

SaaS aansluitvoorwaarden



Vastgesteld op	Vastgesteld door
27-08-2024	Architectenteam
09-09-2024	MT I&S

Wijzigingshistorie

versie	datum	wie	wat
0.1	13-10-2023	Judy	Voorzet op basis van input Stefan / René
0.2	27-11-2023	Stefan	Aanvulling met AV scan
0.3	04-01-2024	Stefan	Tekstuele aanpassingen, in H2 toegevoegd hoe standaarden moeten worden toegepast
0.4	08-08-2024	Judy & Stefan	Inleiding & context toelichting gebruik.
0.5	15-08-2024	Stefan, Mark, Marco & Judy	Review
1.0	27-08-2024	Architectenteam	1.0 na afstemming met security over relatie MMS
1.1	13-10-2024	Judy	Toelichting 'pas toe leg uit' n.a.v. vragen bij vaststellen document in MT I&S

Inhoudsopgave

1	INLEIDING & GEBRUIK	2
1.1	Documentbeheer	2
1.2	Documentgebruik.....	2
1.2.1	Werkwijze	2
1.3	Scope	2
1.4	Toelichting standaarden	2
	'Pas toe of leg uit'	3
1.5	Toelichting SaaS aansluitvoorwaarden	3
2	SAAS AANSLUITVOORWAARDEN	4

1 Inleiding & gebruik

Er is behoefte aan een set van standardeisen om te gebruiken bij het aanbesteden en implementeren van SaaS-oplossingen bij de Gemeente Groningen. Specificeren is maatwerk. Dit document helpt daarbij; het bevat een basisset van technische eisen¹. Het is bedoeld om te gebruiken bij het aanbesteden en/of implementeren van SaaS-oplossingen bij de Gemeente Groningen.

Dit document vervangt alle eerdere documentatie met betrekking tot SaaS-aansluitvoorwaarden.

1.1 Documentbeheer

- Dit document wordt minstens jaarlijks bijgewerkt.
- De actualiteit van dit document blijkt uit de naamgeving; de documentnaam wordt voorafgegaan met minimaal het jaartal en optioneel het kwartaal:
'[YYYY(QQ)] Aansluitvoorwaarden SaaSoplossingen'
- Controleer altijd of je de actuele versie gebruikt neem bij twijfel contact op met één van de architecten.

1.2 Documentgebruik

- Hoofdstuk 'Inleiding & gebruik' (dit hoofdstuk) is voor intern gebruik.
- Hoofdstuk 2 'ICT-eisen SaaS-oplossingen' vormt de basis voor een document dat als bijlage bij een aanbesteding kan worden verstuurd of als onderdeel in een eisenpakket wordt geïntegreerd.

1.2.1 Werkwijze

Om tot een passende set van eisen te komen:

1. Plan je na het lezen van dit document een overleg in met de bij de aanbesteding / implementatie betrokken ICT-architect.
2. Bespreek je samen met de architect de situatie / gewenste oplossing.

De ICT-architect zorgt vervolgens voor een maatwerk-opsomming van eisen.

1.3 Scope

In de praktijk blijkt dat het begrip 'SaaS' vaak in combinatie met 'Cloud' wordt gebruikt. Dat leidt soms tot verwarring. Het onderscheid tussen Cloud (computing) en SaaS is het onderscheid tussen de manier waarop een software-oplossing wordt geleverd en de infrastructuur waarop die draait.

De scope van dit document met aansluitvoorwaarden betreft software-toepassingen die als dienst via (meestal) internet worden aangeleverd.

Deze aansluitvoorwaarden zijn van toepassing op ICT-diensten of -producten: een dienst of product ingericht om de uitwisseling van gegevens of archivering digitaal te doen verlopen en welke bij aanschaf een waarde vertegenwoordigt van ten minste € 50.000².

1.4 Toelichting standaarden

Hoofdstuk 2 'SaaS aansluitvoorwaarden' bevat standaarden die we binnen de Gemeente Groningen hanteren en waaraan leveranciers zich dienen te conformeren.

De bron van deze eisen is [de website van Forum Standaardisatie](https://www.forumstandaardisatie.nl/pas-toe-leg-uit-beleid).

