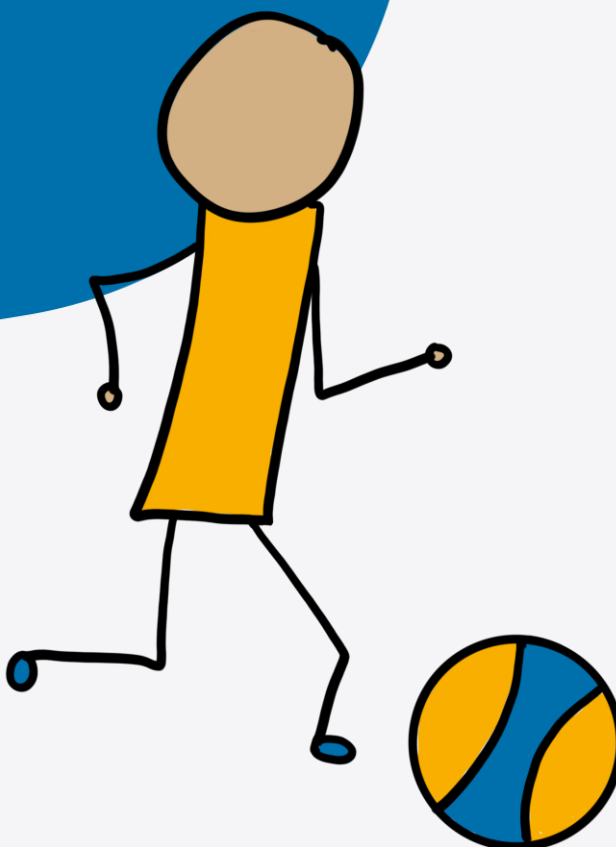


Aansluitvoorwaarden

Eenheid van Dienstverlening
EvD-D Werkplek

Versie: 1.0

Datum: 4-3-2025



Wijzigingshistorie

Dit document valt onder beheer van Werkplek. Dit betekent dat Werkplek zorgt voor aanpassingen waar nodig en het document ter goedkeuring voorlegt.

Werkplek zorgt ervoor dat het document beschikbaar gesteld wordt aan alle belanghebbenden.

Versie	Datum	Bijzonderheden	Auteur
0.1	22-11-2024	Initiële versie	Sogeti Nederland B.V.
0.7	25-11-2024	Interne review	Sogeti Nederland B.V.
0.8	28-11-2024	Initiële versie oplevering	Sogeti Nederland B.V.
0.9	17-01-2025	Oplevering ter goedkeuring	Sogeti Nederland B.V.
0.91	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.
0.92	30-01-2025	Aanpassingen PNH Domeinarchitect verwerkt	Sogeti Nederland B.V.
0.93	17-02-2025	Extra aanpassing PNH Domeinarchitect verwerkt en akkoord	Sogeti Nederland B.V.
0.94	26-02-2025	Applicatie voorwaarden uitgebreid	Sogeti Nederland B.V.
1.0	04-03-2025	WAN vervangen voor verduidelijking. Akkoord door Domein- en Programma-architect.	Sogeti Nederland B.V.

Review en goedkeuring

Naam	Functie	Organisatie	Acceptatie
Saskia de Jager	Domeinarchitect	Provincie Noord-Holland	Verantwoordelijke PNH (Responsible)
Jethro Barreveld	Programma-architect	Provincie Noord-Holland	Goedkeurder (Acceptant)

Verzendlijst

Organisatie	Naam	Rol	0.7	0.8	0.9	0.94	1.0
PNH	Diederik van Tol	Product Owner Werkplek		×	×	×	×
PNH	Ivan Markovic	Service Level Manager			×		×
PNH	Jethro Barreveld	Programma-architect			×	×	×
PNH	Saskia de Jager	Domeinarchitect		×	×	×	×
PNH	Simone Stegers	Programmamanager					×

SOG	Arjan van Vugt	Projectmanager SSW		×	×	×	×
SOG	Dennis van der Linden	Lead Consultant Werkplek	×	×	×	×	×
SOG	Glenn Wesenhagen	Lead Architect	×	×	×	×	×
SOG	Petra van der Kruk	Programmamanager					×
SOG	Roger van der Wiel	Service Manager			×		×

Inhoudsopgave

- Wijzigingshistorie 2
- Review en goedkeuring 2
- Verzendlijst 2
- Inhoudsopgave 4
- 1 Inleiding 5
 - 1.1 Doel 5
 - 1.2 Afbakening 5
 - 1.2.1 Bouwsteen: werkplekategorieën (hardware) 5
 - 1.2.2 Bouwsteen: applicatie-categorieën 5
 - 1.3 Doelgroep 6
 - 1.4 Beheer van document 6
 - 1.5 Gerelateerde documentatie 6
 - 1.6 Werkplek-gerelateerde begrippen 6
- 2 Aansluitvoorwaarden werkplek..... 7
 - 2.1 Bouwsteen: werkplekategorieën (hardware) 7
 - 2.1.1 Wijzigingshistorie 7
 - 2.1.2 Servicebeschrijving (Wat, Wie) 7
 - 2.1.3 Serviceoverzicht (grafisch) 8
 - 2.1.4 Stakeholders van deze bouwsteen 8
 - 2.1.5 Specifieke aansluitvoorwaarden (Hoe) 9
 - Samenvatting: specifieke aansluitvoorwaarden voor hardware 12
 - 2.2 Bouwsteen: Applicaties 13
 - 2.2.1 Servicebeschrijving (Wat, Wie) 13
 - 2.2.2 Serviceoverzicht (grafisch) 14
 - 2.2.3 Stakeholders van deze bouwsteen 14
 - 2.2.4 Aansluitvoorwaarden (Hoe) 15
 - 2.2.5 Applicatiepatronen 21
 - 2.2.6 Koppelvlak 21

1 Inleiding

Dit document, opgesteld door Sogeti Nederland B.V. (Sogeti), beschrijft de aansluitvoorwaarden voor de Managed Workspace die zullen worden gebruikt in de werkomgeving voor Provincie Noord-Holland (PNH). Additionele voorwaarden kunnen toegevoegd worden als het applicatie-landschap verder evolueert door de inzet van nieuwe platformen en technieken.

