

Technische aansluitvoorwaarden SAAS Applicaties

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	6
3	Technische aansluitvoorwaarden	9

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

Afkorting	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 Toelichting op de aansluitvoorwaarden

Dit hoofdstuk bevat de toelichting voor de Gemeente Utrecht voor het gebruik van de aansluitvoorwaarden.

Dit hoofdstuk moet uit het document verwijderd worden als de aansluitvoorwaarden naar een leverancier gestuurd worden.

2.1 Aansluitvoorwaarden zijn maatwerk

De toepassing van de aansluitvoorwaarden is maatwerk!

Zoals in de inleiding beschreven kunnen voor specifieke toepassingen aanvullende aansluitvoorwaarden van toepassing zijn, of kunnen aansluitvoorwaarden juist niet van toepassing zijn.

De algemene stappen voor het bepalen van de aansluitvoorwaarden die van toepassing zijn, zijn:

1. Bepaal het gebruik van de applicatie.
2. Bepaal welke aansluitvoorwaarden van toepassing zijn.
3. Bepaal of de aansluitvoorwaarden een 'Eis' of een 'Wens' zijn.

Aansluitvoorwaarden die niet van toepassing zijn, bijvoorbeeld omdat een applicatie geen koppelingen met andere applicaties heeft, kunnen in de aanbestedingsdocumenten verwijderd worden.

Eis: Raadpleeg een architect van Domstad IT om te bepalen welke aansluitvoorwaarden van toepassing zijn.

2.1.1 Bepaal het gebruik van de applicatie

Het gebruik van de applicatie bepaalt welke aansluitvoorwaarden van toepassing zijn:

- Wordt de applicatie alleen gebruikt door gemeente medewerkers?
- Wordt de applicatie ook gebruikt door inwoners en ondernemers (publieksapplicatie)?
bijvoorbeeld voor het maken van een afspraak of het aanvragen van een product of dienst via het internet
- Heeft de applicatie koppelingen met andere applicaties?

2.1.2 Bepaal welke aansluitvoorwaarden van toepassing zijn

Niet alle aansluitvoorwaarden zijn altijd van toepassing. Naast de indeling uit de voorafgaande paragraaf, zijn, onder andere, de volgende aspecten van belang:

- Het proces dat door de applicatie ondersteund wordt.
- De vertrouwelijkheid van de gegevens die in de applicatie gebruikt worden.
- Beleid, zoals bijvoorbeeld het beleid voor Identity en Access management beleid, informatiebeveiligingsbeleid, de AVG voor verwerking van persoonsgegevens.

Voorbeelden:

- De drempel voor het maken van afspraken voor publieksdienstverlening moet laag zijn. Inwoners hoeven geen gebruik te maken van DigiD.
- Bij het aanvragen van subsidie is van belang dat de identiteit van de aanvrager vastgesteld wordt en dient de aanvrager in te loggen met Digid of eHerkenning.

2.1.3 Bepaal of de aansluitvoorwaarden een 'Eis' of een 'Wens' zijn

De aansluitvoorwaarden zijn een uitwerking beleid van de gemeente Utrecht. Het beleid is uitgewerkt in de onderverdeling van de aansluitvoorwaarden in Eisen en Wensen. Bij de toepassing van de aansluitvoorwaarden moet beoordeeld worden of een aansluitvoorwaarde een 'Eis' of een 'Wens' is:

- Leverancier moeten aan een Eis voldoen, leveranciers die niet aan een Eis kunnen voldoen, vallen af.
- Bij een Wens heeft een leverancier die aan de wens voldoet een '+', leveranciers die niet aan een Wens kunnen voldoen, kunnen nog steeds inschrijven op de aanbesteding.

Bij de bepaling of een voorwaarde een Eis of een Wens is, is het verstandig om bij de oriëntatie of marktverkenning bij potentiële leveranciers te toetsen of ze aan de aansluitvoorwaarden kunnen voldoen. Als een aansluitvoorwaarde een 'Wens' is, dan moet in de kolom 'Punten' het aantal punten ingevuld worden dat de leverancier krijgt als aan de wens voldaan wordt.

