



ZaaS farmbeheerhandleiding

HiX/ZaaS

Gepubliceerd: 05 mei 2023

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar worden gemaakt in enige vorm of op enige andere manier, zonder voorafgaande schriftelijke toestemming van ChipSoft B.V.

Alle reacties voor reproductierechten kunnen gericht worden aan: ChipSoft B.V., Orlyplein 10, 1043 DP Amsterdam (tel: +31 20 4939 000).

Ondanks alle aan de samenstelling van deze tekst bestede zorg, kan ChipSoft B.V. geen aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze tekst zou kunnen voorkomen.

© Copyright 2023 ChipSoft B.V.

Inhoudsopgave

1	Inleiding	5
2	Basisbegrippen	6
3	Technische opzet en componenten	8
3.1	Zorgportaal	8
3.2	Kubernetes	8
3.3	Redis cache	8
3.4	HiX Application Services (HAS)	8
3.5	Hybrid ZaaS: ChipSoft Relay Service	9
3.5.1	Configuratie van ChipSoft Relay Service in HAS	9
3.5.2	Configuratie van ChipSoft Relay Service in Zorgportaal	9
3.6	Visuele weergave ZaaS Private Cloud	9
3.7	Visuele weergave ZaaS Hybrid Cloud	10
4	Configuratie	12
4.1	Standaardauthenticatiemethodes en settings	12
4.1.1	Standaardmethodes en -settings toepassen	12
4.2	Secrets	13
4.3	Verbinding met HAS	16
4.4	Huisstijl	16
4.4.1	Custom CSS en JS laden	17
4.5	Custom authenticatiemethodes toevoegen	17
4.6	Aanpassingen in CSP-header	17
4.6.1	Voorbeeldconfiguratie CSP-header	18
4.7	Zorgportaal als iFrame	18
5	Logging en monitoring	20
5.1	Container logs	20
6	Hotfixprocedure	21

7	Gerelateerde documentatie	22
---	---------------------------------	----

1 Inleiding

Deze handleiding beschrijft hoe de variant Zorgportaal as a Service (ZaaS) van Zorgportaal is opgebouwd, hoe deze variant wordt geconfigureerd en hoe deze moet worden beheerd. De handleiding is vooral van toepassing op zorginstellingen die de Private Cloud-variant van Zorgportaal hebben geïmplementeerd.

➔ zie [Basisbegrippen \(p. 6\)](#) voor een uitleg van de begrippen ZaaS en Private Cloud-variant.

Indien een zorginstelling de Hybrid Cloud-variant afneemt bij ChipSoft, geeft deze handleiding vooral wat dieper inzicht in het product.

➔ zie [Basisbegrippen \(p. 6\)](#) voor een uitleg van het begrip Hybrid Cloud-variant.

Daarnaast wordt in deze handleiding expliciet beschreven wat de ChipSoft Relay Service is en hoe deze wordt geconfigureerd.

2 Basisbegrippen

Hieronder staat de betekenis van een aantal begrippen die in dit document worden gebruikt.

ZaaS

ZaaS staat voor 'Zorgportaal as a Service' en wordt gebruikt om de Zorgportaal-versie gebaseerd op containertechnologie aan te duiden. Functioneel is deze Zorgportaal-versie vergelijkbaar met Zorgportaal op SharePoint, maar de onderliggende techniek is volledig anders.

Private Cloud-oplossing

In het geval Zorgportaal als Private Cloud-oplossing wordt afgenomen, is de zorginstelling zelf verantwoordelijk voor het hosten van Zorgportaal op een Kubernetes-cluster. Dit cluster kan een zorginstelling zelf hosten, hosten op een zelfgekozen cloud-platform, of laten hosten door een externe dienstverlener. In alle gevallen is de zorginstelling zelf verantwoordelijk voor het bijhouden van de configuratie en het updaten en monitoren van de omgeving. Ook is de zorginstelling zelf verantwoordelijk voor een eventuele DigiD-audit.

Hybrid Cloud-oplossing

In het geval Zorgportaal als Hybrid Cloud-oplossing wordt afgenomen, draait Zorgportaal in de cloud-omgeving van ChipSoft. ChipSoft beheert en monitort de volledige portaalomgeving. Zorginstellingen kunnen zelf geen configuratie van ZaaS aanpassen. Zorginstellingen kunnen ook geen eigen maatwerk JavaScript of CSS toepassen. ChipSoft verzorgt de DigiD-aansluiting via een TVS-DigiD Clusteraansluiting. ChipSoft verzorgt ook het grootste deel van de DigiD-audit, zoals de pentest.

Kubernetes

Kubernetes is een 'container orchestration platform' en is de aanbevolen wijze voor het hosten van ZaaS.

Containers

ZaaS wordt uitgeleverd als container images. ChipSoft adviseert daarbij te kiezen voor de ZaaS-containers op basis van Linux. Deze containers gebruiken minder resources en zijn dus goedkoper. De container images bevatten alle benodigde software: OS, third-party componenten en de Zorgportaal-software.