Het betreft eisen die voor de Nederlandse overheid, óók voor gemeenten, gelden voor de aanschaf van software en diensten. Er is uit deze eisen een selectie gemaakt; een selectie die borgt dat een SaaS-applicatie technisch aansluit op de ICT-omgeving van de Gemeente Groningen.

Een aantal eisen zijn *wettelijke* eisen, omdat ze opgenomen zijn in de zgn. 'streefbeeldafspraken'³ of rechtstreeks in een wet⁴. Deze eisen zijn vanwege het belang er van in de tabel **in rode tekst** weergegeven.

¹ in een volgende versie uit te breiden met functionele eisen aan SaaS-Oplossingen

² Overheidsdefinitie ICT dienst zie: <https://www.forumstandaardisatie.nl/pas-toe-leg-uit-beleid>

³ <https://www.forumstandaardisatie.nl/onderwerpen/veilig-internet/streefbeeldafspraken>

⁴ <https://wetten.overheid.nl/BWBR0048156/2023-07-01>

'Pas toe of leg uit'

Het niet toepassen van de voorgeschreven standaarden mag alleen als een dienst of product in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert of om een andere reden die van bijzonder gewicht is. De afwijking en de reden van afwijking horen uitgelegd te worden. Om dat proces te borgen behoort een dergelijke afwijking via het waiverproces te lopen.

1.5 Toelichting Saas aansluitvoorwaarden

In hoofdstuk 2 worden de Saas-aansluitvoorwaarden getoond in een tabel met deze structuur:

Applicatiefunctie	Verplichte standaard	Aanbevolen standaard	Implementatie

- De kolom 'applicatiefunctie' geeft grofweg aan op welk gebied de standaard van toepassing is.
- De kolommen 'verplichte standaard' en 'aanbevolen standaard' bevatten eisen die voor de Nederlandse overheid, óók voor gemeenten, gelden voor de aanschaf van software en diensten. De bron van deze eisen is [de website van Forum Standaardisatie](#).
 - Verplicht betekent dat het in paragraaf 1.4 toegelichte 'pas toe of leg uit principe' van toepassing is
 - Aanbevolen standaarden zijn niet verplicht maar minstens zo nuttig
- Waar sprake is van zowel een verplichte- als aanbevolen standaard wordt in de kolom 'implementatie' verduidelijkt welke eisen op leveranciers van toepassing zijn. Deze kolom "Implementatie" geeft een gedetailleerder uitwerking van hoe we binnen de Gemeente Groningen uitvoering geven aan de standaarden. Op basis van deze informatie kan een leverancier software implementeren op een manier die past binnen de ICT-omgeving van de Gemeente Groningen. Hier kunnen ook standaarden staan die niet van Forum Standaardisatie afkomstig zijn, maar wel essentieel zijn om een applicatie binnen de gemeente te laten functioneren. Deze kolom begrenst bewust het aantal mogelijke oplossingen en daarmee leveranciers. Stelt een leverancier een oplossing voor die niet in de kolom 'implementatie' voorkomt, dan moet je er van uitgaan dat het voorstel niet uitvoerbaar is binnen de ICT-omgeving van de Gemeente Groningen.

2 SaaS aansluitvoorwaarden

Wettelijke eisen en 'streefbeeldafspraken' zijn in rode tekst weergegeven.