Binnen de ICT-dienstverlening vervullen de service integratie en systeemintegratie tools van PNH een centrale rol. Deze tools bevatten voor PNH de juiste versie van de gegevens over de ICT-diensten.

1.1 Doel

Dit document heeft als doel om duidelijkheid te verschaffen over aansluitvoorwaarden van zowel de hardware als applicaties voor de werkplek van PNH.

1.2 Afbakening

Dit document beperkt zich tot de aansluitvoorwaarden die gelden voor de inzet van nieuwe hardware en nieuwe applicaties die gebruikt dienen te worden voor de werkplekomgeving van Provincie Noord-Holland.

1.2.1 Bouwsteen: werkplekcategorieën (hardware)

Nieuwe devices dienen te voldoen aan de in dit document gestelde voorwaarden om gebruikt te kunnen worden binnen de beheerde werkomgeving. Op dit moment wordt de inzet van nieuwe devices beperkt tot de volgende hardware typen:

- Windows 10/11 Enterprise Laptop
- Windows 10/11 Enterprise Desktop
- Apple iPhone/iPad
- Google Android
- Microsoft Azure Virtual Desktop (toekomstig)

1.2.2 Bouwsteen: applicatie-categorieën

Nieuwe applicaties dienen te voldoen aan de in dit document gestelde voorwaarden om gebruikt te kunnen worden binnen de beheerde werkomgeving. Op dit moment wordt de inzet van applicaties onderverdeeld in de volgende applicatie-typen:

- Lokale applicaties
- SaaS-applicaties
- Webapplicaties
- Client/Server applicaties

Het aanbieden van applicaties aan de werkplekken is een belangrijk component binnen de Sogeti Smart Workspace (SSW).

1.3 Doelgroep

De doelgroep voor dit document zijn de afnemers gerelateerd aan PNH. Dit betreft de ICT-gebruikers van PNH zelf en van (interne of externe) partners van PNH.

1.4 Beheer van document

Dit document en de hierin beschreven Werkplek-bouwstenen worden beheerd door het PNH Werkplek-team.

Voor informatie betreffende de inhoud van dit document en voor aanvragen en deelname aan de Werkplek-diensten (bouwstenen) die in dit document beschreven zijn kunt u contact opnemen met het Werkplek-team.

1.5 Gerelateerde documentatie

Onderstaande documenten bevatten soortgelijke informatie over aansluitvoorwaarden.

Documentnaam	Locatie	Documenteigenaar
Aansluitvoorwaarden EVD-B (SIAM) *	Nog te bepalen	Sogeti product team

* Indien besloten wordt om de Aansluitvoorwaarden van alle EVD's samen te voegen, kunnen de verwijzingen naar de Aansluitvoorwaarden van andere EVD's hier verwijderd worden.

1.6 Werkplek-gerelateerde begrippen

Deze paragraaf bevat een overzicht van relevante termen en hun definities die worden gebruikt binnen het spectrum van koppelvlakken en aansluitvoorwaarden.

Term	Definitie
ServiceNow	Centrale IT Service Management tool van sommige leveranciers. ServiceNow is als ITSM-tool van Sogeti verbonden met PNH TOPdesk via het Service IntegratiePlatform.
TOPdesk (TD)	Centrale ITSM-tool van PNH. Binnen TOPdesk worden meldingen en wijzigingsverzoeken gelogd door gebruikers of de Service Desk. De meldingen kunnen bestaan uit vragen, opmerkingen, storingen, klachten of algemene verzoeken tot hulp. Wijzigingsverzoeken kunnen door een beperkt aantal personen in PNH ingelegd worden.
DAP	<u>D</u> ossier <u>A</u> fspraken en <u>P</u> rocedures. Dit document heeft als doel de klant inzicht te geven in de diensten die door Sogeti beschikbaar worden gesteld en hen te laten weten hoe en waar ze hun vragen, kennisgevingen en informatie kunnen vinden en sturen. De DAP is onderdeel van het contract tussen PNH en Sogeti.
WPP	<u>W</u> erkafspraken <u>P</u> rocessen & <u>P</u> rocedures. Dit document is een verbijzondering van de DAP, die onderdeel uitmaakt van de dienstverleningsovereenkomst "Cloud- en Werkplekdiensten, inclusief Service- en integratieondersteuning". Dit document beschrijft op tactisch en operationeel niveau de afspraken die worden gemaakt tussen Provincie Noord-Holland en Sogeti en behoren tot de <i>managed service</i> diensten van Sogeti.

2 Aansluitvoorwaarden werkplek

Binnen de aansluitvoorwaarden voor werkplek wordt een onderscheid gemaakt tussen de werkplek zelf (hardware) en de applicaties.

2.1 Bouwsteen: werkplekategorieën (hardware)

2.1.1 Wijzigingshistorie

Versie	Datum	Wijzigingen	Auteur(s)
0.9	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.