Pods

Een pod stuurt een container aan. Indien binnen Kubernetes een container moet worden gestart, gebeurt dat via een pod.

Application Insights (AI)

Application Insights is een tool in Azure om diensten te monitoren. Zorgportaal kan hier goed op aansluiten.

ASP.NET Core

De technologie/framework van Microsoft waarop Zorgportaal is gebaseerd is. ASP.NET.Core is een framework voor webapplicaties.

ASP.NET Core DataProtection

ASP.NET Core DataProtection is een mechanisme van ASP.NET Core, voor de (cryptografische) bescherming van data. Dit mechanisme omvat sleutelbeheer, en rotatie van deze sleutels. Zorgportaal

gebruikt dit voor de bescherming van data, die in Zorgportaal nodig zijn, zoals inlogtokens/cookies/sessiedata.

3 Technische opzet en componenten

Dit hoofdstuk gaat dieper in op de verschillende componenten en hun samenhang.

3.1 Zorgportaal

De ZaaS-variant van Zorgportaal wordt geleverd als Linux-container. ChipSoft gebruikt daarvoor een recente Linux-distributie: Alpine Linux, zie https://hub.docker.com/_/alpine. Zorgportaal is daarnaast gebouwd op Microsoft .NET (momenteel .NET 7) en levert met iedere hotfix in principe de laatste stabiele versie van .NET mee.

De Zorgportaal-containers worden gehost in een Kubernetes-cluster en maken voor het lezen en schrijven van data in HiX verbinding met HiX Application Services (HAS) over een SSL-verbinding.

Zorgportaal slaat zelf geen (medische) data op in de Zorgportaal-omgeving. Data die worden opgeslagen, worden opgeslagen in een Redis cache, zie [Redis cache \(p. 8\)](#). Deze data worden versleuteld.

3.2 Kubernetes

Kubernetes is een 'container orchestration platform' waarmee de Zorgportaal-container kan worden gehost. Kubernetes kan automatisch containers herstarten bij problemen, maar kan eventueel ook opschalen op het moment dat resources krap worden. ChipSoft adviseert Zorgportaal binnen Kubernetes te draaien voor de optimale ervaring.

3.3 Redis cache

Binnen het ZaaS-cluster dient een Redis cache beschikbaar te zijn voor het cachen van data die beschikbaar moeten zijn voor de verschillende pods. Denk hierbij onder andere aan het bewaren van inlogtokens. De zorginstelling is zelf verantwoordelijk voor het opzetten van de Redis cache, eventueel als cluster met meerdere instanties. In Zorgportaal wordt de verbinding met de Redis cache geconfigureerd.

Alle data die ZaaS opslaat in Redis, worden versleuteld. De versleuteling gebeurt op basis van het mechanisme ASP.NET Data Protection. Afhankelijk van het type data, wordt een andere scope gebruikt voor de afgeleide sleutel.

ChipSoft streeft ernaar altijd de laatste versie van Redis te ondersteunen. Momenteel is dat versie 7.x.

3.4 HiX Application Services (HAS)

HiX Application Services (HAS) is de service die data en functionaliteit uit HiX ontsluit en aanbiedt als API/web service.



Zie voor meer informatie over HAS de handleiding 'HiX Application Services Farmbeheer' (CSID-1126847435-241).

3.5 Hybrid ZaaS: ChipSoft Relay Service

In het geval Zorgpoortaal als Hybrid ZaaS-oplossing wordt afgenomen, draait Zorgpoortaal in de cloud-omgeving van ChipSoft, maar staat HAS geïnstalleerd op server(s) bij de zorginstelling, ook wel 'on-prem' genoemd. In deze specifieke situatie maakt Zorgpoortaal geen SSL-verbinding naar het HAS-endpoint, maar verbinden zowel Zorgpoortaal als HAS met de **ChipSoft Relay Service**, die ook gehost wordt in de cloud-omgeving van ChipSoft.

Voor de HAS-en de Zorgportaal-connectie worden specifieke certificaten aangemaakt om een beveiligde verbinding op te zetten. Daarnaast wordt in de configuratie opgenomen welke relay-endpoints moeten worden toegepast.

3.5.1 Configuratie van ChipSoft Relay Service in HAS

Om HAS met de **ChipSoft Relay Service** te laten verbinden, dient op iedere HAS-server een certificaat met private sleutel te worden geïnstalleerd. ChipSoft genereert dit certificaat.

Het service-account waaronder de HAS Host draait, dient leesrechten te hebben op de private sleutel. Daarnaast dient aan het bestand 'chipsoft.platformservices.farm.config' een nieuwe sectie te worden toegevoegd:

```
<relayConnection>
  <connectionId>klantcode-acc</connectionId>
  <certificate>CN=Klant Relay toegangscertificaat</certificate>
</relayConnection>
```

Tussen '`<certificate>`' en '`</certificate>`' moet het subject van het relaycertificaat staan vermeld. Tussen '`<connectionId>`' en '`</connectionId>`' moet de code worden ingevuld die ChipSoft aanlevert en uniek is voor de relay-verbinding.

