. De voorkeur is dat er gebruik gemaakt wordt van Graph API voor het verzenden en ontvangen van mail.



5.1.5 Toelichting common ground aansluitvoorwaarden

Gemeenten hebben een nieuwe, moderne, gezamenlijke informatievoorziening nodig voor het uitwisselen van gegevens. Het huidige stelsel voor gegevensuitwisseling maakt het lastig om snel en flexibel te vernieuwen, te voldoen aan privacywetgeving en efficiënt om te gaan met data. Dat staat de verbetering van de gemeentelijke dienstverlening en efficiënte bedrijfsvoering in de weg.

Vanuit die behoefte is Common Ground ontstaan. In de kern gaat het bij Common Ground hierom: een hervorming van de gemeentelijke informatievoorziening, door op een andere manier om te gaan met gegevens. Zo koppelen we data los van werkprocessen en applicaties. We bevragen data bij de bron, in plaats van ze veelvuldig te kopiëren en op te slaan. Met de herinrichting van de informatievoorziening kunnen gemeenten hun dienstverlening en bedrijfsvoering ingrijpend verbeteren. Dat stelt ze in staat om op een moderne en flexibele manier in te spelen op maatschappelijke opgaven. (bron: [Common Ground: wat, hoe en waarom?](#))

Om dit verder te verduidelijken: in de huidige gemeentelijke ICT-infrastructuur is data vaak als het ware in 'silo's' per beleidsdomein (lees: applicatie) opgesloten. Gemeenten ontsluiten die gegevens via koppelingen, die vaak complex, kwetsbaar en niet eenduidig gestandaardiseerd zijn. Ze kopiëren veelal gegevens naar de eigen omgeving. Terwijl het beter zou zijn om gegevens eenmalig op te slaan en meervoudig te gebruiken. Met Common Ground komt dat principe binnen handbereik. Common Ground is een gedistribueerd model waarin data en applicaties van elkaar gescheiden zijn. Data wordt ontsloten via API's⁴. Zo'n API of application programming interface is een klein stukje software dat speciaal bedoeld is om gegevens te ontsluiten.

5.1.6 Verplichte standaarden

Standaard	Omschrijving	Waar toegepast
CSV	Tabelbestanden	Voor het importeren en exporteren van meetdata in en uit het telemetriesysteem.
Datum en tijd	Datum en tijd	Alle meetdata, instellingen en andere gelogde data worden vastgelegd met datum en tijd in het telemetriesysteem.
DHCP	Toewijzing netwerkadressen	Op de achtergrond voor de communicatie tussen objecten en telemetriesysteem.
DNS	Netwerkcommunicatie	Idem
FTP	Bestandsuitwisseling	Indien niet middels een API wordt uitgewisseld kan het traditioneel op basis van een FTP koppeling plaatsvinden.
HTML	Opmaak van webpagina's	We vragen om een volledig webgebaseerde oplossing, dus HTML is daarbij van toepassing.
HTTP	Webcommunicatie	Wij vragen om een beveiligde HTTPS verbinding.
IP Sec	Beveiligde IP verbindingen	Voor het opzetten van een beveiligde verbinding tussen objecten en het telemetriesysteem.
JSON	Uitwisselen van datastructuren	Voor het importeren en exporteren van meetdata in en uit het telemetriesysteem.
NTP	Synchroniseren van tijd	Voor het synchroniseren van tijd in de PLC besturingen vanuit het telemetriesysteem.
OAuth	API Autorisatiestandaard	Voor autorisatie bij het gebruik maken van API's beide richtingen op.
OData	Bevraging van REST API's	Voor het gebruik van API's in beide richtingen.
PDF/UA	Formaat documentpublicatie	Voor het rapporteren of exporteren van tabellen, rapporten en/of grafieken.
SMTP	Versturen van e-mail	Voor het doormelden van alarmen op basis van e-mail.
SVG	Grafische afbeeldingen	Voor het (mogelijk) opstellen van processchermen die vector georiënteerd zijn en dus schaalbaar zijn op verschillende devices.
TCP/OP	Netwerkcommunicatie	Voor het opzetten van verbindingen met het telemetriesysteem.
XML	Gestructureerde gegevens in tekstformaat	Voor het importeren en exporteren van meetdata in en uit het telemetriesysteem
XSD	Beschrijven van XML documenten	Voor het importeren en exporteren van meetdata in en uit het telemetriesysteem
XSL	Transformeren XML berichten	Voor het importeren en exporteren van meetdata in en uit het telemetriesysteem