ICT beleid – Technische SAAS applicatiecriteria – versie 10.x – 26-01-2024

Gestelde technische eisen aan applicaties (en software services) die buiten de Gemeenschappelijke Regionale ICT infrastructuur Drechtsteden (GRID) gehost (extern/off-premise) worden (SAAS applicaties).

Vooraf

SAAS staat voor software as a service. Drechtsteden ziet iedere applicatie die door een externe leverancier gehost wordt en via internet (of via andere externe netwerken (bijvoorbeeld KPN Lokale Overheid (voorheen Gemnet)) aangeboden wordt als een SAAS variant. Als zodanig kan de SAAS applicatie onderdeel uitmaken van een publieke clouddienst, maar dat hoeft niet.
Deze bijlage "ICT beleid – Technische SAAS applicatiecriteria" is bedoeld als toetsingsdocument voor applicaties (en software services) die gehost (gaan) worden door een externe hosting leverancier (dus geen hosting op de GRID infrastructuur).
Voor applicaties die intern gehost (on-premise) worden op de GRID infrastructuur bestaat er een apart toetsingsdocument (bijlage) "ICT beleid – GRID applicatiecriteria".

Eisen

1 (Eis)	Het benaderen van de SAAS applicatie dient via het HTTPS protocol (de toepassingslaag volgens het TCP/IP model) te geschieden. Andere protocollen voor het benaderen van de SAAS applicatie zijn niet toegestaan.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
2 (Eis)	Communicatie voor het HTTPS protocol dient plaats te vinden over poort 443. Daarbij dient HTTPS te voldoen aan HTTP over TLS (conform IETF RFC 2917), waarbij de versie van HTTP 1.1 is (conform IETF RFC 2730 t/m 2735) en de versie van TLS 1.2 (conform IETF RFC 5246) of TLS 1.3 (conform IETF RFC 8446), waarbij TLS 1.3 de voorkeur heeft. TLS versie 1.2 of 1.3 dient verder geconfigureerd te zijn conform de adviezen, richtlijnen en verdere overwegingen uit het NCSC document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0, 23-04-2019 , waarbij er gebruik gemaakt dient te worden van "GOEDE" instellingen, m.u.v. daar waar er geen "GOEDE" instelling beschikbaar is, daar dient een "VOLDOENDE" instelling toegepast te worden.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
3 (Eis)	De SAAS applicatie dient benaderbaar te zijn via een "fully qualified domain name".
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
4 (Eis)	De SAAS applicatie dient benaderbaar te zijn via IPv4 en IPv6.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
5 (Eis)	Het maken van onderscheid in geleverde functionaliteit aan organisaties/klanten o.b.v. het source IP-adres (van de GRID infrastructuur), waar vandaan de SAAS applicatie benaderd wordt, is niet toegestaan. Ook het maken van onderscheid naar organisaties/klanten o.b.v. het source IP-adres is niet toegestaan.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".

6 (Eis)	Alle gebruikersinterfaces (GUI's) zijn volledig 'webbased' en conformeren zich aan de W3C standaard zonder enige beperking voor wat betreft weergave en functionaliteit (interfaces t.b.v. functioneel beheer vallen hier ook onder).
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
7 (Eis)	Voor de presentatie van de SAAS applicatie aan eindgebruikers (inclusief functioneel beheerders) is het niet toegestaan gebruik te maken van zogenaamde remote desktop, virtual desktop infrastructuur (VDI) en/of server based computing (SBC) technologieën (voorbeelden hiervan zijn o.a. VMware Horizon, Citrix Xenapp en Microsoft remote desktop services). Deze technologieën worden niet als "volledig webbased" beschouwd (zie voorgaande eis).
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
8 (Eis)	Drechtsteden streeft naar browseronafhankelijkheid van SAAS applicaties, daarom dient de SAAS applicatie (voor wat betreft de volledig aangeboden functionaliteit) geschikt te zijn voor het gebruik in de volgende webbrowsers en versies: • Mozilla Firefox versie 68.x en hogere stable releases; • Google Chrome (desktop)versie 72.x en hogere stable releases; • Apple Safari (OS X) versie 12.x en hogere stable releases en (iOS) versie 12.x en hogere stable releases.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
9 (Eis)	Er wordt geen gebruik gemaakt van plug-in componenten (zoals o.a. Microsoft Active X, Microsoft Silverlight, Microsoft ClickOnce, Adobe Flash en Java plug-in[1]). Onder plug-in componenten worden tevens de volgende software verstaan VMware Horizon client, Citrix Receiver en Microsoft remote client.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
10 (Eis)	Voor het functioneren van de SAAS applicatie op het client device en/of in de webbrowser zijn geen verdere instellingen, dan wel installaties (op het client device en/of in de browser) benodigd.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
11 (Eis)	De ICT infrastructuur Drechtsteden (GRID) handelt al het **uitgaande** http en https verkeer af via een zogenaamde forward proxy server (Forcepoint V10000 G4). De SAAS applicatie dient geschikt te zijn om in combinatie met een forward proxy server volledig te functioneren.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
12 (Eis)	De SAAS leverancier accepteert dat goedkeuring tot het gebruik van de SAAS applicatie alleen afgegeven wordt na een technische acceptatietest waarbij nagegaan wordt of de SAAS applicatie, voor wat betreft de volledige functionaliteit, ook daadwerkelijk aan de gestelde eisen in dit document voldoet.
	Geef aan of deze eis wordt geaccepteerd, vul in: "Ja". Indien deze eis niet geaccepteerd wordt vul in: "Nee".

[1] Bedoeld wordt Java-software voor een client-device, ook Java Runtime Environment, Java Runtime, JRE, Java Virtual Machine, Java VM, JVM, Java-uitbreiding of Java-download genoemd.

13 (Eis)	De ICT infrastructuur Drechtsteden (GRID) handelt al het **inkomende** http en https verkeer (geïnitieerd door een systeem op een extern netwerk) af via een zogenaamde reverse proxy server (F5 BIG-IP 4000), hierbij is het vereist dat SNI (https://en.wikipedia.org/wiki/Server_Name_Indication) ondersteunt wordt. Eventuele geautomatiseerde koppeling(en) dienen geschikt te zijn om in combinatie met een reverse proxy server volledig te functioneren. *Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".*
14 (Eis)	Voor authenticatie (uitdrukkelijk wordt hier alleen authenticatie bedoeld) van de gebruiker dient gebruik te worden gemaakt van de Microsoft ENTRA ID (voorheen Azure Active Directory (AAD)) binnen de tenant van Servicegemeente Dordrecht. Dit in de rol van "identity provider" (ook bekend als Identity Assertion Provider). De SAAS applicatie dient dit te bewerkstelligen op basis van SAML v2.0 OF Open ID Connect (gebaseerd op het OAuth 2.0). - SAML v2.0 conform specificatie: https://saml.xml.org/saml-specifications. - Open ID connect gebaseerd op OAuth 2.0 conform framework of specifications (IETF RFC 6749 and 6750). De implementatie dient Microsoft onafhankelijk te zijn, oftewel op basis van één van bovenstaande twee standaarden dient deze omgezet te kunnen worden naar een andere identity provider dan Microsoft. T.a.v. HTTPS dient te worden voldaan aan HTTP over TLS (conform IETF RFC 2917), waarbij de versie van HTTP 1.1 is (conform IETF RFC 2730 t/m 2735) en de versie van TLS 1.2 (conform IETF RFC 5246) of TLS 1.3 (conform IETF RFC 8446), waarbij TLS 1.3 de voorkeur heeft. TLS versie 1.2 of 1.3 dient verder geconfigureerd te zijn conform de adviezen, richtlijnen en verdere overwegingen uit het NCSC document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0, 23-04-2019[2], waarbij er gebruik gemaakt dient te worden van "GOEDE" instellingen, m.u.v. daar waar er geen "GOEDE" instelling beschikbaar is, daar dient een "VOLDOENDE" instelling toegepast te worden. *Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee". Indien deze eis niet van toepassing is vul in: "n.v.t.". Geef tevens aan welke van de twee standaarden zal worden toegepast.*