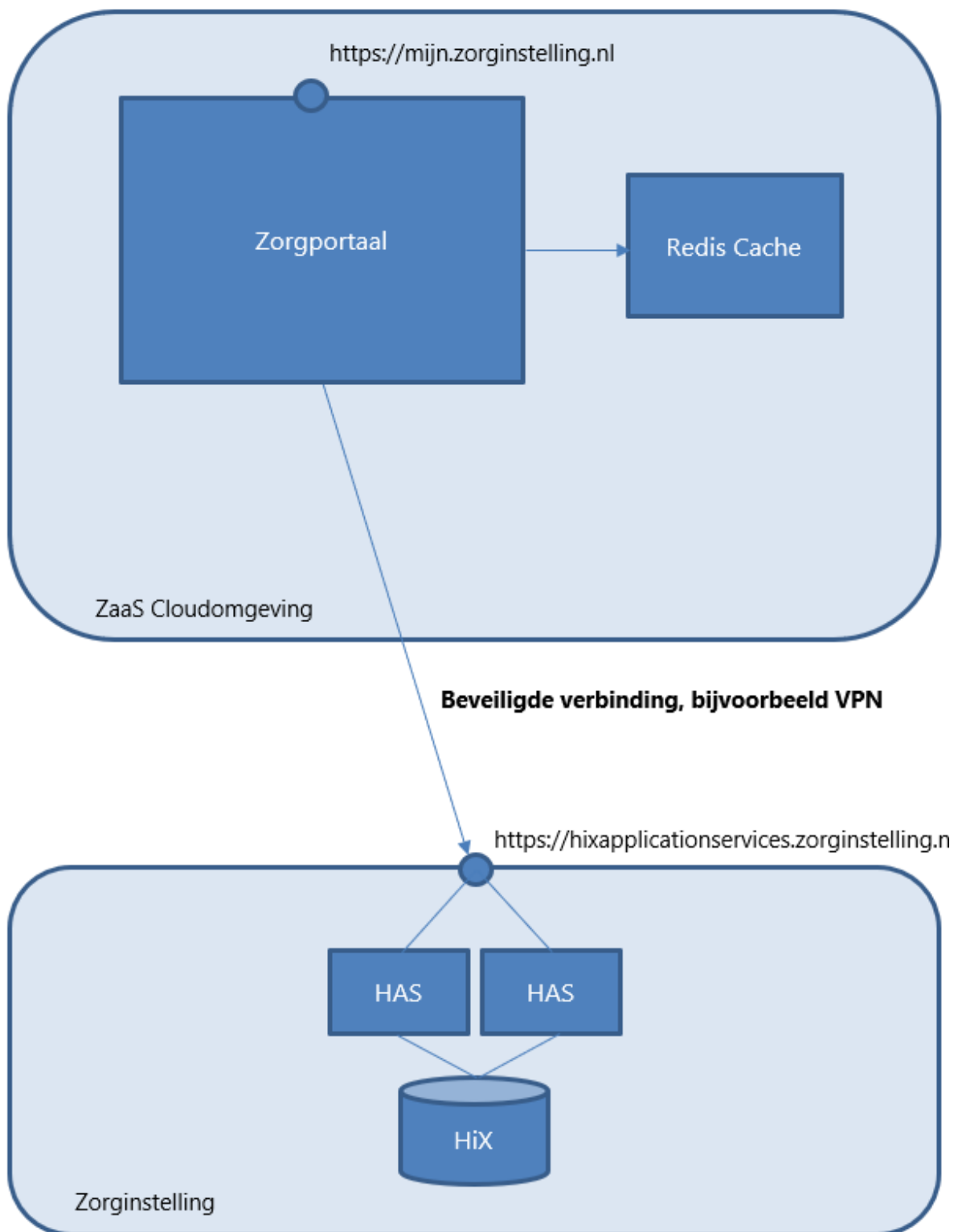
3.5.2 Configuratie van ChipSoft Relay Service in Zorgportaal

In Zorgportaal wordt de connectie met HAS geconfigureerd in het bestand 'CarePortal.*.environment.json'. Bij "hasConnectionType" dient "Relay" te worden ingevuld en het "hasAddress" bevat een lijst aan relay endpoints. "hasCredentials" bevat het certificaat om te authenticeren bij de **ChipSoft Relay Service**. Dit is een eigen, uniek certificaat, dat wordt aangemaakt door ChipSoft.

```
{
  "id": "CUSTOMER-environment-VI",
  "hostname": "MiK_Acceptance",
  "addresses": [ { "addr": "relay01.csrrelay.svc.cluster.local:6000/client/CUSTOMER-acc", "addr": "relay02.csrrelay.svc.cluster.local:6000/client/CUSTOMER-acc" } ],
  "connectionType": "Relay",
  "credentials": {
    "type": "ChipSoft.CsrPortal.Core.MiKEnvironmentRelayAccess, ChipSoft.CsrPortal.Core",
    "certificate": "MIIEGQIBAQCCGCCgSIBzDQENAAOCCEAggggMIIIGqCDBGCSCGCSIBzDQENBgCDBAGwgtAqEAMIIIVZJvXeoZlhwvBAQCBSHSGclqgSIBzDQENAGVwDgQtEKNfioFawIA",
    "certificateProvider": "Blob",
    "stateCertificate": "MIIBIjANBgkqhkiG9w0BAQEFAAACCAQ8AMIIDCgKCAGEAQMIIHic1sh731bzWabb60C2SWivYr2hFTj;FuhoC9yFe2uDShmW/dciHnI12Win/E7+WsUdO6fhgTgQR04GXPhzh"
  },
}
```

