

## UZI pas in uw ICT omgeving?

Elektronische informatie-uitwisseling van gegevens komt ook in de zorg meer en meer voor. Waar patiënten vroeger met een recept van de dokter naar de apotheek werden doorverwezen, of met een verwijsbrief bij een andere dokter terecht konden, is nu veel van deze informatie gedigitaliseerd. Hierdoor kunnen patiënten veel beter en sneller geholpen worden en kunnen, in uiterste gevallen, levens worden gered.

Toch ligt het uitwisselen van digitale patiëntinformatie gevoelig. Hoe kan immers worden gegarandeerd dat deze gegevens echt bij de juiste persoon terecht komen en dat niet iemand anders deze informatie kan opvragen of onderscheppen?

### UZI Pas

Hiervoor is een aantal jaar geleden het Uniek Zorgverlener Identificatie Register



(Seinregister) opgezet. Het UZI-register is de organisatie die de unieke identificatie van zorgaanbieders en indicatieorganen in het elektronisch verkeer mogelijk maakt. Zorgverleners worden geregistreerd, zodat deze te identificeren zijn. De UZI pas, die voor elke zorgverlener aan te vragen is, bevat de elektronische identiteit van de zorgverlener. Hierdoor kan binnen software of op websites worden gecontroleerd of diegene die informatie probeert op te vragen ook daadwerkelijk diegene is, die hij of zij beweert te zijn. De UZI pas is als het ware een digitaal paspoort. (Zonder een geldige identiteitskaart of paspoort kan een persoonlijke UZI pas ook niet worden aangevraagd of afgehaald).

### Gebruik binnen uw omgeving

Deze strenge manier van beveiligen, binnen de ICT beter bekend als Smartcard Authentication, is ook te gebruiken binnen uw eigen ICT omgeving. Doordat de UZI pas de unieke identiteit van de houder garandeert, kan deze uitstekend uw huidige authenticatiemethode, veelal een gebruikersnaam en een wachtwoord, vervangen. De UZI pas zal fungeren als gebruikersnaam, terwijl de bijbehorende PIN code het wachtwoorddeel voor zijn rekening neemt. Deze methode is een stuk veiliger dan het simpel invoeren van een gebruikersnaam en wachtwoord. Even meekijken met uw collega, of zelfs een wildvreemde die even meekijkt terwijl iemand inlogt, vormt geen gevaar meer. Als iemand de PIN code weet, heeft diegene immers de pas nog nodig. Andersom geldt hetzelfde. Als iemand zijn of haar UZI pas verliest, kan de vinder niets zonder de PIN code. Deze methode valt daarom ook onder de categorie "Strong Authentication" en wordt in veel standaarden (denk aan NEN7510) aanbevolen of verplicht.

IT Oost Nederland biedt u de mogelijkheid om de UZI pas authenticatie te integreren in uw eigen authenticatiesysteem (meestal Active Directory). Op elke werkplek die is voorzien van een smartcard reader kan een bij u bekende houder van een UZI pas

inloggen op het systeem. Zo wordt voor zowel de zorgapplicatie of website als uw eigen systeem dezelfde veilige autorisatie gebruikt. Deze authenticatie kan worden gebruikt binnen uw Citrix of terminal server omgeving, maar ook prima binnen een zogenaamde Client-server omgeving.

Zelfs uw portal is te beveiligen met smartcard-authenticatie, waardoor ook thuisgebruikers met een smartcardreader gebruik kunnen maken van de veilige UZI pas om in te loggen.



Door een aantal aanpassingen door te voeren in uw ICT infrastructuur kan de veiligheid van uw ICT omgeving enorm worden vergroot, tegen lage kosten. Degenen die recht hebben op een UZI pas kunnen deze immers tot juni 2011 gratis aanvragen.

### **Snel wisselen van gebruikers**

Het gebruik van de UZI pas als loginmethode biedt meer dan alleen een veilige omgeving. Doordat er gebruik wordt gemaakt van een smartcard die continue gechecked wordt, is het ook mogelijk om gebruik te maken van zogenaamde smooth roaming. Dit houdt in dat een gebruiker kan inloggen met zijn UZI pas door deze in de lezer te plaatsen en de PIN code in te voeren. Als de gebruiker zijn plaats verlaat, hoeft diegene slechts zijn of haar UZI pas uit de lezer te halen en de gebruikerssessie wordt automatisch gedisonnected. Hiermee wordt de werkplek geschikt voor een andere gebruiker. Als de gebruiker die zijn of haar UZI pas in de kaartlezer van een andere werkplek plaatst, krijgt de gebruiker automatisch zijn of haar gebruikerssessie terug. De sessie wordt als het ware meegenomen op de UZI pas. Uitloggen en het later opnieuw opstarten van applicaties is dus niet meer nodig, waardoor het gemak en de snelheid voor de gebruiker enorm vergroot kan worden.

### **Alleen zorgverleners?**

Doordat het gebruik van de UZI pas binnen uw netwerk gelimiteerd is tot de zogenaamde "medewerkerspas op naam", of de "zorgverlenerspas" (de "medewerkerspas niet op naam" kan immers de identiteit van een persoon niet garanderen), kan het zijn dat niet elke gebruiker automatisch recht heeft op een geschikte pas.

IT Oost Nederland biedt daarom de mogelijkheid om voor medewerkers die geen recht hebben op een UZI pas, aparte Safesign Smartcards aan te vragen. Doordat deze passen van dezelfde leverancier komen als de UZI pas, kan de oplossing voor 100% geïntegreerd worden binnen uw ICT omgeving. Hiermee kunt u voor iedere medewerker smartcard logon mogelijk maken en wordt de veiligheid van uw omgeving enorm vergroot.

Geïnteresseerd? Neem contact op met IT Oost Nederland, om de mogelijkheden te bespreken. Telefoon: 074-850 42 00 of via [www.itoostnederland.nl](http://www.itoostnederland.nl)

Ook als u vragen heeft over het werkend krijgen van de UZI pas binnen uw omgeving voor bijvoorbeeld het gebruik van de BSN diensten, zonder direct de pas te gebruiken voor Smartcard Logon kan IT Oost Nederland u van dienst zijn!