NB: Voor het afwijken van de aansluitvoorwaarden die als 'Eis' in dit document zijn opgenomen is, voorafgaand aan de publicatie van de aanbesteding, toestemming van de architectuurboard van de gemeente vereist ('comply or explain').

2.2 Bijlagen bij de aansluitvoorwaarden

De aansluitvoorwaarden verwijzen naar een aantal bijlagen. Deze bijlagen moet bij een aanbesteding in de aanbestedingsdocumenten worden opgenomen.

- ICT Infrastructuur van de gemeente Utrecht;
- Authenticatie en provisioning standaarden;
- Aansluiting op de maildienst van Gemeente Utrecht;
- Richtlijn voor het gebruik van domeinnamen.

Deze bijlagen zijn geen onderdeel van het document met de aansluitvoorwaarden aangezien deze documenten een eigen levenscyclus hebben.

Je vindt de meest recente versie van deze bijlagen op het intranet. De juiste verwijzing naar de bijlagen moet opgenomen worden in de **geel gekleurde cellen in de tabellen van hoofdstuk 3**.

2.3 Informatiebeveiliging en aansluitvoorwaarden

Zoals in de inleiding van dit document beschreven, zijn deze technische aansluitvoorwaarden **geen** vervanging van de eisen ten aanzien van informatiebeveiliging. Deze aansluitvoorwaarden bevatten eisen en wensen die een bijdrage leveren aan het veilig gebruik van een SaaS applicatie.

Voor informatiebeveiliging voor overheidsorganisaties geldt de [Baseline Informatiebeveiliging Overheid \(BIO\)](#). De eisen en maatregelen uit de BIO worden voor de gemeente Utrecht ingevuld met Utrechts beleid voor informatiebeveiliging en daarvan afgeleid beleid zoals het Utrechts beleid voor Identity en Access Management.

De eisen en maatregelen voor informatiebeveiliging voor een aanbesteding worden bepaald door het Utrechtse beleid. Belangrijke factoren zijn:

1. Kenmerken van het bedrijfsproces en de informatie (BIV classificatie):
 - Beschikbaarheid: informatie moet beschikbaar en toegankelijk zijn. Classificatie gaat in op de mogelijke gevolgen als informatie, of een informatie set, niet beschikbaar is.
 - Integriteit: Het in overeenstemming zijn van informatie met de werkelijkheid (informatie is juist, volledig en actueel). Goed beheer van bevoegdheden en mogelijkheden tot muteren, toevoegen, of vernietigen van gegevens voor een gedefinieerde groep gerechtigden is cruciaal voor de integriteit van informatie. Classificatie gaat in op de mogelijke gevolgen wanneer informatie onjuist, onvolledig is of niet actueel is.

- **Vertrouwelijkheid:** De bevoegdheden en mogelijkheden om kennis te nemen van informatie voor een gedefinieerde groep gerechtigden. Classificatie gaat in op de mogelijke gevolgen wanneer informatie in handen komt van derden die hiertoe niet zijn geautoriseerd.

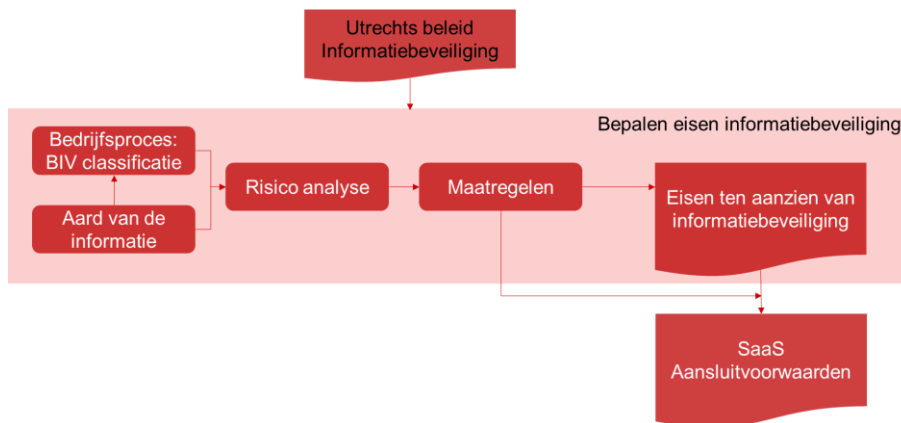
2. De 'aard' van de informatie die verwerkt wordt, voorbeelden:

- **Persoonsgegevens:** Hiervoor geldt de AVG en moet een verwerkersovereenkomst worden afgesloten.
- **Bijzondere persoonsgegevens:** Hiervoor gelden aanvullende eisen.
- **Financiële gegevens.**
- **Concurrentie gevoelige gegevens** (bijvoorbeeld: inschrijvingen van leveranciers voor aanbestedingen).

3. De resultaten van stap 1 en 2 zijn input voor het uitvoeren van een risico analyse om risico's en maatregelen te bepalen.

De maatregelen kunnen resulteren in eisen en wensen ten aanzien van informatiebeveiliging en extra aansluitvoorwaarden.

Eis: Raadpleeg voor het opstellen van de beveiligingseisen voor een aanbesteding de DISO.



Figuur 1: Informatiebeveiliging en aansluitvoorwaarden

2.4 Service Level Agreement en aansluitvoorwaarden

De aansluitvoorwaarden bevatten de eisen en wensen voor het aansluiten en gebruik van SaaS applicaties. Eisen ten aanzien van beschikbaarheid, performance, technische beheer worden beschreven in de eisen ten aanzien van de Service Level Agreement.

Voor de aansluitvoorwaarden is belangrijk dat de SaaS leverancier niet alleen de huidige versie van genoemde normen en standaarden ondersteunt, maar, als onderdeel van het reguliere beheer van de applicatie, ook nieuwe versies van normen en standaarden implementeert en ondersteunt.

3 Technische aansluitvoorwaarden

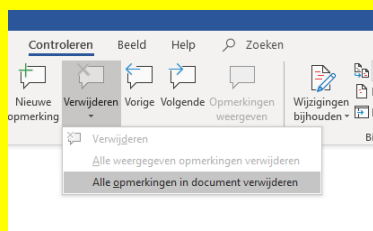
Dit hoofdstuk bevat de aansluitvoorwaarden. De aansluitvoorwaarden worden kort toegelicht met Word opmerkingen.

Nummer	Eis / Wens	Punten	Specificatie
1	Eis		<p>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.</p> <p>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.</p>

Auteur
 Deze eis wordt gesteld om de invulling van de eisen en wensen voor de aansluitvoorwaarden door de leverancier te kunnen verifiëren.
 Het document wordt bij de inschrijving gevraagd omdat de verificatie van de inschrijven een te laat moment in de tijd is om eventuele aansluitvoorwaarden te controleren.

Deze opmerkingen moeten uit het document verwijderd worden als de aansluitvoorwaarden naar een leverancier gestuurd worden.

In Microsoft Word -> Controleren -> Verwijderen -> Alle opmerkingen in document verwijderen



3.1 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		<p>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.</p> <p>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.</p>

Met opmerkingen [A1]: Deze eis wordt gesteld om de invulling van de eisen en wensen voor de aansluitvoorwaarden door de leverancier te kunnen verifiëren.
 Het document wordt bij de inschrijving gevraagd omdat de verificatie van de inschrijven een te laat moment in de tijd is om eventuele aansluitvoorwaarden te controleren.

3.2 Aansluitvoorwaarden

3.2.1 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

3.2.2 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>w</u> e https://applicatie.domeinnaam.nl of <u>n</u> iet 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.
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	Wens		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.

Met opmerkingen [A2]: Deze eis is opgenomen om te voorkomen dat programmatuur op de infrastructuur van de gemeente moet worden geïnstalleerd. Voorbeeld: Bij gebruik van Citrix moet de Citrix client geïnstalleerd worden om alle functionaliteit (bijvoorbeeld printen) van de applicatie mogelijk te maken.

