Beveiliging en toegang HubBI

Beveiligingsdocument 2023

HubBI

Inhoudsopgave

Versie 1.1 – april 2023

HubBI in het kort

HubBI is een automatiserings- en integratieplatform op basis van Digital Proces Automation (DPA). Met het platform maak je een proces in AFAS sneller en efficiënter. Daarnaast is HubBI uitermate geschikt om andere systemen te koppelen met AFAS. Tot slot wordt HubBI ingezet voor omvangrijke AFAS conversies.

Redenen om gebruik te maken van HubBI:

- Tijdbesparend
- Continuïteit bedrijfsvoering borgen
- Minder foutgevoelig
- Compliancy is geen uitdaging meer
- Snelle automatische afhandeling
- Een geïntegreerde rekentool
- Laagdrempelig in gebruik

1. Beveiliging HubBI

Bewerkingen die plaatsvinden met HubBI kunnen verschillen, dit is geheel afhankelijk van wat er aan data uitgewisseld moet worden en of dat in AFAS moet gebeuren of tussen AFAS en andere systemen. Omdat het om gevoelige persoonsgegevens kan gaan, loopt dit via een streng beveiligde Microsoft Azure omgeving.
Deze omgeving voldoet aan alle ISO- en NEN-certificeringen die vereist zijn.

Hieronder meer informatie over de beveiliging en certificering vanuit zowel IJK, AFAS als Microsoft via onderstaande deeplinks:

- Microsoft – Compliance
- IJK – Certificeringen
- IJK – Privacy
- AFAS- Architectuur
- AFAS- Security
- AFAS- Certificeringen

2. Toegang HubBI

HubBI draait volledig in de cloud op de Europese servers van Microsoft en alleen op basis van een gebruikersnaam en wachtwoord kan er toegang worden verkregen. Als extra beveiligingsmaatregel is het verplicht om gebruik te maken van twee-factor-authenticatie, ook wel bekend als 2FA. Deze verplichte 2FA-maatregel is sinds begin juni 2023 operationeel.

IJK is hoofdbeheerder van alle accounts en verleent de initiële rechten bij het aansluiten van een nieuwe organisatie. Deze kan vervolgens zelf extra accounts voor medewerkers toevoegen binnen de eigen omgeving.

IJK maakt ook gebruik van de cloud-diensten van Microsoft, Azure en Office365. Alle cloud-diensten van Microsoft en van IJK zijn IS027001 gecertificeerd en voldoen aan de Nederlandse en Europese wet- en regelgeving.

3. Data handling HubBI

Voor de verbinding van HubBI naar AFAS en visa versa wordt er gebruikgemaakt van de REST API van AFAS. In AFAS is alleen data op te halen en in te sturen op basis van een token die in AFAS zelf moet worden aangemaakt door degenen die daar rechten toe hebben binnen AFAS.

https://help.afas.nl/help/NL/SE/App_Cnr_Rest_Api.htm

HubBI kan voor gegevens bewerkingen in AFAS worden gebruikt of tussen AFAS en andere derde partij systemen. Hieronder wordt het verschil tussen de twee typen gegevensbewerkingen schematisch toegelicht.

3.1 Bewerkingen binnen AFAS

Het globale proces ziet er als volgt uit:

Met de AFAS-connectoren kan de gewenste data uit AFAS worden gehaald door middel van GetConnectoren. De gebruiker die toegang heeft tot HubBI bepaalt vervolgens zelf de bewerkingen op de data en stuurt deze data terug naar AFAS door middel van UpdateConnectoren.

3.2 AFAS met behulp van HubBI koppelen met een ander systeem?

Dan geldt hetzelfde principe zoals omschreven in paragraaf 3.1 aangevuld met extra functionaliteit. Het globale proces ziet er als volgt uit:

HubBI kan doormiddel van een API (Application Programming Interface) gegevens uitwisselen met een ander systeem. Een API is een software-interface ofwel internationale koppelstandaard die het mogelijk maakt dat twee applicaties over een beveiligde verbinding met elkaar communiceren. Met een PUT en POST verzoek stuur je data naar het te koppelen softwaresysteem en met een PULL verzoek haal je data op uit een ander systeem. De meeste software leveranciers hebben de eigen data beveiligd en de toegang tot die data ook net zoals AFAS dat ‘token based’ doet. De verbinding die HubBI legt naar een ander pakket gaat via een beveiligd https protocol met daarbovenop aanvullende beveiligingsmaatregelen rondom de API van de desbetreffende derde partij.

Voor de communicatie vanuit HubBI met derde partij systemen via een API ondersteunt HubBI momenteel de volgende aanvullende beveiligingsmaatregelen:

- Geen verificatie: voor gebruik bij bijvoorbeeld openbare API's met publiekelijk toegankelijke gegevens.
- Basisverificatie: de API in kwestie is beveiligd met een gebruikersnaam en wachtwoord.
- API-sleutel: de API is token gebaseerd beveiligd.
- OAuth 2.0: wanneer de internationale en veelgebruikte OAuth 2.0 beveiligingsstandaard van toepassing is. Deze is token gebaseerd en geeft slechts toegang tot een specifieke set van gegevens voor een bepaalde duur. Hierbij hoeft er geen gebruikersnaam en wachtwoord afgegeven te worden wat bijdraagt aan de informatiebeveiliging.
- Certificaat: op het moment dat de gegevens met een certificaat beveiligd en geëncrypt moeten worden. Dit certificaat wordt in overleg tussen twee partijen uitgegeven door de derde partij waar de externe gegevens worden beheerd.

HubBI