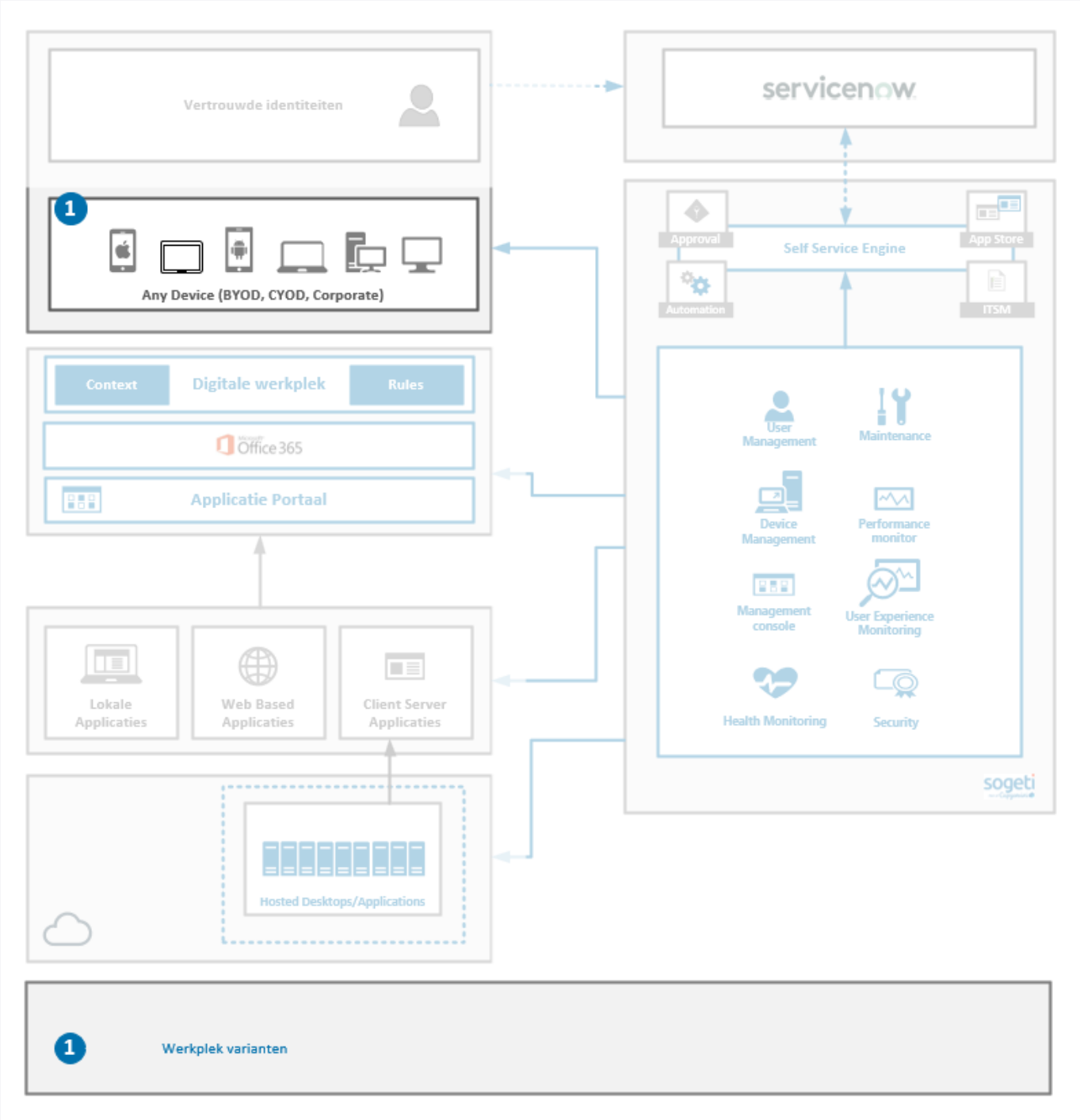
2.1.2 Servicebeschrijving (Wat, Wie)

De werkplek is *het* integratieplatform van de provincie. Binnen deze omgeving komen verschillende ICT-functies bij elkaar en worden beschikbaar gesteld aan eindgebruikers. De werkplek is in te delen in verschillende categorieën c.q. verschijningsvormen. Afhankelijk van deze categorieën zijn voorwaarden van toepassing maar ook welke functionaliteit beschikbaar is. Niet alle functies/ functionaliteiten zijn op alle categorieën beschikbaar.

Voor Provincie Noord-Holland zijn de volgende werkplek typen van toepassing:

1. Windows 10/11 Enterprise Laptop ([paragraaf 2.1.5.1](#))
2. Windows 10/11 Enterprise Desktop ([paragraaf 2.1.5.2](#))
3. Apple iPhone/iPad ([paragraaf 2.1.5.3](#))
4. Google Android ([paragraaf 2.1.5.4](#))
5. Microsoft Azure Virtual Desktop (toekomstig) ([paragraaf 2.1.5.5](#))

2.1.3 Serviceoverzicht (grafisch)



Figuur 1: schematisch overzicht werkplek (hardware) binnen de ICT-dienstverlening van PNH

2.1.4 Stakeholders van deze bouwsteen

De volgende functies binnen PNH zijn stakeholder van deze bouwsteen. In de onderstaande tabel wordt weergegeven welke functie zij bekleden binnen de bouwsteen.

Functie	Organisatie-onderdeel	Afnemer
PO Werkplek	PNH	Nee
Domeinarchitect	PNH	Nee
Productteam	Sogeti	Nee

2.1.5 Specifieke aansluitvoorwaarden (Hoe)

In deze paragraaf worden de specifieke aansluitvoorwaarden voor de vijf verschillende werkplekcategoryen verder uitgewerkt.

2.1.5.1 Windows 10/11 Enterprise Laptop

Binnen Provincie Noord-Holland wordt gebruik gemaakt van laptop en desktop devices op basis van het Windows platform, beheerd door Microsoft Intune. Bij de selectie van nieuwe devices dient er rekening gehouden te worden met een aantal vereisten op basis van software en hardware. Er zit geen verschil tussen laptop of desktop om opgenomen te worden binnen Sogeti Smart Workspace (SSW).

Standard user versus heavy user

Binnen de provincie zijn twee typen hardware in omloop: een voor de *standard user* en de zogenaamde *heavy user*. Dat beide varianten andere requirements hebben is vanuit een aansluitvoorwaardenperspectief niet relevant. Voor werkplek worden slechts de minimale requirements gesteld om binnen Sogeti Smart Workspace (SSW) opgenomen te kunnen worden.

2.1.5.1.1 Hardware requirements

Voor de levering van hardware wordt er uitgegaan van systemen op basis van compatible x64 processoren welke voldoen aan de minimale eisen van Windows 11 24H2 (ARM wordt vooralsnog niet ondersteund).

Hoewel Microsoft minimale eisen aangeeft voor het draaien van Windows 11, kan een goede gebruikerservaring niet gegarandeerd worden van een systeem dat alleen aan deze minimale eisen voldoet.

De uiteindelijke hardware-specificaties zijn afhankelijk van het gebruiksdoel van de devices, maar dienen voldoende ruim gedimensioneerd te zijn om probleemloos het OS en de basis applicaties te kunnen draaien. Voor nieuwe devices worden de volgende minimale specificaties aangehouden om een goede gebruikerservaring te garanderen.

