

Technische aansluitvoorwaarden SAAS Applicaties (*Roosterapplicatie*)

Gemeente Utrecht

22 Oktober 2020

Kenmerk

Versie 1.5

Definitief



Gemeente Utrecht

Utrecht.nl

Inhoud

1	Technische aansluitvoorwaarden SaaS applicaties	4
2	Toelichting op de aansluitvoorwaarden	Fout! Bladwijzer niet gedefinieerd.
3	Technische aansluitvoorwaarden	6

Documenteigenschappen

Historie

Versie	Datum	Auteur	Aanpassingen
1.1	16 december 2019	Domstad IT	Gepubliceerde versie.
1.2	14 juli 2020	Domstad IT	Aanvullingen.
1.3	29 sept. 2020	Domstad IT	Verwerking opmerkingen review architectuurboard.
1.4	19 Okt. 2020	Domstad IT	Verdere aanvulling.
1.5	22 Okt.2020	Domstad IT	Verwerking review architectuurboard.

Distributie / Review

Naam	Rol	Versie ¹					
		1.0	1.1	1.2	1.3	1.4	1.5
Architectuurboard		☺				☺	✓

¹ I = ter informatie R = ter review ☺ = commentaar geleverd ☹ = niet gereageerd ✓ = Akkoord bevonden

1 Technische aansluitvoorwaarden SaaS applicaties

1.1 Inleiding

Dit document bevat de technische aansluitvoorwaarden voor applicaties (en software services, SaaS applicaties) die buiten de ICT infrastructuur van de gemeente Utrecht gehost worden.

Naast deze technische aansluitvoorwaarden gelden aanvullende eisen ten aanzien informatiebeveiliging en privacy, beschikbaarheid en responsetijden, koppelingen etc. Deze eisen worden gescheiden van de technische aansluitvoorwaarden gespecificeerd.

1.2 Definitie

Software as a service (SaaS) is software die als een online dienst wordt aangeboden. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer van de applicatie. De gebruiker benadert de applicatie over het internet.

1.3 Doel van de aansluitvoorwaarden

De technische aansluitvoorwaarden beogen om de algemene eisen voor SaaS applicaties te uniformeren en de technische randvoorwaarden te duiden. De aansluitvoorwaarden bevatten het geen dat als belangrijk, verstandig en veilig wordt beschouwd voor het gebruik van SaaS applicaties door de gemeente Utrecht.

De gemeente streeft de volgende doelen na met de technische aansluitvoorwaarden:

- Het gebruik van SaaS applicaties is veilig;
- Het gebruik van SaaS applicaties is robuust en betrouwbaar;
- De SaaS applicatie sluit aan bij de ICT infrastructuur van de gemeente;
- Het gebruik van SaaS applicaties leidt tot lagere beheerlasten voor de gemeente;
- Uniformiteit in de aansluiting van SaaS applicaties.

1.4 Uitgangspunten

De uitgangspunten van de gemeente Utrecht voor SaaS applicaties zijn:

- Gebruikers hebben toegang tot een SaaS applicatie via een beveiligde internet verbinding;
- Gebruikers van de SaaS applicatie hebben uitsluitend een internetbrowser nodig voor het gebruik van een SaaS applicatie ('zero footprint');
- Voor SaaS applicaties wordt geen software op de infrastructuur van de gemeente Utrecht geïnstalleerd ('zero footprint');
- De aanbieder van de SaaS applicatie 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.

1.5 Indeling van de aansluitvoorwaarden

De aansluitvoorwaarden zijn ingedeeld naar het gebruik van de SaaS applicatie:

- Algemene voorwaarden: deze voorwaarden zijn van toepassing op alle SaaS applicaties.
- Voorwaarden voor gemeente applicaties
Gemeente applicaties worden uitsluitend gebruikt door medewerkers of medewerkers van partners van de gemeente Utrecht. Voor deze applicaties gelden eisen ten aanzien van gebruik van het Utrechtse Identity en Access Management systeem en integratie met de Utrechtse ICT voorzieningen zoals de werkplek.
Voorbeelden van gemeente applicaties zijn:
 - Applicatie voor financiële administratie.
 - Applicatie voor de personeelsadministratie.
- Voorwaarden voor publieksapplicaties²
Publieksapplicaties worden gebruikt door gebruikers die geen medewerker van de gemeente Utrecht zijn, bijvoorbeeld inwoners van de gemeente. Voor deze applicaties gelden aanvullende eisen, bijvoorbeeld voor te gebruiken domeinnamen of het gebruik van Digid en/of eHerkenning.
Een voorbeeld van een publieksapplicatie is de wervings- en selectie applicatie met de 'werkenbij' site voor solliciteren bij de gemeente.
- Voorwaarden voor koppelingen
Voor SaaS applicaties die koppelingen hebben gelden eisen ten aanzien van de beveiliging van verbindingen en de wijze waarop applicaties gekoppeld kunnen worden.

1.6 Bijlagen

De aansluitvoorwaarden verwijzen naar de volgende bijlagen:

- Aansluiting op de maildienst van Gemeente Utrecht;
- Authenticatie en provisioning standaarden;
- ICT Infrastructuur van de gemeente Utrecht;
- Domeinnamen beleid van de gemeente Utrecht.

1.7 Afkortingen

Afking	Betekenis
AD	Active Directory
ADFS	Active Directory Federation Services
AVG	Algemene Verordening Gegevensbescherming
GEMMA	GEMEentelijke Model Architectuur
IAM	Identity and Access Management
SaaS	Software as a Service
SSO	Single Sign On
TEA	Technische Eisen Applicaties

² Veelal zullen publieksapplicaties ook door medewerkers van de gemeente Utrecht gebruikt worden.

Bijvoorbeeld de applicatie voor aanvragen en toekennen van subsidies:

- Inwoners en organisaties gebruiken dit systeem voor het aanvragen van subsidies;
- Medewerkers van de gemeente gebruiken het systeem voor het afhandelen van subsidie aanvragen.

2 Technische aansluitvoorwaarden

2.1 Aansluitdocument van de leverancier

Indien de leverancier een eigen aansluitdocument of aansluitvoorwaarden voor uw applicatie heeft, dan dient dit document bij uw inschrijving meegestuurd te worden.

De eisen uit uw document zullen door de Gemeente vergeleken worden met de aansluitvoorwaarden van de gemeente zoals opgenomen in dit document. Indien uit uw document blijkt dat uw applicatie niet aan de aansluitvoorwaarden van de gemeente voldoet, dan wordt uw aanbidding als ongeldig terzijde gelegd.

Nummer	Eis / Wens	Punten	Specificatie
1	Eis		Indien uw applicatie over een aansluitdocument of aansluitvoorwaarden beschikt, dan dient u dit document bij de beantwoording van de aanbesteding als bijlage op te nemen. Indien dit document niet is bijgesloten, gaat de gemeente er vanuit dat er geen aanvullende (technische) eisen gesteld worden aan het functioneren van de applicatie.

2.2 Aansluitvoorwaarden

2.2.1 Toelichting

De tabellen in deze paragraaf bevatten de aansluitvoorwaarden:

Kolom	Omschrijving
Nr.	Nummer van de aansluitvoorwaarde
Eis/Wens	Geeft aan of het een Eis of Wens betreft
Punten	Aantal punten dat u voor een Wens kunt krijgen
Omschrijving	Beschrijving van de aansluitvoorwaarden
Waarom?	Toelichting van het beoogde doel
Invulling	Invulling of nadere toelichting voor de aansluitvoorwaarde

2.2.2 Algemeen

Deze aansluitvoorwaarden zijn van toepassing op alle typen SaaS applicaties.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
1	Eis		De verbinding met de SaaS webapplicatie is beveiligd.	Borgen van vertrouwelijkheid en integriteit.	Gebruik https over TLS. http is niet toegestaan. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC , waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden.
2	Eis		De URL SaaS applicatie dient te kunnen benaderd middels de Fully Qualified Domain Name.	Borgen van integriteit.	Voorbeeld: <u>wel</u> https://applicatie.domeinnaam.nl of <u>niet</u> https://applicatie.nl