[2] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

15 (Eis)	Indien er gebruikt wordt gemaakt van één of meerdere geautomatiseerde koppeling(en) tussen de applicatie en één of meerdere andere applicatie(s) en/of syste(e)m(en) dan dienen deze te voldoen aan de volgende eisen: - Voor transport dient de koppeling gebaseerd te zijn op het TCP/IP protocol, zowel IPv4 als IPv6 dient ondersteund te kunnen worden. De implementatie zal momenteel nog onder IPv4 plaatsvinden. - Voor de logistieke communicatielaag dient het verkeer gebaseerd te zijn op het https. - Het https verkeer met applicaties/systemen op een extern netwerk dient op poort 443 geconfigureerd te kunnen worden. - Daarbij dient https te voldoen aan HTTP over TLS (conform IETF RFC 2917), waarbij de versie van HTTP 1.1 is (conform IETF RFC 2730 t/m 2735) en de versie van TLS 1.2 (conform IETF RFC 5246) of TLS 1.3 (conform IETF RFC 8446), waarbij TLS 1.3 de voorkeur heeft. - TLS versie 1.2 of 1.3 dient verder geconfigureerd te zijn conform de adviezen, richtlijnen en verdere overwegingen uit het NCSC document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0, 23-04-2019[3], waarbij er gebruik gemaakt dient te worden van "GOEDE" instellingen, m.u.v. daar waar er geen "GOEDE" instelling beschikbaar is, daar dient een "VOLDOENDE" instelling toegepast te worden.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee". Indien deze eis niet van toepassing is (dus als er geen sprake is van geautomatiseerde koppelingen met applicaties/systemen) vul in: "n.v.t.".
16 (Eis)	Indien de SAAS leverancier en/of de SAAS applicatie e-mail gaat verzenden namens één of meerdere e-mail domeinnamen van één van de organisaties van de Drechtsteden[4] dan wel van haar klantorganisatie(s) dan dient de SAAS leverancier hiervoor een mailrelay met de GRID e-mailomgeving te realiseren (dit zodat de Drechtsteden de juiste implementatie van de e-mail beveiligingstandaarden DKIM, SPF en DMARC af kan dwingen). De mail relay dient gebruikt te maken van het SMTP protocol met TLS beveiliging op poort 587. Hierbij geldt: - SMTP conform IETF RFC 5321. - TLS versie 1.2 (conform IETF RFC 5246) of TLS versie 1.3 (conform IETF RFC 8446), waarbij TLS versie 1.3 de voorkeur heeft. - TLS versie 1.2 of 1.3 dient verder geconfigureerd te zijn conform de adviezen, richtlijnen en verdere overwegingen uit het NCSC document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0, 23-04-2019[5] , waarbij er gebruik gemaakt dient te worden van "GOEDE" instellingen, m.u.v. daar waar er geen "GOEDE" instelling beschikbaar is, daar dient een "VOLDOENDE" instelling toegepast te worden. - Voor het mail relay wordt gebruikt gemaakt van een functionele mailbox binnen de GRID omgeving. - Er wordt gebruikt gemaakt van authenticatie op de functionele mailbox.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee". Indien deze eis niet van toepassing is vul in: "n.v.t.".

[3] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

[4] Met de organisaties van de Drechtsteden wordt hier bedoeld één of meerdere gemeenten (en/of onderde(e)l(en) daarvan) die onderdeel zijn van de Drechtsteden en/of de gemeenschappelijke regeling Drechtsteden (en/of onderde(e)l(en) daarvan).

[5] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

17: Beveiligingscriteria SAAS applicatie De beveiligingseisen zijn overgenomen van de NCSC ICT-beveiligingsrichtlijnen voor webapplicaties (te vinden op de NCSC website (www.ncsc.nl): https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties). Het genoemde nummer in de eis verwijst naar het nummer van de richtlijn (en maatregelen) in de NCSC ICT-beveiligingsrichtlijnen (document Richtlijnen versie 2015). In het document Verdieping versie 2015 is een nadere toelichting te vinden.	
17A (Eis)	U/WA.03: De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
17B (Eis)	U/WA.04: De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".
17C (Eis)	U/WA.05: De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.
	Indien aan de eis voldaan wordt vul in: "Ja". Indien niet aan de eis voldaan wordt vul in: "Nee".