Bij de selectie van nieuwe apparaten voor standard of heavy users dienen tevens de geadviseerde hardware-eisen voor de applicaties meegenomen worden.

De volgende aangepaste minimale eisen worden aangehouden voor Provincie Noord-Holland:

Hardware	Requirement
Processor	Recente x64 processor uit huidige of voorgaande generatie. Windows 11 supported AMD processors Windows 11 supported Intel processors
RAM	16 gigabytes (GB).
Opslag	256 GB of groter (NVMe) SSD.
System Firmware	UEFI, Secure Boot capable.

TPM	Trusted Platform Module (TPM) versie 2.0.
Grafische kaart	Compatibel met DirectX 12 of nieuwer met WDDM 2.0-stuurprogramma.
Scherf	High-definition (720p) beeldscherm dat groter is dan 9" diagonaal, 8 bits per kleurkanaal.
Connectiviteit	Laptops dienen voorzien te zijn van een wifi-adapter; desktops dienen voorzien te zijn van een netwerkkaart.

Deze eisen zijn van toepassing op de huidige ondersteunde releases (November 2024), maar zijn aan verandering onderhevig.

2.1.5.1.2 Software requirements

Nieuwe hardware dient uitgeleverd te worden met een vooraf vastgestelde versie van Windows 11 Pro. Op dit moment is de te gebruiken Windows 11 versie vastgesteld op 24H2.

Het Operating System (OS) dient als 'clean image' aangeleverd te worden. Dit wil zeggen dat er geen onnodige applicaties binnen de installatie aanwezig zijn. De aanwezige componenten dienen zich te beperken tot:

- Windows 11 Pro installatie (24H2)
- Applicaties die standaard zijn binnen het Windows platform (bijvoorbeeld Notepad)
- Noodzakelijke drivers;
- Additionele applicaties benodigd voor het beheer van het device.

De installatie dient uitgevoerd te worden met de standaard Windows configuratie (next-next-finish). De gebruikte sources dienen niet ouder te zijn dan drie maanden, waaronder verstaan dient te worden dat de aanwezige updates niet ouder zijn dan drie maanden gerekend vanaf het moment van oplevering.

Overige applicaties, waaronder bijvoorbeeld Microsoft Office dienen geen onderdeel te zijn van de applicaties.

Additionele Windows componenten

Indien noodzakelijk voor de additionele applicaties is het mogelijk en toegestaan om additionele features (waaronder bijvoorbeeld .NET 3.5) als onderdeel van de installatie te activeren.

2.1.5.1.3 Schijfindeling

Bij de indeling van de primaire schijf dient rekening gehouden te worden met een recovery partitie. Deze recovery partitie dient aanwezig te zijn voor het gebruik van de Windows Recovery Environment (WinRE).

2.1.5.1.4 Registratie

Van de uitgeleverde devices dient de hardware hash informatie meegeleverd te worden voor het gebruik van Windows AutoPilot. Deze informatie dient opgeleverd te worden in de vorm van een comma-separated-values (CSV) bestand, welke gebruikt kan worden voor de import binnen Microsoft Intune.

2.1.5.1.5 Licentie

De uitgeleverde devices dienen voorzien te zijn van een Windows 11 Pro (OEM) licentie.

2.1.5.1.6 Security

De onderstaande beveiligingsmiddelen moeten aanwezig en ingeschakeld zijn:

Hardware	Requirement
Secure Boot	Secure Boot vereist firmware die UEFI v2.3.1 Errata B ondersteunt en de Microsoft Windows Certification Authority in de UEFI-handtekeningdatabase heeft.
Trusted Platform Module (TPM)	Alle apparaatmodellen, lijnen of series moeten de Internationale Standaard ISO/IEC 11889:2015 of de Trusted Computing Group TPM 2.0 Library implementeren en naleven. Een component die de TPM 2.0 implementeert moet aanwezig zijn en standaard ingeschakeld zijn.
BitLocker	TPM 2.0 is vereist voor automatische versleuteling tijdens het aansluiten op een Entra ID domein.
Windows Hello	Windows Hello vereist een gespecialiseerde verlichte infraroodcamera voor gezichtsherkenning of irisscan of een vingerafdruklezer die het Windows Biometric Framework ondersteunt. Windows Hello op basis van een pincode kan gebruikt worden bij het ontbreken van deze hardware.
Exploit Guard & Application Control	Recente UEFI-firmware, Secure Boot, TPM 2.0 en ondersteuning voor Virtualization-based security (VBS).

2.1.5.2 [Windows 10/11 Enterprise Desktop](#)

Binnen Provincie Noord-Holland wordt gebruik gemaakt van laptop en desktop devices op basis van het Windows platform, beheerd door Microsoft Intune. Bij de selectie van nieuwe devices dient er rekening gehouden te worden met een aantal vereisten op basis van software en hardware. Er zit geen verschil tussen laptop of desktop om opgenomen te worden binnen Sogeti Smart Workspace (SSW).

2.1.5.3 [Apple iPhone/iPad](#)

Binnen Provincie Noord-Holland wordt er gebruik gemaakt van Apple iPhone en iPad devices beheerd door Microsoft Intune op basis van Mobile Device Management (MDM). Bij de selectie van nieuwe devices dient er rekening gehouden te worden met een aantal vereiste op basis van software en hardware.

2.1.5.3.1 [Hardware requirements](#)

Voor de levering van hardware wordt er uitgegaan van systemen welke voldoen aan de minimale eisen van de meest recente iOS of iPadOS versie.

[Apple security releases - Apple Support](#)

In bovenstaande link is de laatste versie van iOS te vinden.

2.1.5.3.2 [Software Requirements](#)

Nieuwe hardware dient uitgeleverd te worden met de meest recente versie van iOS of iPadOS; op moment van schrijven (februari 2025) is dit iOS/iPadOS 18.3.

2.1.5.3.3 [Apple Business Manager](#)

Nieuwe Apple hardware dient voor uitlevering toegevoegd te worden aan Apple Business Manager (ABM). Vanuit ABM worden de devices gesynchroniseerd met Microsoft Intune voor uitrol.

