Platform extern vergaderaanbod

Datum rapport	6 november 2026
Kenmerk rapport	
Versie rapport	1.0
Status rapport	Concept

Inhoudsopgave

Inhoudsopgave **2**

Doel van deze bijlage **3**

Architectuurvisie **3**

Architectuurprincipes **3**

Dienstverlening staat centraal 3

Hergebruik boven nieuwbouw 3

Open en uitwisselbaar 3

Gegevens bij de bron 4

Veilig en verantwoord 4

Verwachtingen ten aanzien van landschapsinpassing **5**

Domeinnamen, bereikbaarheid en digitale herkenbaarheid 6

Identity & Access Management 6

Communicatievoorzieningen 6

Financiële verwerking 6

Beheer en rapportage 7

Integratiestrategie 7

Verwachtingen ten aanzien van beveiliging en compliance **7**

Doel van deze bijlage

Gemeente Utrecht wil de dienstverlening voor het zoeken, reserveren en administratief afhandelen van externe vergaderlocaties onderbrengen bij één leverancier. De aangeboden oplossing wordt onderdeel van het gemeentelijke applicatielandschap en dient daarom aan te sluiten op bestaande gemeentelijke voorzieningen voor identiteit, communicatie, financiële verwerking en beheer. Het doel van deze bijlage is het beschrijven van de architectuuruitgangspunten en technische randvoorwaarden voor de inpassing van de oplossing binnen het gemeentelijke landschap. De in deze bijlage beschreven uitgangspunten zijn nader uitgewerkt in concrete eisen en wensen in het Programma van Eisen dat onderdeel uitmaakt van het bestek.

Architectuurvisie

Gemeente Utrecht streeft naar een samenhangend applicatielandschap waarin oplossingen zoveel mogelijk gebruik maken van bestaande voorzieningen en open standaarden. Nieuwe oplossingen dienen eenvoudig integreerbaar te zijn, gebruik te maken van gestandaardiseerde interfaces en te passen binnen de gemeentelijke cloudstrategie. De gemeente verwacht dat de aangeboden oplossing:

- onderdeel wordt van het bestaande digitale ecosysteem;
- bestaande gemeentelijke voorzieningen hergebruikt;
- gegevensuitwisseling ondersteunt via standaardkoppelingen;
- geen onnodige maatwerkinterfaces introduceert;
- toekomstbestendig en uitbreidbaar is.

De oplossing dient zich te gedragen als een geïntegreerde dienst binnen het gemeentelijke landschap en niet als een afzonderlijk platform met eigen beheer- en authenticatievoorzieningen.

Architectuurprincipes

De architectuur van Gemeente Utrecht is gebaseerd op een aantal principes die richting geven aan de inrichting van processen, informatievoorziening en technologie. Leveranciers worden geacht deze principes te ondersteunen en waar mogelijk actief te faciliteren.

Dienstverlening staat centraal

De oplossing dient bij te dragen aan een eenvoudige en samenhangende dienstverlening voor medewerkers. Gebruikers moeten de dienstverlening kunnen afnemen vanuit hun bestaande digitale werkomgeving zonder onnodige administratieve handelingen of aanvullende gebruikersregistraties.

Hergebruik boven nieuwbouw

Gemeente Utrecht investeert in generieke voorzieningen voor identiteit, communicatie, beveiliging en beheer. De verwachting is dat de oplossing deze voorzieningen hergebruikt in plaats van vergelijkbare functionaliteit zelfstandig te introduceren.

Open en uitwisselbaar

De gemeente streeft naar een open informatievoorziening waarin gegevens via gestandaardiseerde interfaces kunnen worden uitgewisseld. Afhankelijkheden van leveranciers dienen zoveel mogelijk

beperkt te worden. Daarom hebben open standaarden en gedocumenteerde API's nadrukkelijk de voorkeur.

Gegevens bij de bron

Gegevens worden bij voorkeur beheerd bij de bron en niet onnodig gekopieerd naar andere systemen. Wanneer gegevensuitwisseling noodzakelijk is, dient deze plaats te vinden via gestandaardiseerde en beveiligde interfaces.

