

Authenticatie problemen met UZI-pas

Auteur:

Michiel Stoop Bsc, Msc

Identity & Access Management Business Consultant *Traxion*

In mei 2008 heeft NICTIZ het besluit genomen dat zorgverleners van zorgaanbieders toegang krijgen tot het EPD met behulp van authenticatie op basis van één UZI-pas (Unieke Zorgverlener Identificatie). Door dit besluit ligt de verantwoordelijkheid voor toegang tot het Elektronisch patiënten Dossier (EPD) van de zorgverlener via het Goed Beheerd Zorginformatiesysteem (GBZ) bij de zorgaanbieder. Met gevolg dat de zorgaanbieder nu een Identity & Access management (IAM) oplossing moet neer zetten die voldoet aan de door NICTIZ gestelde GBZ eisen. Alle GBZ eisen zijn immers IAM gerelateerd.

Het probleem lag in het feit dat in eerste instantie op de UZI-pas was vastgelegd wie de zorgverlener is en voor welke zorgaanbieder deze werkt. Waardoor de zorgverlener meerdere UZI-passen nodig had wanneer deze voor meerdere zorgaanbieders werkt.

Naar aanleiding van dit probleem heeft NICTIZ in mei 2008 het besluit genomen dat niet meer op de UZI-pas wordt vastgelegd waarvoor de zorgverlener werkt. Zorgverleners hebben dan niet meer meerdere passen nodig, maar één UZI-pas. Het voordeel hiervan is dat de zorgverlener met één UZI-pas bij verschillende zorgaanbieders gebruik kan maken van het GBZ voor het raadplegen van patiëntgegevens.

Doordat op de UZI-pas niet meer is vastgelegd welke zorgverlener gebruik mag maken van het GBZ van een zorgaanbieder. Heeft dit als gevolg dat de zorgaanbieder verantwoordelijk is voor welke zorgverlener toegang krijgt tot het EPD. Door het besluit dat is genomen door NICTIZ is de zorgaanbieder voortaan verantwoordelijk voor het identificeren en authenticeren van de zorgverleners voor toegang tot het EPD via het GBZ. De zorgaanbieder moet hierbij een aantal zaken inregelen om te voldoen aan GBZ eisen en de wet beschermingpersoonsgegevens (WBP), namelijk¹:

- 1) *Administratie van abonneehouders en gastgebruikers*
- 2) *Controleren van abonneehouders en gastgebruikers*
- 3) *Mandateren van abonneehouders en gastgebruikers*
- 4) *Toekennen van toegangsrechten abonneehouders en gastgebruikers tot GBZ*

Door dit besluit wordt de zorgaanbieder gedwongen om bovenstaande beheersmaatregelen te nemen. IAM biedt een oplossing met betrekking tot deze beheersmaatregelen waardoor de zorgaanbieder voldoet aan de GBZ-eisen en WBP.

Welke oplossing kan IAM hierbij aanbieden?

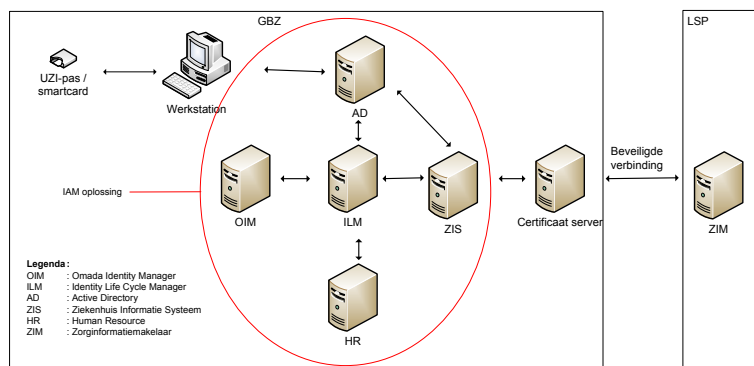
Identity Management is het beheren van identiteiten en de daarbij behorende processen en kenmerken. In dit geval van de zorgverleners wordt de identiteit vastgesteld aan de hand van unieke en persoonsgebonden gegevens op de UZI-pas. Identity management biedt de oplossing voor de zorgaanbieder voor het beheren van de identiteiten van de zorgverleners met betrekking tot identificatie en authenticatie. De abonneehouders en gastgebruikers worden niet meer lokaal vastgelegd in verschillende zorginformatiesystemen van de zorgaanbieder maar centraal. Hiermee wordt het eerste aandachtspunt registratie van abonneehouders en gastgebruikers ingeregeld. Access Management is het beheren van de autorisaties en de daarbij behorende processen en kenmerken van een gebruiker tot een bepaald bronstelsel. Access management biedt de oplossing om de controle, mandatering en toekennen van toegangsrechten voor de zorgverleners tot het GBZ te regelen. Hiermee wordt