Applicatiefunctie	Verplichte standaard	Aanbevolen standaard	Implementatie
Gegevensintegratie	• OpenAPI Specification 3.0 • REST-API Design Rules 1.0 • NL GOV Assurance Profile for OAuth 2.0	• REST • OData 4.0 • SOAP 1.2	• Koppeling met on premise systemen van gemeente uitsluitend via gemeentelijke (API) gateway. • Transformatie en queueing d.m.v on premise ESB is mogelijk. • SFTP voor bestandsuitwisseling is mogelijk. • Bestanden die aan de gemeente worden aangeboden dienen gecontroleerd te zijn op virussen en andere malware en dienen schoon aangeleverd te worden. • Geen rechtstreekse koppeling (ODBC, JDBC, SQL Net) met databases toegestaan. • Rechtstreekse koppelingen tussen leveranciers onderling zijn (onder voorwaarden) toegestaan.
Authenticatie, autorisatie & SSO	• SAML 2.0	• OIDC, OAuth 2.0 • RBAC • Least privilege	• Vereist is een koppeling met de gemeentelijke Entra ID (Azure AD) op basis van de verplichte of aanbevolen standaarden. • Door deze koppeling wordt tevens voorzien in twee factor authenticatie en single sign-on. • Deze eis impliceert dat een eventuele eigen twee factor authenticatie implementatie van de leverancier uitgeschakeld moet kunnen worden, zodat de 2fa van gemeente gebruikt kan worden.
Identity provisioning	• SCIM 2.0	• Actuele versie MS Graph API	• SCIM d.m.v. Entra ID heeft de voorkeur.
Office-applicaties & Werkplek			• Office 365, Teams, bureaublad versies van Office applicaties zijn beschikbaar. • Windows 10 Enterprise • Citrix XenDesktop VDI • FollowMe printing • In geval van applicaties die over een App beschikken voor smartphones of Tablets, moeten zowel Android als iOS/iPadOS worden ondersteund. • Uitgaande connecties zijn altijd ontkoppeld via forward proxy van gemeente
e-mail	• DKIM • DMARC • SPF • DNSSEC • STARTTLS • DANE	• Exchange webservices	• Mailhosting is alleen on premise beschikbaar, door middel van Microsoft Exchange. • Wanneer als onderdeel van de SaaS applicatie e-mail verzonden moet worden uit naam van de gemeente, dan is dit alleen toegestaan wanneer de leverancier vanuit een eigen e-mailvoorziening de mail verstuurt en verwerkt en daarbij voldoet aan de verplichte standaarden. We stellen hiervoor een subdomein ter beschikking. De mailserver van de leverancier die dit subdomein host, wordt opgenomen in de gemeentelijke SPF records. • Overige vormen van e-mail-integratie (bijvoorbeeld mail-relay) zijn niet toegestaan.
Applicatie	• Voor het gebruik van de applicatie(s) volstaat een HTML5 compliant Web	• Ontwikkeld en ingericht op basis richtlijnen OWASP Top 10, of aantoonbaar gelijkwaardige richtlijnen	• De Google Chrome Enterprise Browser is de standaard browser op gemeentelijke Windows werkplekken. • Geen rechtstreekse koppelingen tussen interne en externe systemen toegestaan. Deze

	Browser (browser onafhankelijk)	Zie: https://owasp.org/www-project-top-ten/ • Webapplicatie-richtlijnen NCSC ⁵	dienen altijd ontkoppeld te zijn via (reverse/forward) proxy server.
Verbinding	• HTTPS • HSTS • TLS 1.2 • TLS 1.3 • DNSSEC • RPKI	• IPv6	• Voor burgers en bedrijven toegankelijke voorzieningen (websites en e-mail) moeten zowel via IPv4 als IPv6 bereikbaar zijn. Applicaties die alleen binnen gemeentelijke netwerk worden ontsloten kunnen volstaan met IPv4. • Verbinding over Internet d.m.v. TLS heeft voorkeur, als alternatief kan een IPsec verbinding over Internet worden gerealiseerd. • Leverancier dient applicatie uitsluitend beschikbaar te maken voor het IP-adres van gemeente, bijvoorbeeld door middel van whitelisting. • (TLS) encryptie ingericht conform wettelijke eisen voor overheden⁶. • RPKI is alleen van toepassing op publieke IP-adressen van IT-systemen van de overheid.
Certificaten		• X509	• Certificaten dienen passend te zijn voor de toepassing. • Conform X509 dient een CRL gepubliceerd te worden. • Beheer conform factsheet “veilig beheer digitale certificaten” van het NCSC⁷ of gelijkwaardig. • Enkel gebruik van publieke PKI's is toegestaan, dus geen self-signed certificaten of gebruik van een eigen CA voor koppelingen van/naar gemeente over publiek Internet. • Geldigheid van een certificaat maximaal 3 jaar.

⁵ <https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties>

⁶ <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>

⁷ <https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten>