Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

EPD Scherm Integratie voor GemsTracker

Sinds versie 1.8.7 van GemsTracker is er een generieke methode waarmee EPD's het scherm van een patiënt kunnen tonen in een venster binnen de applicatie. Voor deze versie waren er verschillende specifieke oplossingen die alleen werkten binnen een specifieke omgeving en die vaak ook nog beveiligingsrisico's met zich meebrachten. De nieuwe oplossing is generiek en werkt met tijdelijk sleutels die niet langer dan een paar uur geldig blijven.

Deze handleiding beschrijft eerste hoe de link vanuit het EPD opgebouwd (kan) worden. Daarna wordt besproken hoe e.e.a. in GemsTracker ingericht kan worden.

De EPD link voor HIX

De volledige URL

De link voor integratie met HiX bestaat uit een aantal vaste en variabele onderdelen:

{siteurl}/embed/login?epd=**{systemUser}**&usr=**{epdUser}**
&pid=**{patientId}**&org=**{organizationId}**&key=**{key}**

Variabele	Omschrijving	Voorbeeld
{siteurl}	De url van de GemsTracker site.	https://zorgmonitor.umcutrecht.nl/schisis
{systemUser}	Een "Embedded EPD Login account" Systeem gebruiker in GT.	HiX
{epdUser}	De gebruikersnaam van degene die ingelogd is in het EPD. Er kan ingesteld worden wat er moet gebeuren als de gebruiker niet bekend is.	m.de.jong
{patientId}	Het patiëntnummer dat getoond moet worden. Ingesteld kan worden of een niet bestaande patiënt gelijk aangemaakt moet worden of een foutmelding geeft.	12345678
{organizationId}	De organisatie waar de patiënt onder valt. Dit is met name van belang bij multi-organisatie installaties.	72 Of bijvoorbeeld "utrecht" of een zorginstelling identificatiecode mits deze ingevoerd zijn onder de organisatie in GT.
{key}	Standaard een tijd-afhankelijke sleutel bestaand uit een vast gedeelte en een tijd-variabel gedeelte. Deze code moet versleuteld worden met bijvoorbeeld sha256 (default) en vervolgens met base64 gecodeerd worden.	KCMjF4tDVUI%2Fh%2BUz2LJkTD2sZ8bP d6raCN83p0ltOyk%3D Oftewel, met **test** als vast gedeelte: Base64(Sha256(**test**{YYYYMMDDHH})) (ingevoerd in GT als: test%s)
{YYYYMMDDHH}	Jaar-maand-dag-uur notatie	2019101217

Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

De volgorde van de variabelen is niet van belang. Ook mag een POST statement gebruikt worden in plaats van het bovenstaande GET voorbeeld.

De tijdcode zorgt ervoor dat deze maximaal een uur geldig is. In de praktijk ongeveer drie uur omdat GT ook de codes van een uur eerder en een uur later accepteert, voor het geval de tijd op de systemen niet synchroon loopt.

Verkorte URL's

Om de link korter te houden en de naam van de **{systemUser}** en het **{organizationId}** verborgen te houden is het mogelijk om project-specifiek een verkorte notatie te gebruiken. Bijvoorbeeld:

> **{siteurl}**/embed/hix?usr=**{epdUser}**&pid=**{patientId}**&key=**{key}**

Hiervoor moet wel een kleine aanpassing uitgevoerd worden in GemsTracker, maar dat is weinig werk.

Ook is het op deze manier mogelijk het type sleutel aan te passen en te zorgen dat die bijvoorbeeld 5 uur geldig is of juist maar 15 minuten. Of waar een andere versleuteling van SHA256 gebruikt wordt.

Een HiX implementatie voorbeeld

De volgende code is een voorbeeld van hoe de (verkorte) URL te genereren in HiX:

```
setvar('Medewerker', '?usr=' +
  display('CODE', HuidigeMutatieGebruiker));

setvar('Patnum', '&pid=' +
  ValueAsString('PATIENT_PATIENT.Patientnummer'));


setvar('Secret', '&key=' + URLEncode(ComputeHashAsBase64(
  "sha256", 'test' + FormatDateTime('YYYYMMDDHH', Now)));

setvar('Url',
  'https://zorgmonitor.umcutrecht.nl/embed/hix' +
  Medewerker + Patnum + Secret);
```

(De schrijver van dit stuk heeft zelf geen toegang tot HiX, dus sorry: ik weet niet waar het ingesteld wordt en heb geen screenshot.)