2.1.5.4 [Google Android](#)

Binnen Provincie Noord-Holland wordt er gebruik gemaakt van Android devices beheerd door Microsoft Intune op basis van Mobile Device Management (MDM). Bij de selectie van nieuwe devices dient er rekening gehouden te worden met een aantal vereiste op basis van software en hardware.

2.1.5.4.1 Hardware requirements

De minimale eis van Microsoft voor Android-apparaten die beheerd kunnen worden door Intune is dat het apparaat draait op Android 5.0 of hoger. De minimale hardware eisen aan Android toestellen zijn afhankelijk van de versie van het aanwezige OS.

Voor Provincie Noord-Holland wordt uitgegaan van een minimale versie van 12.0 of hoger:

Hardware	Requirement
RAM	4 gigabyte (GB)
Opslag	32 gigabyte (GB)*
Processor	Een quad-core 64-bit CPU met een kloksnelheid van minimaal 1,4 GHz
Scherm	Een scherm resolutie van tenminste 720p (1280 x 720 pixels)

* 32GB is slechts de minimale vereiste die noodzakelijk is om binnen SSW opgenomen te kunnen worden.

2.1.5.4.2 Software Requirements

Nieuwe hardware dient uitgeleverd te worden met een ondersteunde versie van Android Enterprise. Op dit moment (februari 2025) worden versies van 12.0 of hoger ondersteund.

Om ondersteuning op langere termijn te garanderen zal voor nieuwe leveringen worden uitgegaan van de nieuwste versie; op moment van schrijven is dit 15.0 of hoger.

2.1.5.4.3 Enrollment

Nieuwe Android devices, welke op basis van Mobile Device Management (MDM) beheerd worden en eigendom zijn van Provincie Noord-Holland, dienen op basis van Zero-Touch deployment uitgerold te kunnen worden.

2.1.5.5 Microsoft Azure Virtual Desktop (toekomstig)

In de volgende fase van het programma wordt dit verder uitgewerkt

Samenvatting: specifieke aansluitvoorwaarden voor hardware

Id	Omschrijving
WCH-1	Werkplekken van PNH dienen gemanaged te kunnen worden vanuit Intune.
WCH-2	Windows 10/11 Enterprise Laptop (2.1.2.1)
WCH-3	Windows 10/11 Enterprise Desktop (2.1.2.2)
WCH-4	Apple iPhone/iPad (2.1.2.3)
WCH-5	Google Android (2.1.2.4)
WCH-6	Microsoft Azure Virtual Desktop (toekomstig) (2.1.2.5)

2.2 Bouwsteen: Applicaties

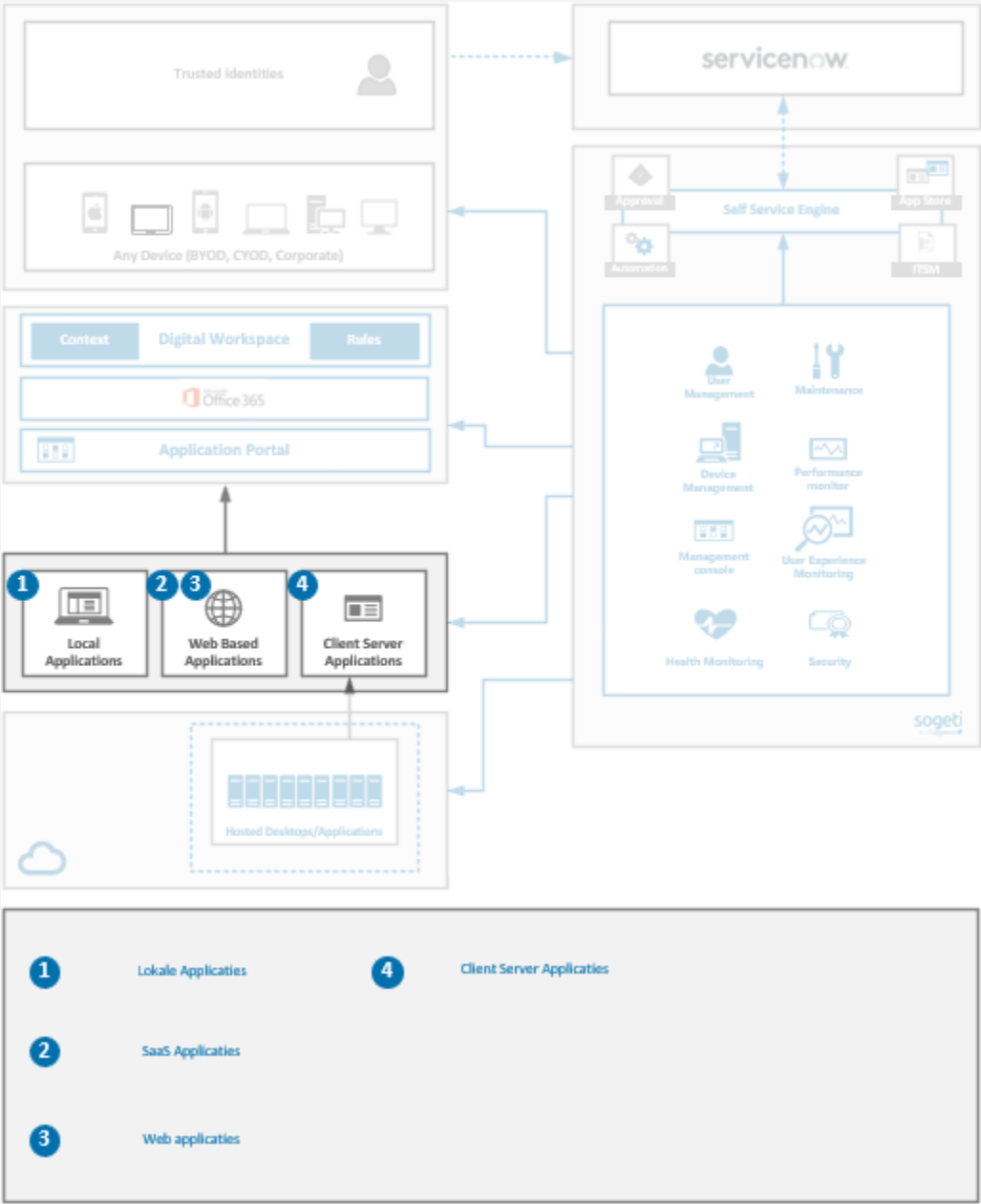
2.2.1 Servicebeschrijving (Wat, Wie)

Er wordt onderscheid gemaakt in een aantal verschillende typen applicaties. Buiten de generieke aansluitvoorwaarden die voor alle applicaties gelden, kunnen er additionele voorwaarden gelden op basis van het type applicatie.