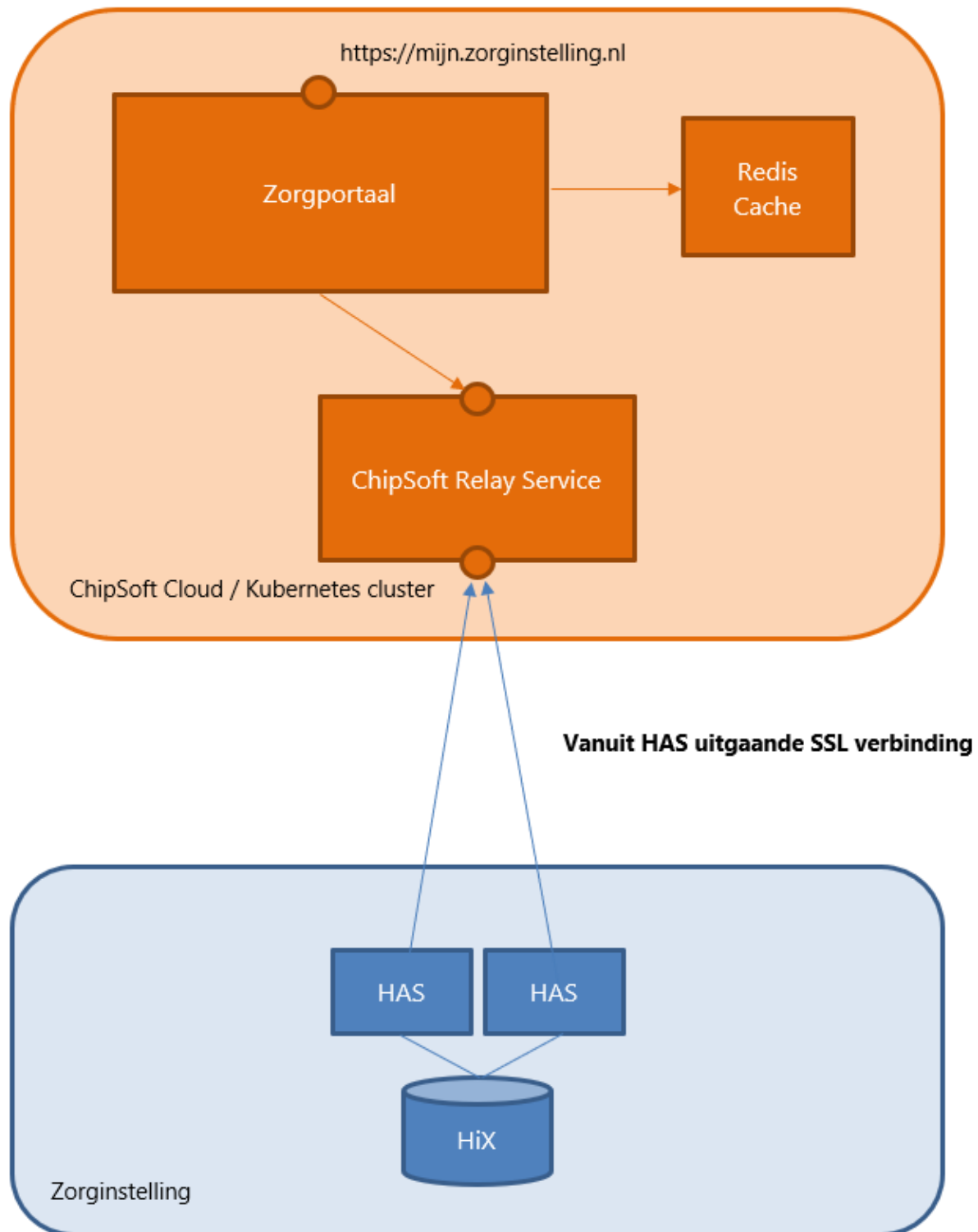
3.6 Visuele weergave ZaaS Private Cloud

Zie hieronder een visuele weergave van ZaaS Private Cloud.



3.7 Visuele weergave ZaaS Hybrid Cloud

Zie hieronder een visuele weergave van ZaaS Hybrid Cloud.



4 Configuratie

De configuratie van ZaaS gebeurt volledig via YAML- en JSON-bestanden.

4.1 Standaardauthenticatiemethodes en settings

ZaaS wordt geleverd als containerimages en een set van configuratiebestanden. In deze configuratiebestanden worden de standaardapplicaties, met bijbehorende standaardauthenticatiemethodes beschreven. Doordat grote delen van de configuratie gestandaardiseerd wordt uitgeleverd, is het voor ChipSoft eenvoudiger nieuwe features en opties standaard uit te rollen bij zorginstellingen.

De standaardapplicaties die worden uitgeleverd, zijn standaard niet actief. Daarvoor dienen de bestanden via het 'portals'-configuratiebestand te worden opgenomen.

Alle standaard authenticatiemethodes worden inactief ('disabled') uitgeleverd. Om ze te activeren dient een zorginstelling-specifieke instelling te worden aangezet en dient de authenticatiemethode in HAS beschikbaar te zijn.

Om deze reden kan ChipSoft niet zomaar applicaties of authenticatiemethodes activeren. Dat zal altijd een keuze van de zorginstelling blijven. Wijzigingen in de standaardconfiguratie worden gedocumenteerd via releasenotes, net zoals dat gebeurt voor wijzigingen in de software.

De bij de hotfix meegeleverde standaardconfiguratiebestanden dienen altijd ook te worden geplaatst bij de uitrol van de hotfix en overschrijven de bestaande bestanden.

➡ Zie voor meer informatie betreffende de installatie van hotfixes het installatiedocument dat bij de ZaaS-huisstijlhotfix wordt meegeleverd. ⚠ Let op: deze is momenteel nog in ontwikkeling.

4.1.1 Standaardmethodes en -settings toepassen

Portalen (portals) worden gedefinieerd in het configuratiebestand 'portals'. Zie hieronder een voorbeeld van een deel van een dergelijk bestand.

```
"Portals": [
  {
    "Id": "Caregiverportal",
    "Name": "Caregiverportal",
    "AppConfig": "/config/CarePortal.caregiverportal.config.json",
    "AppSettings": [
      "/settings/CarePortal.KLANTCODE.caregiverportal.settings.json",
      "/settings/CarePortal.KLANTCODE.environment.json"
    ],
    "ContentConfig": "/content/CarePortal.caregiverportal.content.json"
  }
]
```

Daarbij wordt door de variabele "AppConfig" de standaardconfiguratie van het Zorgverlenersportaal geladen. Deze standaardconfiguratie laadt vervolgens weer een standaardbestand voor

authenticatiemethodes en een bestand met alle standaardwaarden voor de verschillende instellingen, zie onderstaande figuur.

```
"applicationServicesLogFilter": "$applicationServicesLogFilter",
"applicationServicesLogCategoryFilter": "$applicationServicesLogCategoryFilter",
"applicationServicesLogEventFilter": "$applicationServicesLogEventFilter",
"hiXEnvironment": {
  "name": "$hiXName",
  "address": "$hasAddress",
  "connectionType": "$hasConnectionType",
  "credentials": "$hasCredentials",
  "stsCertificate": "$stsCertificate",
  "stsCertificateProvider": "$stsCertificateProvider",
  "compression": "LZ4"
},
"authenticationMethodIncludes": [ "authentication.methods/CarePortal.caregiverportal.authentication.methods.json" ],
"defaultSettings": [ "default.settings/CarePortal.caregiverportal.default.settings.json" ]
}
```

Vervolgens is het mogelijk in een zorginstelling-specifiek settings-bestand 'CarePortal.ZORGINSTELLINGCODE.caregiverportal.settings.json' met minimale configuratie verschillende authenticatiemethodes te activeren, zie onderstaande figuur.

```
{
  "$id": "KLANTCODE-settings-V1",
  "appCertificate": "MIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKggSkAgEAAoIBAQDAYf2TR5C
  "signingKey": "MIIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKggSkAgEAAoIBAQDtTKqXpLGN2Sj
  "objectIdKey": "Nyic0uDCTYe5cmcRRHukHdLFLbfb3zGdYQY2WD1+6YdqwxJjX0v1X9nRPDrWt
  "requestDigestKey": "MrfwoD3j0mv3000jQuj2U28ogUFaySopCvDqeUgM8SDJQ3tSgPL6OEGnl

  "usePageClusters": true,

  "CareplatformEnabled": true,


  "HiXUserEnabled": true,

  "ZorgIDEnabled": true,


  "GeneralPractitionerCenterHospitalZorgIDEnabled": true
}
```

4.2 Secrets

Zorgportaal maakt gebruik van verschillende gegevens die extra beschermt dienen te worden, zoals private delen van certificaten of connectiestrings. Deze kunnen op verschillende manieren binnen de containers beschikbaar worden gemaakt. De meeste configuratieopties volgen een specifiek patroon, in de volgende vorm:

 {Instelling} > Instellingswaarde
 {Instelling}Provider > De manier waarop en waar de daadwerkelijke instellingswaarde wordt opgehaald

Bijvoorbeeld voor de connectiestring voor Redis:

 "RedisServer": "REDIS_CONNECTIONSTRING",
 "RedisServerProvider": "EnvironmentVariable",

Met de provider 'EnvironmentVariable' wordt de instellingswaarde uit een omgevingsvariabele gelezen, met de naam die in de instelling staat. Zo kunnen 'Kubernetes secrets' bijvoorbeeld als 'environment variable' in een container beschikbaar worden gesteld. Op deze manier kan een 'Kubernetes secret' worden gebruikt voor deze specifieke instelling. In het geval geen provider wordt gespecificeerd, is in de meeste gevallen de geconfigureerde waarde de daadwerkelijk geconfigureerde of effectieve instelling.

Voor gevoelige instellingen, zoals certificaten en connectiestring, wordt aangeraden deze niet direct in de configuratie op te nemen, maar deze uit een andere bron te lezen, zoals een Kubernetes secret. De software biedt ondersteuning voor verschillende 'providers' en 'EnvironmentVariable' is daar één van. De software biedt daarnaast ondersteuning voor 'File' (waarde uit een bestand lezen) of 'FileBase64' (waarde als base64 uit een bestand lezen).

Ook is er ondersteuning voor Azure KeyVault. Azure KeyVault is een sleutelbeheeroplossing, aangeboden door Microsoft in Azure. Afhankelijk van het soort instelling, kan Azure KeyVault op verschillende manieren worden gebruikt. Bijvoorbeeld als tekstuele secret in Azure KeyVault door de provider 'AzureKeyVaultSecret' te gebruiken, of als Azure KeyVault beheerd certificaat, met de provider 'AzureKeyVaultCertificate'. Indien gebruik wordt gemaakt van Azure KeyVault, is aanvullende configuratie nodig voor de connectie naar Azure KeyVault.

In het bestand 'CarePortal.global.json' kan dit op de volgende wijze worden geconfigureerd:



```
"AzureKeyVaultSettings": {
  "BaseUrl": "https://kvinstance.vault.azure.net/"
},
"AzureKeyVaultCredentials": {
  "$type": "ChipSoft.CarePortal.Config.AzureCredentials,
ChipSoft.CarePortal.Core",
  "TenantId": "00000000-0000-0000-0000-000000000000",
  "ClientId": "00000000-0000-0000-0000-000000000000",
  "ClientSecret": "00112233-4455-6677-8899-AABBCCDDEEFF"
},
```

Voor bovenstaande waardes is het ook mogelijk andere bronnen te gebruiken, bijvoorbeeld voor het "Clientsecret". Dit kan op de volgende wijze.



```
"ClientSecret": "AzureAdKeyVaultClientSercretEnvironmentVariable "
"ClientSecretProvider": "EnvironmentVariable"
```

Voor de binding van het TLS-certificaat kan dan op de volgende wijze een certificaat uit Azure KeyVault worden gebruikt:



```
"ServerBindings": [
  { "port": 443, "config": {
    "ServerCertificateProvider": "AzureKeyVaultCertificate",
    "ServerCertificate": "zp-tls"
  }
}
```

In het voorbeeld hierboven is 'zp-tls' de naam, het ID, van het certificaat in Azure KeyVault.

Zorgportaal kan worden geïntegreerd met Application Insights (AI). In een dergelijk geval worden logmeldingen naar AI gestuurd. AI biedt verschillende tools waarmee deze data kunnen worden geanalyseerd. Voor de configuratie en het gebruik van AI, dient de AI-connectiestring in het bestand 'CarePortal.global.json' te worden geconfigureerd. Dat kan op de volgende manier:



```
"Logging": {
  // connectiestring zoals deze ook in het Azure Portal bij AI wordt getoond
  "AppInsightsConnectionString": "InstrumentationKey=00000000-0000-0000-0000000000000000;IngestionEndpoint=https://westeurope-0.in.applicationinsights.azure.com/",
  // optioneel, afhankelijk van of AD authenticatie vereist is voor AI
  "AzureCredentials": {
    "$type": "ChipSoft.CarePortal.Config.AzureCredentials, ChipSoft.CarePortal.Core",
    "TenantId": "27d59339-64ab-4595-a1c5-324354244984",
    "ClientId": "e29de841-7f00-4bfe-96d6-949b438e76c1",
    "ClientSecret": "7hSxUw5VIXsuTRjtKBBkNU4XRQ9AK68M96N31to5Dnw="
  }
},
```

Standaard wordt alle log met een niveau van 'Verbose' of hoger naar AI verstuurd. Dit niveau is instelbaar.



```
"Logging": {
  "AppInsightsFilter": "Verbose"
```

Ook kan per categorie het logniveau worden ingesteld. Dit is mogelijk via:



```
"Logging": {
  "AppInsightsCategoryFilter": {
    "CategoryName": "Verbose"
  }
}
```

Het is ook mogelijk specifieke events uit te sluiten of juist te includeren. Dat is mogelijk via:

```

💡 "Logging": {
    "ApplnsightsEventFilter": {
        "EventTag": false
    }
}

```

Met de waarde 'false' worden events uitgesloten en met 'true' worden de events wel gelogd.

4.3 Verbinding met HAS

De verbinding met HAS wordt geconfigureerd in het bestand 'CarePortal.KLANTCODE.environment.json'. HAS moet bereikbaar zijn op het adres dat is ingevuld in de variabele 'hasAddress', zie hieronder.

```

{
  "Sid": "KLANTCODE-environment-V1",
  "hixName": "HiX_Production",
  "hasAddress": "https://hixappservices.klant.nl/externalrouter",
  "stsCertificate": "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApcEModLdkmXDbr3SUPGwMCo0XrFbxOORtK1OWgbrmJ98PLgAWgiC+hAH5FE9rWkuICf213NolksMEID"
}

```

In het geval van Hybrid Cloud is de configuratie afwijkend en worden hier de endpoints van de **ChipSoft Relay Service** opgenomen.

4.4 Huisstijl

De huisstijl, ook wel 'branding' genoemd, van een zorginstelling wordt voorlopig nog als een ziekenhuisspecifieke download aangeboden. In de toekomst verandert dit: de huisstijl, de branding-informatie zoals kleuren en logo's, wordt dan vastgelegd in HiX. Op het moment dat die verschuiving naar HiX is gerealiseerd, is een ziekenhuisspecifieke hotfix voor de huisstijl niet meer nodig.

Tot die tijd dient de huisstijl, nadat deze is uitgeleverd, te worden geïnstalleerd, ook wel 'uitgerold' genoemd. Huisstijlen worden minder vaak uitgeleverd dan 'gewone' hotfixes: in de regel één keer per kwartaal. Een huisstijl wordt uitgeleverd met een hotfixnummer gelijk aan het hotfixnummer van HiX en ZaaS dat minimaal moet zijn geïnstalleerd. Dit betekent dat een huisstijl-hotfix **minimaal** die onderliggende hotfix vereist. Een huisstijl-hotfix 6.3 HF22.0 kan dus draaien op een Zorgportaal met 6.3 HF22.0 en hoger, maar niet op Zorgportaal met 6.3 HF21.0.

De huisstijl wordt als zip-bestand uitgeleverd. Dit zip-bestand kan na het hernoemen van het bestand naar 'branding.zip' direct worden 'gemount' binnen de containers. Het is ook mogelijk het zip-bestand uit te pakken en daarna te mounten, maar deze aanpak heeft niet de voorkeur.

Het bestand 'CarePortal.global.json' dat initieel als voorbeeld wordt aangeleverd, veronderstelt dat het zip-bestand 'branding.zip' op de volgende locatie staat in de container:
/app/AppConfig/branding/branding.zip. Mount op deze plek in de container storage de folder, die het zip-bestand bevat.

➔ Zie voor meer informatie over de installatie van de huisstijl het document 'Installatie-instructies Huisstijl CS-Zorgportaal ZaaS' (CSID-193-4197). Dit document is onderdeel van het zip-bestand dat wordt uitgeleverd bij een huisstijl-hotfix.

4.4.1 Custom CSS en JS laden

Net zoals het in de SharePoint-versie mogelijk was eigen CSS en JavaScript aanpassingen toe te voegen aan het portaal, is dat ook in de ZaaS-versie mogelijk. Hiervoor dienen naast de branding die is gemount is, de volgende bestanden te worden geplaatst:

- <ContainerVolume>\branding\wwwroot\themes\<KlantCode>\<PortaalType>\js\custom.js
- <ContainerVolume>\branding\wwwroot\themes\<KlantCode>\<PortaalType>\css\custom.cs

Het juiste PortaalType (Zorgportaal, Zorgdomein, Kiosk, Queue) is af te leiden uit de bestaande branding-bestanden die zijn geplaatst en door ChipSoft worden geleverd. Aanpassingen aan de bestanden 'custom.js' en 'custom.css' worden door ChipSoft niet overschreven. Aanpassingen binnen deze bestanden zijn volledig onder beheer van de zorginstelling zelf; ChipSoft levert geen support op de inhoud en bij vermoedelijke conflicten met de ChipSoft-branding of scripts kan ChipSoft vragen de inhoud van deze bestanden tijdelijk te wissen.

➔ Zie voor eventueel meer opties rond aanpassingen in CSS het document 'Content ontwikkelen voor ZaaS Private Cloud – Eigen inrichting' (CSID-193-4441).

4.5 Custom authenticatiemethodes toevoegen

Het is mogelijk naast de standaardauthenticatiemethodes volledig zorginstellingspecifieke authenticatiemethodes op te nemen. Deze maatwerkmethodes moeten eerst in HAS worden opgenomen. Vervolgens kan in ZaaS (bij voorkeur) een los bestand voor de authenticatiemethode en een los bestand voor de settings worden opgenomen en geladen via het portal-configuratiebestand.

ChipSoft kan ondersteunen bij de configuratie van zorginstellingspecifieke authenticatiemethodes.

4.6 Aanpassingen in CSP-header

ZaaS probeert de CSP-header zoveel mogelijk automatisch te configureren. Dit betekent bijvoorbeeld dat bij de integratie van PACS-viewers de header op die pagina's wordt aangevuld. Ook in het geval gekoppelde media wordt getoond (in een iFrame), wordt de header automatisch aangevuld.