Veilig en verantwoord

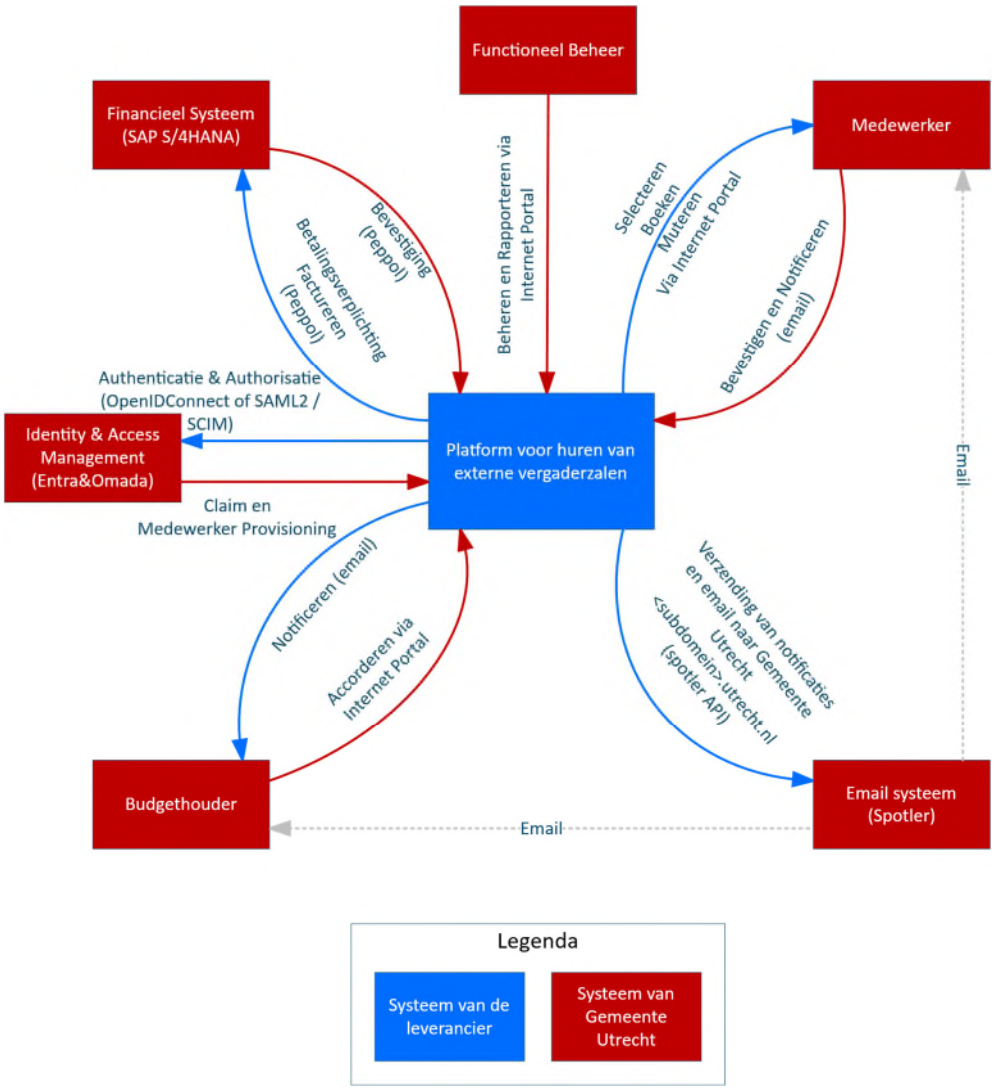
Informatiebeveiliging, privacy en compliance vormen een integraal onderdeel van de dienstverlening. De gemeente verwacht dat beveiliging en privacy vanaf het ontwerp zijn meegenomen en niet achteraf worden toegevoegd. Uitgangspunten zoals Security by Design, Security by Default, Privacy by Design en Privacy by Default zijn daarbij leidend.

Verwachtingen ten aanzien van landschapsinpassing

Uitgangspunt is dat de oplossing aansluit op de reeds aanwezige gemeentelijke voorzieningen.
De beoogde architectuur bestaat uit integraties met:

Gebied	**Gemeentelijke voorziening**
Identity & Access Management	Microsoft Entra ID
Gebruikersprovisioning	Omada Identity Cloud / SCIM
E-mailvoorziening	Spotler SendPro
Werkplek en e-mail	Microsoft 365
Financiële verwerking	SAP S/4HANA
Beheer	Leverancierspportaal

Deze voorzieningen zijn opgenomen in het doelbeeld van de oplossing.



Figuur 1: Doelbeeld

Domeinnamen, bereikbaarheid en digitale herkenbaarheid

Gemeente Utrecht heeft de voorkeur voor dienstverlening die wordt ontsloten via een door Gemeente Utrecht beheerd domein of subdomein. Indien de leverancier gebruikmaakt van een eigen domein dient gemotiveerd te worden aangegeven waarom een gemeentelijk domein niet mogelijk is en welke maatregelen worden getroffen om herkenbaarheid, beheerbaarheid, veiligheid en continuïteit te waarborgen.