Applicaties worden onderverdeeld in een van de volgende vier categorieën:

- Lokale applicaties ([2.2.4.2.1](#))
- SaaS-applicaties ([2.2.4.2.2](#))
- Webapplicaties ([2.2.4.2.3](#))
- Client/Server applicaties ([2.2.4.2.4](#))

2.2.2 Serviceoverzicht (grafisch)



Figuur 2: schematisch overzicht werkplek (hardware) binnen de ICT-dienstverlening van PNH

2.2.3 Stakeholders van deze bouwsteen

De volgende functies binnen PNH zijn stakeholder van deze bouwsteen. In de onderstaande tabel wordt weergegeven welke functie zij bekleden binnen de bouwsteen.

Functie	Organisatie-onderdeel	Afnemer?
PO Werkplek	PNH	Nee
Domeinarchitect	PNH	Nee
Productteam	Sogeti	Nee

2.2.4 Aansluitvoorwaarden (Hoe)

In dit hoofdstuk worden de aansluitvoorwaarden voor applicaties benoemd. Ongeacht het type applicatie is er een aantal generieke voorwaarden waaraan voldaan moet worden voordat deze op de werkplek beschikbaar gesteld kan worden. Indien het niet mogelijk is om aan deze voorwaarden te voldoen dienen er additionele afspraken en maatregelen getroffen worden om deze applicatie alsnog (tijdelijk) beschikbaar te stellen.

2.2.4.1 Generieke aansluitvoorwaarden

De in deze paragraaf benoemde aansluitvoorwaarden gelden initieel voor nieuwe of aangepaste applicaties. Bij de keuze voor deze applicaties zal bepaald moeten worden of deze aan onderstaande voorwaarden voldoen. Voor bestaande applicaties geldt dat deze na vervanging aan deze voorwaarden dienen te voldoen.

2.2.4.1.1 Applicatieversie

Van applicaties dient een recente versie ingezet te worden. Hierbij wordt een versie van tenminste "N-1" aangehouden.

Buiten het feit dat een recente versie van de applicatie gebruikt wordt, dient deze ook nog door de leverancier ondersteund te zijn. Applicaties dienen op basis van Lifecycle Management (LCM) tijdig vervangen en opgewaardeerd te worden.

Zodra een update beschikbaar komt zal deze na acceptatie gedistribueerd worden naar alle relevante werkplekken.

2.2.4.1.2 Authenticatie

Indien authenticatie noodzakelijk is voor een applicatie, dient hierbij gebruik gemaakt te worden van Entra ID. Door het gebruik van Entra ID kunnen medewerkers veilig toegang kunnen krijgen tot toepassingen, gegevens en services binnen een organisatie.

Het biedt authenticatie- en autorisatiemogelijkheden waarmee medewerkers veilig kunnen inloggen op toepassingen, zowel lokaal als in de Cloud. Hierbij kan er gebruik gemaakt worden van een of meer van de volgende technologieën:

- Single Sign-On (SSO): Een medewerker dient één keer inloggen om toegang te krijgen tot meerdere toepassingen.
- Multi-Factor Authentication (MFA): Medewerker dient een extra factor te gebruiken naast het wachtwoord.
- Federated Authentication: Integratie met externe identiteitsproviders zoals OpenID Connect- of SAML-providers.
- Passwordless Authentication: Authenticatie zonder wachtwoorden, bijvoorbeeld via biometrie (Windows Hello), FIDO2-sleutels, of verificatie via een mobiele app.

2.2.4.1.3 Autorisatie

Applicaties worden alleen aangeboden aan medewerkers die hier gerechtigd voor zijn. Voor persoons of rol gebonden applicaties geldt dat deze geïnstalleerd worden zodra de medewerker zich aanmeldt op een device. Het toekennen van deze applicaties zal op basis van applicatiegroepen plaatsvinden. Door een medewerker in een betreffende groep te plaatsen zal deze de applicatie toegewezen krijgen.

Indien een medewerker niet langer gerechtigd is om een applicatie te gebruiken zal deze van het systeem verwijderd moeten worden. Het op een juiste manier kunnen verwijderen van een applicatie vanuit Microsoft Intune moet tijdens de implementatie meegenomen en getest worden.

2.2.4.1.4 Beheer

Voor een nieuwe applicatie dient het beheer ingeregeld te zijn voordat deze op de werkplek aangeboden kan worden. Hierbij dient de applicatie geregistreerd te zijn en een functioneel beheerder toegewezen en bekend.

De functioneel beheerder is verantwoordelijk voor functionele acceptatie-testen van de applicatie voordat deze in de productie-omgeving wordt toegekend aan de medewerkers. De technische applicatietest wordt gedaan door Sogeti.

2.2.4.1.5 Beschikbaar stellen

Applicaties zullen vanuit Microsoft Intune beschikbaar gesteld worden. Hierbij wordt onderscheid gemaakt in applicaties die voor iedereen beschikbaar zijn, en applicaties die aan een persoon of rol toegekend worden.

Applicaties die voor iedereen beschikbaar dienen te zijn zullen tijdens de uitrol van een nieuw device direct geïnstalleerd worden. De applicaties worden beschikbaar gesteld in het startmenu.

Voor persoons of rol gebonden applicaties geldt dat deze geïnstalleerd worden zodra de medewerker zich aanmeldt op een device. Het toekennen van deze applicaties zal op basis van applicatiegroepen plaatsvinden. Door een medewerker in een betreffende groep te plaatsen zal deze de applicatie toegewezen krijgen.