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
3	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).	Remote desktop uitschakelen, applicatie niet aanbieden via digitale workspace software zoals bijv. Citrix/horizon view etc. (PCOIP), ICA en RGS.
4	Eis		De SaaS applicatie is vanuit elke mogelijke locatie via het internet benaderbaar.	In het kader van flexibiliteit van levering via welk medium dan ook, zonder gebonden te zijn aan type medium (bijv. niet gebonden aan werkplek).	De applicatie kan ook buiten Utrechtse werkplek gebruikt worden.
5	Wens		De toegang tot de SaaS applicatie kan worden beperkt op basis van de bron.	Borgen vertrouwelijkheid.	Toegang tot de applicatie kan beperkt worden op basis van de bron, bijv. IP adres of een reeks IP-adressen. Voorbeeld: De applicatie kan alleen van een Utrechtse werkplek gebruikt worden. VERVALLEN
6	Eis		De SAAS applicatie maakt geen gebruik van plug-in componenten.	Borgen van interoperabiliteit en beheer van de beheerde werkplek infrastructuur van de gemeente Utrecht.	Geen gebruik maken van o.a. Microsoft Active X, Microsoft Silverlight, Microsoft ClickOnce, Adobe Flash en Java plug-in.
7	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.
8	Eis		De applicatie voldoet aan de voorwaarden van de gemeente Utrecht voor het gebruik van de email faciliteiten van Utrecht en/of email versturen namens de gemeente.	Waarborgen integriteit	Zie Bijlage: Aansluiting op de maildienst van Gemeente Utrecht v1.0

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
9	Eis		Het gebruik van voorzieningen voor opslag en bestandsuitwisseling in 'de cloud' kan geconfigureerd worden.	Waarborgen integriteit en vertrouwelijkheid	Met opslag en bestandsuitwisseling worden diensten als Dropbox, OneDrive, Google Drive, iCloud, WeTransfer, SendAnywhere etc. bedoeld. Met 'geconfigureerd' wordt bedoelt: 1. Het gebruik van deze diensten kan in- of uitgeschakeld worden en 2. De dienst ingesteld kan worden. Voorbeeld: in de applicatie kan ingesteld worden dat applicatie OneDrive voor bestandsuitwisseling gebruikt.
10	Wens		De beschikbaarheid van SaaS applicaties kan door de gemeente Utrecht gemonitord worden.	Borgen van continuïteit	De constructie van de SaaS applicatie dient toe te laten dat de applicatie door de gemeente Utrecht gemonitord wordt.
11	Eis		De database van de SaaS applicatie beschikt over de optie om (persoons) gegevens versleuteld op te slaan.	Waarborgen van vertrouwelijkheid.	Versleuteling is onderdeel van het database management systeem dat door de SaaS applicatie gebruikt wordt.

2.2.3 Gemeente applicaties

De eisen en wensen zijn van toepassing op applicaties die door medewerkers van de gemeente Utrecht gebruikt worden. De eisen en wensen in deze paragraaf zijn aanvullend op de overige aansluitvoorwaarden.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
12	Eis		De SAAS applicatie sluit aan op de binnen de Gemeente Utrecht geldende standaarden ten aanzien van de ICT-infrastructuur.	Borgen interoperabiliteit.	Wanneer er sprake is van het aansluiten op een component binnen Utrecht dan rekening houden met de aspecten zoals benoemd in Bijlage: ICT_Infrastructuur_gemeente_Utrecht_v1.7.
13	Eis		De SaaS applicatie ondersteunt, zonder beperking van functionaliteit, de	Borgen toegankelijkheid en laagdrempeligheid qua gebruik.	Rekening houden met compatibiliteit/ondersteuning door gangbare desktop browsers en of mobiele browsers. Microsoft Edge is de standaard browser op de Windows 10 werkplek.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
			browsers die in gebruik zijn bij gemeente Utrecht.		Zie Bijlage: ICT_Infrastructuur_gemeente_Utrecht_v1.7.
14	Eis		De applicatie is verplicht gebruik te maken van de Utrechtse IAM voorziening voor authenticatie van gebruikers, inclusief multi factor authenticatie door middel van Single Sign On.	Verlagen beheerinspanning en verhogen beveiligingsniveau, om integratie mogelijk te maken.	De gebruiker kan hiermee inloggen met de Utrechtse netwerk inlognaam en wachtwoord, en indien vereist, een token voor multifactor authenticatie. Zie Bijlage: Authenticatie_en_provisioning_standaarden_v1.3.
15	Wens		De SaaS applicatie dient over features te beschikken die het mogelijk maken om eenvoudig multi factor authenticatie in te zetten.	Flexibiliteit benodigd, als extra tegenmaatregel.	Indien invulling wordt gegeven aan voorwaarde 14 dan kan de MFA voorziening van Utrecht worden ingezet.
17	Eis		Indien een applicatie gebruik maakt wordt van Single Sign On wordt het wachtwoord van gebruikersaccounts niet opgeslagen in de applicatie.	Informatiebeveiliging.	