Identity & Access Management

Gemeente Utrecht verwacht dat de oplossing gebruikmaakt van de centrale voorzieningen voor Identity & Access Management. Medewerkers dienen toegang te krijgen met hun bestaande gemeentelijke account zodat één digitale identiteit kan worden gebruikt binnen het volledige applicatielandschap.

De voorkeur gaat uit naar integratie met Microsoft Entra ID voor authenticatie en autorisatie. Voor federatieve authenticatie heeft OpenIDConnect de voorkeur, waarbij SAML 2.0 als alternatief wordt geaccepteerd. Voor geautomatiseerde gebruikersprovisioning heeft ondersteuning van SCIM de voorkeur. Hierdoor kan de gebruikersadministratie centraal worden beheerd en blijven autorisaties synchroon met de gemeentelijke organisatie.

Voorkeursvolgorde:

- OpenIDConnect/Oauth
- SAML 2.0

Voor automatische provisioning van gebruikers wordt de standaard SCIMv2 gebruikt.

Communicatievoorzieningen

De oplossing zal naar verwachting reserveringsbevestigingen, wijzigingen, annuleringen en andere notificaties versturen aan medewerkers en betrokkenen. Gemeente Utrecht verwacht dat hiervoor wordt aangesloten op de gemeentelijke mailvoorzieningen.

Voor geautomatiseerde en transactionele e-mailstromen heeft aansluiting op Spotler SendPro de voorkeur. Dit is binnen de gemeente de standaardvoorziening voor geautomatiseerde e-mailcommunicatie. De leverancier wordt gevraagd inzichtelijk te maken hoe de oplossing op deze voorziening kan aansluiten.

Voorkeursvolgorde:

- Spotler SendPro API
- Spotler SendPro SMTP met TLS 2.1 of hoger aangevuld met IP-Whitelisting

Financiële verwerking

Reserveringen van externe vergaderlocaties leiden tot financiële verplichtingen. Daarom verwacht Gemeente Utrecht dat de oplossing kan samenwerken met het financiële landschap van de gemeente.

De voorkeur gaat uit naar een gestandaardiseerde integratie met SAP S/4HANA voor de verwerking van budgetinformatie, budgethouders, kostenplaatsen, financiële boekingen en factuurafhandeling. Leveranciers dienen aan te geven welke standaardkoppelingen beschikbaar zijn en hoe deze aansluiten op SAP-gebaseerde processen. Gemeente Utrecht heeft de voorkeur voor het gebruik van Peppol.

Beheer en rapportage

De gemeente verwacht dat functioneel beheerders zelfstandig inzicht kunnen verkrijgen in het gebruik van de dienstverlening. De aangeboden oplossing dient daarom te beschikken over adequate beheer- en rapportagefunctionaliteit waarmee onder andere reserveringen, gebruikers, locaties, kosten en gebruiksgegevens kunnen worden geraadpleegd.

Deze functionaliteit wordt aangeboden via een volledig webgebaseerd beheerportaal. Voor het functioneren van de SaaS-applicatie zijn op het client device en/of in een courante webbrowser geen aanvullende instellingen, configuraties of software-installaties noodzakelijk. De SaaS-applicatie maakt geen gebruik van plug-incomponenten. Toegang tot de applicatie via remote display-, virtual desktop- of digitale workspace-software is niet toegestaan.

Integratiestrategie

Gemeente Utrecht geeft de voorkeur aan API-gebaseerde integraties boven bestandsuitwisseling of maatwerkinterfaces. Integraties dienen zoveel mogelijk realtime of near realtime plaats te vinden en gebaseerd te zijn op open standaarden. Bij nieuwe koppelingen heeft de volgende volgorde de voorkeur:

- REST API's gebaseerd op JSON (op basis van de NL API Strategie).
- Gestandaardiseerde SaaS-API's.

De leverancier wordt gevraagd inzicht te geven in de beschikbare API's, documentatie, versiebeheer en mogelijkheden voor toekomstige uitbreiding.

Verwachtingen ten aanzien van beveiliging en compliance

De oplossing dient aantoonbaar te voldoen aan de geldende wet- en regelgeving en aan de gemeentelijke uitgangspunten voor informatiebeveiliging en privacy. Van leveranciers wordt verwacht dat zij aantonen hoe invulling wordt gegeven aan:

- AVG;
- BIO;
- beveiligde gegevensuitwisseling;
- logging en auditing;
- continuïteitsvoorzieningen;
- incidentmanagement;
- toegangsbeveiliging;
- gegevensbescherming.

De gemeente verwacht daarnaast dat gegevens binnen de Europese Economische Ruimte worden verwerkt en dat passende maatregelen zijn getroffen om vertrouwelijkheid, integriteit en beschikbaarheid van gegevens te waarborgen.