2.2.4.1.6 Connectiviteit

Applicaties dienen op een veilige manier ontsloten te kunnen worden vanuit of op de werkplek. Voor zowel externe als interne applicaties dient er gebruik gemaakt te worden van zero-trust. Door het gebruik van Zero-trust wordt geen enkele entiteit (gebruiker, apparaat of applicatie) automatisch vertrouwd, ongeacht of deze zich binnen of buiten het netwerk van de organisatie bevindt.

Medewerkers en applicaties dienen alleen toegang te krijgen tot de resources die ze absoluut nodig hebben (Least Privilege).

2.2.4.1.7 Distributie

Voor de distributie van applicaties wordt er gebruik gemaakt van Microsoft Intune. Voor de distributie van applicaties op Windows systemen tijdens de pre-provisioning fase is het van belang dat deze op een consistente manier aangeboden worden. Voor applicaties die een lokaal component hebben wordt er gebruik gemaakt van een "Windows app (Win32)" configuratie.

De gebruikte packaging methode moet geschikt zijn om deze applicatie via een Windows app (Win32) uit te rollen. Hierbij zal gebruik gemaakt worden van de PowerShell App Deployment Toolkit (PSADT).

Voor applicaties die uitsluitend uit een URL bestaan kan er gebruik gemaakt worden van een "Web link".

2.2.4.1.8 Front-end applicatieplatformen

Geselecteerde applicaties dienen gebruik te maken van onderstaande applicatieplatformen. De applicatie moet benaderbaar zijn en gebruikt kunnen worden vanuit een of meerdere van deze platformen.

Platform	N	N-1
Windows Werkplek	- Windows 11 (24H2) - Windows 11 Multi-Session (24H2) - Microsoft Edge (134+) - Google Chrome (132+)	Niet van toepassing ¹
Mobile Werkplek	- Android (Google) laatste versie - iOS (Apple) laatste versie - iPadOS (Apple) laatste versie	Niet van toepassing ¹

2.2.4.1.9 Protocollen

Geselecteerde applicaties dienen gebruik te maken van de onderstaande protocollen.

Platform	LAN/Interne netwerken	Externe netwerken/internet
Bestands uitwisseling	- SFTP - FTPS - HTTPS - SMB 3 (Encrypted)	- SFTP - FTPS - HTTPS - SMB over QUIC
Data uitwisseling	- REST (over https) - SOAP (over https)	- REST (over https) - SOAP (over https)
Authenticatie	- OAuth 2.0 - OpenID Connect (OIDC) - SAML 2.0 (over https) - Kerberos - LDAPs	- OAuth 2.0 - OpenID Connect (OIDC) - SAML 2.0 (over https) - WS-FED(over https; uitzondering)

2.2.4.2 Specifieke aansluitvoorwaarden

Hieronder worden voor de verschillende soorten applicaties de applicatie-specifieke aansluitvoorwaarden aangegeven:

2.2.4.2.1 Lokale applicaties

Versie	Datum	Wijzigingen	Auteur(s)
0.9	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.
0.94	26-02-2025	Voorwaarden lokale applicatie toegevoegd	Sogeti Nederland B.V.

Onder lokale applicaties worden applicaties verstaan die lokaal op een werkplek geïnstalleerd worden en vanuit daar zelfstandig kunnen werken. Deze applicaties kunnen zonder een actieve netwerk of internetverbinding gebruikt worden.

¹ Voor nieuw te selecteren applicaties geldt dat deze de laatste versie van de genoemde platformen moet ondersteunen. Wanneer deze vanuit LCM vervangen worden kunnen ze als N-1 gedefinieerd worden.

Voorbeelden van lokale applicaties zijn: Adobe Reader en 7Zip.

Voorwaarden Lokale applicatie

#	Omschrijving
1	Authenticatie via Entra ID (SSO), indien van toepassing.
2	Compatible met Microsoft Edge of Google Chrome.
3	Compatible met Microsoft 365 Apps.
4	Aanleverformaat op basis van MSI, AppX of MSIX.

2.2.4.2.2 SaaS-applicaties

Versie	Datum	Wijzigingen	Auteur(s)
0.9	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.
0.94	26-02-2025	Voorwaarden SaaS-applicatie toegevoegd	Sogeti Nederland B.V.

SaaS (Software as a Service) is een model voor het leveren van software waarbij applicaties via het internet beschikbaar worden gesteld aan gebruikers, in plaats van dat ze lokaal op een apparaat worden geïnstalleerd. Bij SaaS worden de applicaties gehost en beheerd door een externe serviceprovider en de gebruikers hebben toegang via een webbrowser of een andere clientapplicatie.

Voorbeeld van SaaS-applicatie is: Blue Dolphin

Voorwaarden SaaS-applicatie

#	Omschrijving
1	Authenticatie via Entra ID (SSO).
2	Verkeer encrypted middels TLS (meest recente versie) over http (https).
3	Compatible met Microsoft Edge of Google Chrome.
4	Geen applicatie-specifieke plug-ins.
5	Compatible met Microsoft 365 Apps.
6	Geen interactie met overige applicaties binnen de provinciale infrastructuur behalve wanneer deze internet enabled API's hanteren (m.a.w. geen backchannel communicatie).
7	Authenticatie op basis van Externe netwerk-authenticatie protocollen (§2.2.4.1.9; op basis van Post/Post).
8	User provisioning op basis van SOAP/ REST.

2.2.4.2.3 Webapplicaties

Versie	Datum	Wijzigingen	Auteur(s)
0.9	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.
0.94	26-02-2025	Voorwaarden Webapplicatie toegevoegd	Sogeti Nederland B.V.

Een Webapplicatie is een model voor het leveren van software waarbij applicaties via de browser beschikbaar worden gesteld aan gebruikers, in plaats van dat ze lokaal op een apparaat worden geïnstalleerd. Hoewel deze applicaties veel weg hebben van SaaS wordt het onderscheid gemaakt dat deze applicaties intern gehost en beheerd worden. Over het algemeen zijn deze applicaties alleen intern beschikbaar en is er een verbinding naar het interne netwerk benodigd voor toegang tot de applicatie. Voor externe systemen kunnen deze applicaties alsnog beschikbaar gemaakt worden door het gebruik van een VPN of applicatie proxy.