De EPD link voor Epic

De volledige URL

De link voor het Epic EPD bestaat uit een aantal vaste en variabele onderdelen, waarvan een deel middels AES 256 (iv lengte is 16) versleutelt en ontsleutelt worden:

Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

{siteurl}/embed/login?epd=**{systemUser}**
&org=**{organizationId}**& key={usr=**{epdUser}**&pid=**{patientId}**&chk=**{YYYYMMDDHH}}**

Variabele	Omschrijving	Voorbeeld
{siteurl}	De url van de GemsTracker site.	https://register.cpregsiter.nl/schisis
{systemUser}	Een "Embedded EPD Login account" Systeem gebruiker in GT.	EpicUMCG
{organizationId}	De organisatie waar de patiënt onder valt. Dit is met name van belang bij multi-organisatie installaties.	72 Of bijvoorbeeld "umcg" of een zorginstelling identificatiecode mits deze ingevoerd zijn onder de organisatie in GT.
{key}	Versleutelde data met een tijd-afhankelijke gedeelte zodat een url niet hergebruikt kan worden. Deze code wordt versleuteld met het AES256 algoritme (met de IV waarde 16) *geheime sleutel* als encryptie sleutel. De input string voor encryptie bestaat uit 1 of meerdere sub-query strings voor de waardes usr, pid en chk, waarbij usr en pid eventueel los van de key gespecificeerd kunnen worden.	KCMjF4tDVUI%2Fh%2BUz2LJkTD2sZ8bP d6raCN83p0ltOyk%3D Ontsleutelde waarde: usr= m.de.jong&pid=12345678&chk=2019101217
{epdUser}	De gebruikersnaam van degene die ingelogd is in het EPD. Er kan ingesteld worden wat er moet gebeuren als de gebruiker niet bekend is. Kan versleuteld aangeleverd worden of als zelfstandige parameter.	m.de.jong
{patientId}	Het patiëntnummer dat getoond moet worden. Ingesteld kan worden of een niet bestaande patiënt gelijk aangemaakt moet worden of een foutmelding geeft. Kan versleuteld aangeleverd worden of als zelfstandige parameter.	12345678
chk	Een datum tijd waarde zoals hieronder opgegeven, om te zorgen dat de juist url telkens anders is.	2019101217
{YYYYMMDDHH}	Jaar-maand-dag-uur notatie.	2019101217

Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

De volgorde van de variabelen is niet van belang. Ook mag een POST statement gebruikt worden in plaats van het bovenstaande GET voorbeeld.

De tijdcode zorgt ervoor dat deze maximaal een uur geldig is. In de praktijk ongeveer drie uur omdat GT ook de codes van een uur eerder en een uur later accepteert, voor het geval de tijd op de systemen niet synchroon loopt.

Verkorte URL's

Om de link korter te houden en de naam van de **{systemUser}** en het **{organizationId}** verborgen te houden is het mogelijk om project-specifiek een verkorte notatie te gebruiken. Bijvoorbeeld:

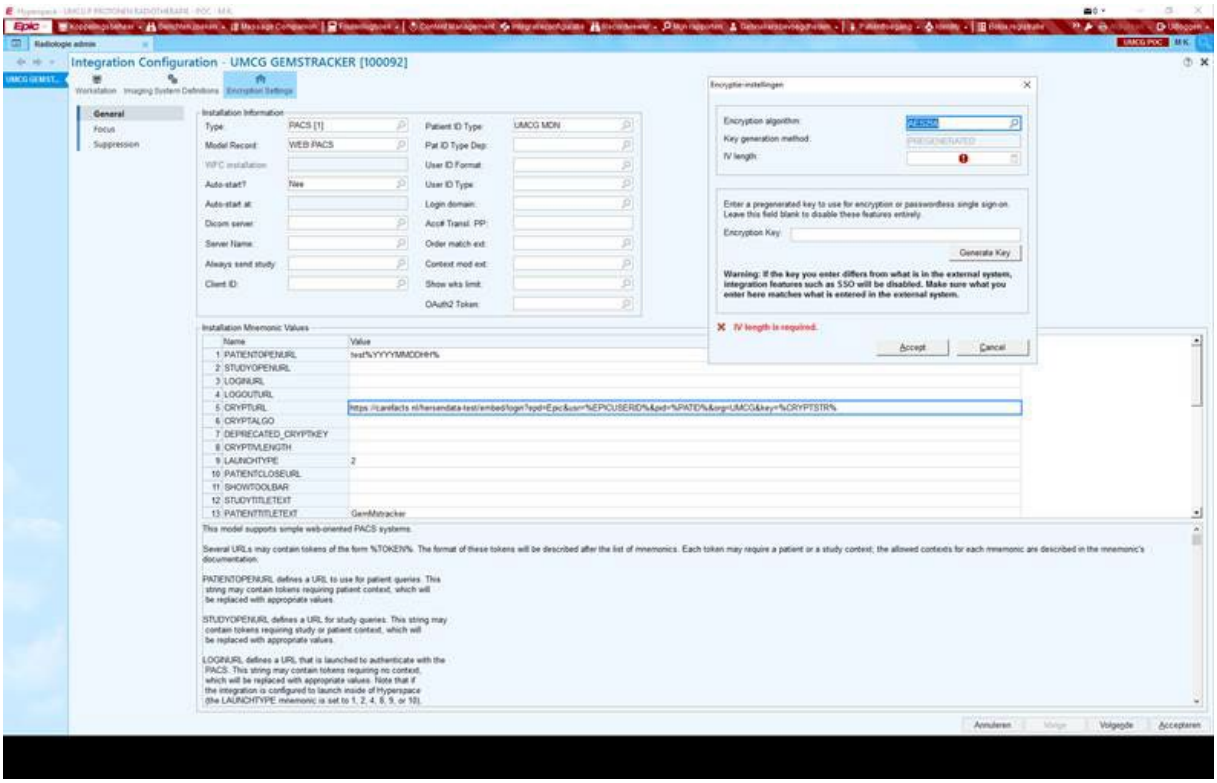
{siteurl}/embed/umcg? &key=**{**usr=**{epdUser}**&pid=**{patientId}&chk={{YYYYMMDDHH}}**