Met opmerkingen [A3]: Let op: Het beveiligingsbeleid van de gemeente staat niet voor iedere applicatie toe dat deze buiten de Utrechtse werkplek wordt gebruikt.

Met opmerkingen [A4]: Afhankelijk van de aard van de gegevens en applicatie

Deze voorwaarde is als Wens opgenomen omdat niet alle leveranciers hieraan kunnen voldoen. Indien noodzakelijk kan van deze Wens een Eis gemaakt worden.

Met opmerkingen [A5]: De redenen zijn (niet uitputtend):

- Plugins moeten in de standaard werkplek worden opgenomen (compatibiliteit met werkplek en overige applicaties, beheer)
- Publieksgebruikers kunnen niet 'verplicht' worden tot installatie van plugins.
- Beveiliging

Met opmerkingen [A6]: De redenen zijn (niet uitputtend):

- Gebruikers van de gemeente kunnen veel instellingen niet zelf aanpassen.
- Aanpassingen moeten in de standaard werkplek worden opgenomen (compatibiliteit met werkplek en overige applicaties, beheer)
- Beveiliging

Met opmerkingen [A7]: Hier de verwijzing naar de bijlage uit de TEA opnemen.

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	Wens		De database van de SaaS applicatie beschikt over de optie om gegevens versleuteld op te slaan.	Waarborgen van vertrouwelijkheid.	Versleuteling is onderdeel van het database management systeem dat door de SaaS applicatie gebruikt wordt.

Met opmerkingen [A8]: Deze eis wordt gesteld zodat de gemeente:
1) Zelf de beschikbaarheid van belangrijke applicaties kan monitoren en niet alleen van signalering door de leverancier afhankelijk is
2) Mogelijkheid tot controleren van de SLA.

Met opmerkingen [A9]: Bij de verwerking van persoonsgegevens is dit waarschijnlijk een Eis.

3.2.3 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 (v1.3).
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.

Met opmerkingen [A10]: Hier de verwijzing naar de bijlage uit de TEA opnemen.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
			browsers die in gebruik zijn bij gemeente Utrecht.		Zie Bijlage: ICT Infrastructuur gemeente Utrecht (v1.3).
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.
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 van Single Sign On wordt het wachtwoord van gebruikersaccounts niet opgeslagen in de applicatie.	Informatiebeveiliging.	

Met opmerkingen [A11]: Hier de verwijzing naar de bijlage uit de TEA opnemen.

Met opmerkingen [A13]: Hier de verwijzing naar de bijlage uit de TEA opnemen.

Met opmerkingen [A12]: Of SSO verplicht is, is afhankelijk van de BIV classificatie van de applicatie. Raadpleeg het IAM beleid om te bepalen of SSO verplicht is.

3.2.4 Publieksapplicaties

De eisen en wensen zijn van toepassing op publieksapplicaties. De eisen en wensen in deze paragraaf zijn aanvullend op de overige aansluitvoorwaarden.

Met opmerkingen [A14]: Deze voorwaarden zijn van toepassing voor applicaties die door inwoners en ondernemers gebruikt worden.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
18	Eis		De SaaS applicatie ondersteunt, zonder beperking van functionaliteit, de recente versies van alle gangbare browsers zowel op desktop, tablet als telefoon.	Borgen toegankelijkheid en borgen laagdrempelig gebruik.	Rekening houden met compatibiliteit/ondersteuning door gangbare desktop browsers en of mobiele browsers. De applicaties worden ook gebruikt door personen die geen medewerker van de gemeente Utrecht zijn (bijv. sollicitanten).

Met opmerkingen [A15]: Indien vereist moet in de eisen voor de applicatie worden opgenomen dat de applicatie ontworpen is zodat de webpaginas meeschalen met de grootte van het gebruikte scherm. (responsive webdesign, zie: https://nl.wikipedia.org/wiki/Responsive_webdesign).