Voorbeelden van Webapplicaties zijn: FactuurValidatie, IdentityNow

Voorwaarden Webapplicatie

#	Omschrijving
1	Authenticatie via Entra ID (SSO).
2	Verkeer encrypted middels TLS (meest recente versie) over http (https).
3	Compatible met Microsoft Edge of Google Chrome.
4	Geen applicatie-specifieke plug-ins.
5	Compatible met Microsoft 365 Apps.
6	Geen interactie met overige applicaties binnen de provinciale infrastructuur behalve wanneer deze internet enabled API's hanteren (m.a.w. geen backchannel communicatie).
7	Authenticatie op basis van Externe netwerk-authenticatie protocollen (§2.2.4.1.9; op basis van Post/Post).
8	User provisioning op basis van SOAP/ REST.

2.2.4.2.4 Client/Server applicaties

Versie	Datum	Wijzigingen	Auteur(s)
0.9	29-01-2025	Opmaak in lijn gebracht met Aansluitvoorwaarden-document EvD-B SIAM	Sogeti Nederland B.V.
0.94	26-02-2025	Voorwaarden Client/Server-applicatie toegevoegd	Sogeti Nederland B.V.

Onder Client/Server applicaties worden applicaties verstaan die naast een lokale component ook gebruik maken van een centrale server voor het uitvoeren van een applicatie. De centrale servers kunnen hierbij verschillende rollen aannemen, variërend van applicatie- tot databaseservers.

Het onderscheid met de voorgaande categorieën wordt gemaakt door het feit dat er een lokale installatie van een client nodig is en er niet uitsluitend gebruik gemaakt kan worden van een webbrowser. Als het lokale component alleen een browser plug-in betreft worden deze applicaties alsnog onder SaaS of webapplicaties geplaatst.

Over het algemeen zijn deze applicaties alleen intern beschikbaar en is er een verbinding naar het interne netwerk benodigd voor toegang tot de applicatie. Voor externe systemen kunnen deze applicaties alsnog beschikbaar gemaakt worden door het gebruik van VPN technologie.

Voorbeelden van client/server applicaties zijn: RIS SQL, SAP

Voorwaarden Client/Server applicatie

#	Omschrijving
1	Authenticatie via Entra ID (SSO).
2	Verkeer encrypted middels TLS (meest recente versie) over HTTP (HTTPS).
3	Connectie op basis van internet routable DNS.
4	API's zijn gebaseerd op POX, REST of SOAP.
5	Geen applicatie-specifieke plug-ins.
6	Geen interactie met overige applicaties binnen de provinciale infrastructuur behalve wanneer deze internet enabled API's hanteren (m.a.w. geen backchannel communicatie).
7	Alle output, exports, of gecreëerde bestanden via de front-end benaderbaar. Geen shares of bestandsservices die rechtstreeks moeten worden benaderd (behalve via daarvoor geschikte API's).
8	Printing via de PNH Workspace en niet via de server (behalve via daarvoor geschikte API's).
9	Compatible met Microsoft 365 Apps.
10	Authenticatie op basis van Externe netwerk-authenticatie protocollen; LAN protocollen kunnen alleen bij uitzondering gebruikt worden (§2.2.4.1.9).
11	Geen generieke user authenticatie.
12	User provisioning op basis van SOAP/ REST.

In een aantal gevallen kan het noodzakelijk zijn om Client/Server applicaties via een SBC- omgeving aan te bieden. In dit geval kan er gebruik gemaakt worden van een volledige desktop of een RemoteApp configuratie. Hierbij gelden additionele voorwaarden.

Additionele voorwaarden SBC/RemoteApp applicatie

#	Omschrijving
1	Maakt uitsluitend gebruik van de PNH omgeving op basis van Azure Virtual Desktop (toekomstig).
2	Uitsluitend ondersteuning voor RDP-verkeer via HTTPS.
3	Ontsluiting middels een portaal (geen losse RDP files of lokale client configuraties).
4	Federatieve authenticatie op basis van Externe netwerk-authenticatie protocollen (§2.2.4.1.9).
5	Compatible met de laatste client (RDP) release en loopt nooit meer dan 1 client release achter (N-1).

6	Uitsluitend via de PNH werkplek aangeboden en benaderbaar (§2.2.4.1.8).
7	Geen forwarding van lokale resources (printers, lokale disks of netwerk disks).

2.2.5 Applicatiepatronen

Met de overgang van de applicaties naar Microsoft Azure en het gebruik van Entra ID is het mogelijk om nieuwe applicatie patronen te definiëren voor het ontsluiten van nieuwe applicaties.

De applicatiepatronen zijn nog geen onderdeel van de initiële opzet van dit document, maar is als placeholder opgezet.

2.2.6 Koppelvlak

Met de overgang van de applicaties naar Microsoft Azure en het gebruik van Entra ID is het mogelijk om een koppelvlak te definiëren voor het ontsluiten van nieuwe applicaties.

Dit koppelvlak is nog geen onderdeel van de initiële opzet van dit document, maar is als placeholder opgezet.

About Sogeti

Part of the Capgemini Group, Sogeti makes business value through technology for organizations that need to implement innovation at speed and want a local partner with global scale. With a hands-on culture and close proximity to its clients, Sogeti implements solutions that will help organizations work faster, better, and smarter. By combining its agility and speed of implementation through a DevOps approach, Sogeti delivers innovative solutions in quality engineering, cloud and application development, all driven by AI, data and automation.

Capgemini is a global business and technology transformation partner, helping organizations to accelerate their dual transition to a digital and sustainable world, while creating tangible impact for enterprises and society. It is a responsible and diverse group of 340,000 team members in more than 50 countries. With its strong over 55-year heritage, Capgemini is trusted by its clients to unlock the value of technology to address the entire breadth of their business needs. It delivers end-to-end services and solutions leveraging strengths from strategy and design to engineering, all fueled by its market leading capabilities in AI, cloud and data, combined with its deep industry expertise and partner ecosystem. The Group reported 2023 global revenues of €22.5 billion.

Get The Future You Want.
www.capgemini.com

Visit us at www.sogeti.com

This document contains the information that may be the privileged or confidential Group.
Copyright © 2024 Sogeti