Bijlage L - SaaS aansluitvoorwaarden

Applicatiefunctie	Verplichte standaard	Aanbevolen standaard	Implementatie
Gegevensintegratie		• 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 privilige	• 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	• Mogelijkheid tot Identity provsioning is een wens, geen eis. 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 vanuit het gemeentelijke zijn altijd ontkoppeld via de 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 DNS 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 Browser (browser onafhankelijk)	• Ontwikkeld en ingericht op basis richtlijnen OWASP Top 10, of aantoonbaar gelijkwaardige richtlijnen Zie: https://owasp.org/www-project-top-ten/ • Webapplicatie-richtlijnen NCSC[1]	• De Google Chrome Enterprise Browser is de standaard browser op gemeentelijke Windows werkplekken. • Rechtstreekse koppelingen tussen interne en externe systemen zijn niet toegestaan. Deze 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 overheden[2]. • 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 NCSC[3] 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.

[1] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
[2] https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
[3] https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-beheer-van-digitale-certificaten