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
19	Eis		Het dient mogelijk te zijn om op aangeven van Utrecht gebruik te kunnen maken van een willekeurige URL voor het benaderen van de SaaS applicatie.	Gebruiksvriendelijkheid, uitstraling, uniformiteit	De applicatie kan gebruik maken van een domeinnaam die bij een derde geregistreerd is Zie Bijlage Richtlijn domeinnaambeleid Gemeente Utrecht
20	Eis		De SaaS applicatie dient voor identificatie te integreren met DIGID / eIDAS (personen).	Omwille van Interoperabiliteit en waarborgen integriteit	De applicatie beschikt over gecertificeerde koppeling met DIGID en/of eIDAS.
21	Eis		De SaaS applicatie dient voor identificatie te integreren eHerkenning / eIDAS (bedrijven).	Omwille van Interoperabiliteit en waarborgen integriteit	De applicatie beschikt over gecertificeerde koppeling met eHerkenning en/of eIDAS met het vereiste betrouwbaarheidsniveau.

Met opmerkingen [A16]: Een voorbeeld is de werken bij site, deze moet de url werkenbijutrecht.nl gebruiken.

Deze voorwaarde is hier als EIS gedefinieerd. Niet alle leveranciers kunnen aan deze EIS voldoen.

Met opmerkingen [A17]: Redenen:

- 1) Zodat voor de gebruikers duidelijk is dat deze applicaties van de gemeente Utrecht zijn (en niet van een willekeurige leverancier of phishing site).
- 2) De 'branding' van de gemeente, denk aan de 'werkenbijutrecht' site
- 3) Ter voorkoming van misbruik, bijvoorbeeld dat de domeinnaam / site na afloop van het contract nog gebruikt kan worden (datalekken).

Met opmerkingen [A18]: Deze eis is alleen relevant als inwoners / personen moeten inloggen met DIGID zodat hun identiteit vastgelegd wordt.

Met opmerkingen [A19]: Deze eis is alleen relevant als eHerkenning vereist is.

Met opmerkingen [A20]: Deze eisen zijn van toepassing als een SaaS applicatie koppelingen met andere applicaties vereist.

3.2.5 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 end' beveiligd te worden d.m.v. encryptie.	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 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

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
					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.
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 applicaties die door de gemeente Utrecht gebruikt worden, dan identificeren de SaaS applicaties zich namens de gemeente Utrecht.	Borgen traceerbaarheid	De leverancier en de gemeente maken gezamenlijk afspraken met de beheerder van de voorziening of SaaS applicatie.
28	Eis		Koppelingen van SaaS applicaties naar applicaties die gehost worden in het	Borgen vertrouwelijkheid en integratie, alsmede	De constructie van de applicatie dient hiertoe niet belemmerend te zijn.

Met opmerkingen [A21]: Deze Wens is opgenomen zodat API's van de SaaS applicatie centraal, in het API management platform van de gemeente ontsloten kunnen worden, in plaats van dat API's van SaaS applicaties in alle SaaS applicaties afzonderlijk ontsloten moeten worden (complexiteit van beheer).

Met opmerkingen [A22]: Vanuit risico, kosten en beheeraspect verdient het de voorkeur om transformaties door de leverancier van de SaaS applicatie te laten uitvoeren (en beheren).

De gemeente maakt gebruik van een leverancier voor het ontwikkelen en beheer van koppelingen op de ESB (OpenTunnel). Dit heeft invloed op de planning en begroting.

Met opmerkingen [A23]: Koppelingen van SaaS applicaties verlopen direct en niet via de infrastructuur van de gemeente. Redenen zijn (niet uitputtend): performance, robuustheid, betrouwbaarheid, complexiteitsreductie van de koppelingen en lagere beheerinspanning voor de gemeente.

Nr.	Eis / Wens	Punten	Omschrijving	Waarom?	Invulling
			datacenter van de gemeente Utrecht verlopen altijd via DMZ van de gemeente Utrecht.	borgen stabiliteit platformen	