Toch kan het in uitzonderlijke situaties denkbaar zijn dat toevoegingen aan de standaardoplossing nodig zijn. Het is **niet** mogelijk de ChipSoft standaard CSP-header **niet** toe te passen; het is alleen mogelijk afwijkingen aan de standaard toe te voegen. Deze wijzigingen kunnen per portaal worden ingesteld in de ZaaS-configuratiebestanden.

Mogelijk elementen om aanvullingen te doen zijn:


- frameSrc
- frameAncestors
- connectSrc
- imageSrc
- mediaSrc
- scriptSrc
- fontSrc
- styleSrc

4.6.1 Voorbeeldconfiguratie CSP-header

De CSP-afwijkingen (CSP: Content Security Policy) kunnen worden opgenomen in de settings van een ZaaS-portaal, zie onderstaand voorbeeld:

```
"DigiDEnabled": true,
"DigiDOrganization": "ChipSoft",
"IRMAEnabled": true,
"PatientAccountEnabled": true,
"ReferralEnabled": true,
"TemporaryAccountEnabled": true,
"careplatformSettings": {
  "PublicKeyMode": "Key",
  "PublicKeyProvider": "Base64PKCS8",
  "PublicKey":
},
"contentSecurityPolicyOptions": {
  "connectSrc": ["https://connect.externalapp.nl", "https://connect.zorginstelling.nl"],
  "frameAncestors": ["https://externalapp.zorginstelling.nl"],
  "frameSrc": ["https://embeddedframe.zorginstelling.nl"]
}
```

Effectief leidt dat tot de volgende CSP-responseheader:

 default-src 'none'; script-src 'self' 'sha256-GsiBAplzyJX33owlF3Kn+TqpGwlgGCVVbXV86VP6xzl=' 'sha256-D9/ArJOp+fdB0HlpyNmqlYPkMdenvsDpPbbs6sbb3HE='; connect-src 'self' https://connect.externalapp.nl https://connect.zorginstelling.nl; img-src 'self' data:; style-src 'self' 'sha256-AbpHGcgLb+kRsJGnwFEktk7uzpZOCcBY74+YBdrKVGs='; frame-src 'self' https://embeddedframe.zorginstelling.nl; media-src 'self' data:; font-src 'self' data:; frame-ancestors 'self' https://externalapp.zorginstelling.nl; base-uri 'self'

4.7 Zorgportaal als iFrame

Indien een ZaaS-portaal als iFrame wordt gedraaid, bijvoorbeeld in een 'narrowcasting'-oplossing zoals dat bij Wachtrijportalen gebeurt, dient een aanpassing te worden doorgevoerd om de SameSite-

waarde van de cookies aan te passen. Deze aanpassing kan per access mapping worden doorgevoerd, door het toevoegen van de instelling 'UseSameSiteNoneCookies' met de waarde 'true', zie onderstaand voorbeeld:

```
"Portals": [  
  "Queueportal"  
],  
"InternalUri": "https://preprod-wachtrijmanagement.isala.nl",  
"PublicUri": "https://preprod-wachtrijmanagement.isala.nl",  
"Tag": "intranet",  
"UseSameSiteNoneCookies": true,  
"RequestHeaders": null  
}
```

5 Logging en monitoring

Zorgportaal schrijft zo veel mogelijk logging weg naar HAS. HAS bewaart de logging vervolgens. In HiX 6.2 is dat in een separate monitoringdatabase. In het geval van HiX 6.3 en hoger, wordt de logging opgeslagen in de HiX-databases. Dit is meestal de database HIX_LOGGING.

De log van Zorgportaal en HAS kan vervolgens worden ingezien via een Managementportaal. Daarnaast is het vanaf HiX 6.3 mogelijk log in te zien via HiX: **Menu > Application Services > Log inzage**.

5.1 Container logs

In het geval geen verbinding met HAS kan worden gemaakt, kan het ook voorkomen dat foutmeldingen in de log van een container worden weggeschreven. Daarom adviseert ChipSoft deze container-log te monitoren. Gebruik hiervoor bijvoorbeeld infrastructuur tooling, aangeboden door het gebruikte Kubernetes-platform.

6 Hotfixprocedure

➡ Zie voor meer informatie betreffende de installatie van hotfixes het installatiedocument dat bij de ZaaS-huisstijlhotfix wordt meegeleverd. ⚠ Let op: dit installatiedocument is momenteel nog in ontwikkeling.

7 Gerelateerde documentatie

De volgende documentatie is relevant voor het beheer van Zorgportaal:

- HiX Application Services Farm Beheerhandleiding (CSID-1126847435-241)
- ChipSoft HiX 6.2 server infrastructuur en specificaties (CSID-410-40)
- ChipSoft HiX 6.3 server infrastructuur en specificaties (CSID-410-41)
- In het geval van ZaaS Private Cloud – Eigen Inrichting: Beheer Zorgportaal Sharepoint 2013/2019 (CSID-193-1948)
- Technisch draaiboek certificaatvernieuwing Zorgportaal (CSID-193-2620)
- Installatiehandleiding hotfix ZaaS (volgt nog).