¹ Nictiz, Achtergrondnotitie 1 UZI-pas versie 1.0.0.1, 19 juni 2008

aandachtspunten controle, mandatering en toekennen van toegangsrechten van abonneehouders en gastgebruikers ingeregeld. Door het implementeren van een IAM oplossing wordt inzichtelijk gemaakt wie met een bepaalde functie wat mag zien. Dit betekent dat de zorgaanbieder “in control” is en voldoet aan GBZ eisen² door het registreren, controleren, mandateren en toekennen van toegangsrechten op basis van de UZI-passen van zorgverleners.

Hoe ziet bijvoorbeeld een IAM oplossing eruit en hoe werkt het?

In figuur 1 hieronder weergegeven is een voorbeeld gegeven van een IAM oplossing in een interne organisatie.



Figuur 1: IAM oplossing in de interne organisatie van de zorgaanbieder

Door het implementeren van een IAM oplossing kan de zorgaanbieder de toegang tot het GBZ voor zorgverleners beheeren. Hoe werkt nu IAM met betrekking tot het proces rond administratie, controle, mandatering en het toekennen van toegangsrechten?

Administratie

De identiteit van de zorgverlener wordt vastgesteld door de zorgaanbieder op basis van gegevens op de UZI-pas. Na identificatie wordt de zorgverlener geregistreerd in het IAM systeem van de zorgaanbieder. De zorgverlener is immers in dienst van de zorgaanbieder. In het IAM systeem krijgt de zorgverlener een uniek identificatienummer toegewezen en wordt de beoefende functie vastgelegd. Vanaf dit moment is de zorgverlener uniek te identificeren bij de zorgaanbieder. Dit is het begin punt van de levenscyclus van een identiteit van een zorgverlener bij de zorgaanbieder. De zorgverlener heeft na registratie in het HR informatiesysteem nog geen gebruikersaccount toegewezen gekregen voor gebruik van het GBZ. Na het invoeren van de zorgverlener in het IAM systeem, wordt (semi) automatisch een gebruikersaccount aangemaakt en het authenticatiemiddel vastgelegd in dit geval de UZI-pas. Toegangsrechten worden gekoppeld aan de zorgverlener op basis van de gegevens op de UZI-pas.

Toegang

Als de zorgverlener zich aanmeldt op het GBZ met behulp van de UZI-pas dan wordt gecontroleerd of de zorgverlener is geregistreerd als abonneehouder of gastgebruiker. Als de zorgverlener in geen van beide situaties bekend is op het zorginformatiesysteem wordt de toegang geweigerd. Is de zorgverlener geïdentificeerd door het GBZ dan wordt bij het Landelijk Schakelpunt (LSP) eerst gecontroleerd of het toegangscertificaat op de UZI-pas nog geldig is. Indien het geldig is dan krijgt de zorgverlener toegang tot het GBZ op basis van de toegangsrechten uit de IAM oplossing. Is het toegangscertificaat niet meer geldig dan wordt toegang tot het GBZ geweigerd.

² Nictiz, programma van eisen voor Goed Beheerd Zorgsysteem, versie 2.0, 31 mei 2007

Conclusie:

IAM biedt de zorgaanbieder de oplossing met betrekking tot het authenticatie probleem rond de UZI-pas waardoor het interne zorginformatiesysteem voldoet aan de GBZ-eisen. Dit door het inregelen van administratie, controle, mandatering en toekennen van toegangsrechten voor zorgverleners met UZI-pas.

Voordelen van een IAM oplossing:

- Zorginformatiesysteem van de zorgaanbieder voldoet aan de GBZ-eisen van NICTIZ.
- Zorginformatiesysteem voldoet aan wet en regelgeving met betrekking tot WBP
- Centrale administratie/vastlegging van abonneehouders en gastgebruikers.
- Inzicht en controle over gastgebruikers en toegangsrechten.
- Inzicht en controle over abonneehouders en toegangsrechten.
- Opheffen zorgverleners als abonneehouders of gastgebruikers in interne Zorginformatiesysteem.
- Zorgverleners die geregistreerd zijn als abonneehouder kunnen andere zorgverleners mandateren.
- Mandatering van zorgverlener wordt centraal vastgelegd.
- Alleen zorgverleners hebben toegang tot het zorginformatiesysteem die hiervoor gerechtigd zijn, dus geen onbevoegden.