2.2.4 Koppelingen

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

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
22	Eis		De verbinding voor koppelingen tussen de SaaS applicatie en andere applicaties of systemen (zowel voor applicaties in het datacenter van de gemeente Utrecht als koppelingen met andere SaaS applicaties) moet 'end to	Borgen vertrouwelijkheid en integriteit.	Https moet voldoen aan HTTP over een met TLS beveiligde verbinding. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC , waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
			end' beveiligd te worden d.m.v. encryptie.		geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden.
23	Eis		Bij het opzetten van de verbinding wordt de identiteit van de client en server vastgesteld en gecontroleerd.	Borgen vertrouwelijkheid en integriteit.	Hierbij wordt gebruik gemaakt van tweezijdige TLS, waarbij zowel client als server zich identificeren met een certificaat. TLS moet geconfigureerd zijn conform de recente adviezen, richtlijnen en verdere overwegingen van het NCSC , waarbij er gebruik gemaakt dient te worden van "GOEDE" -instellingen, met uitzondering van daar waar er geen "GOEDE" -instelling beschikbaar is, dient een "VOLDOENDE" -instelling toegepast te worden.
23	Eis		Bestandsoverdracht is beveiligd.	Waarborgen integriteit en vertrouwelijkheid	Er dient minimaal gebruik te worden gemaakt van SFTP met een SSH Key.
24	Wens		Publicatie en autorisatie van afnemers voor API's van de SaaS applicatie kan via het API management platform van de gemeente Utrecht worden uitgevoerd.	Borgen van interoperabiliteit	De gemeente kan API's van de SaaS applicatie centraal, in het API management platform van de gemeente, ontsluiten, in plaats van de API's van iedere SaaS applicatie afzonderlijk ontsluiten. NLX wordt gebruikt voor API's waarbij gegevens van personen of bedrijven worden uitgewisseld. VERVALLEN
25	Eis		Koppelingen van de SaaS applicatie met bij de gemeente Utrecht gehoste applicaties, die gebruik maken van XML en transformatie, verlopen via de ESB van de gemeente Utrecht.	Omwille van Interoperabiliteit	Aansluiten via de Utrechtse Enterprise Service Bus (ESB).
26	Eis		Koppelingen van de SaaS applicatie met applicaties buiten de infrastructuur van de gemeente Utrecht (zoals andere SaaS applicaties of landelijke voorzieningen) verlopen direct van de SaaS applicatie met de voorziening of SaaS applicatie.	Verminderen complexiteit beheer alsmede efficiëntie.	Koppelingen verlopen direct van de SaaS applicatie met de voorziening of SaaS applicatie en dus niet via de infrastructuur van de gemeente Utrecht. De leverancier en de gemeente maken gezamenlijk afspraken met de beheerder van de voorziening of SaaS applicatie.
27	Eis		Als de SaaS applicatie koppelingen heeft met landelijke voorzieningen (bijv. een basisregistratie) en/of SaaS	Borgen traceerbaarheid	De leverancier en de gemeente maken gezamenlijk afspraken met de beheerder van de voorziening of SaaS applicatie.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
			applicaties die door de gemeente Utrecht gebruikt worden, dan identificeren de SaaS applicaties zich namens de gemeente Utrecht.		
28	Eis		Koppelingen van SaaS applicaties naar applicaties die gehost worden in het datacenter van de gemeente Utrecht verlopen altijd via DMZ van de gemeente Utrecht.	Borgen vertrouwelijkheid en integratie, alsmede borgen stabiliteit platformen	De constructie van de applicatie dient hiertoe niet belemmerend te zijn.