Hiervoor moet wel een kleine aanpassing uitgevoerd worden in GemsTracker, maar dat is weinig werk.

Ook is het op deze manier mogelijk het type sleutel aan te passen en te zorgen dat die bijvoorbeeld 5 uur geldig is of juist maar 15 minuten. Of waar een andere versleuteling van SHA2567 gebruikt wordt.

Een Epic implementatie voorbeeld

Dit is wat we nu hebben gemaakt in Epic POC omgeving:



Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

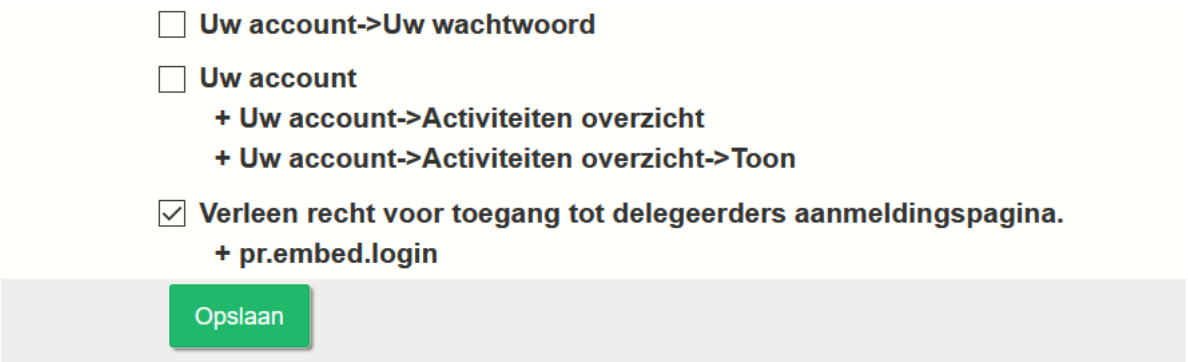
(De schrijver van dit stuk heeft zelf geen toegang tot Epic, dus sorry: ik weet niet waar het ingesteld wordt en heb geen screenshot.)

Instellingen in GemsTracker voor alle EPD's

De juiste rechten instellen

Standaard kan de embed/login pagina niet gebruikt worden. Om deze toegankelijk te maken moet de "nologin" rol aangepast worden onder Beheer => Toegang => Rollen. Dit kunnen over het algemeen alleen super administratoren oftewel applicatie beheerders.

Het onderstaande recht voor toegang tot delegeerders aanmeldingspagina moet toegankelijk gemaakt worden voor niet-ingelogde gebruikers.



Indien dit niet aanstaat wordt de gebruiker altijd naar de algemene login pagina verwezen. Als de embedded login pagina wel toegankelijk is, maar er een andere instelling verkeerd staat, verschijnt altijd de mededeling: "**Authenticatie mislukt**".

De pagina in kwestie is overigens nooit toegankelijk via een menu keuze.

Pas op: Het is verstandig om naast de nologin rol dit recht ook aan alle andere rollen te geven. Anders bestaat het risico dat als een gebruiker al keer een patiënt bekeken heeft via het EPD, deze een foutmelding krijgt als hij/zij een tweede patiënt bekijkt.

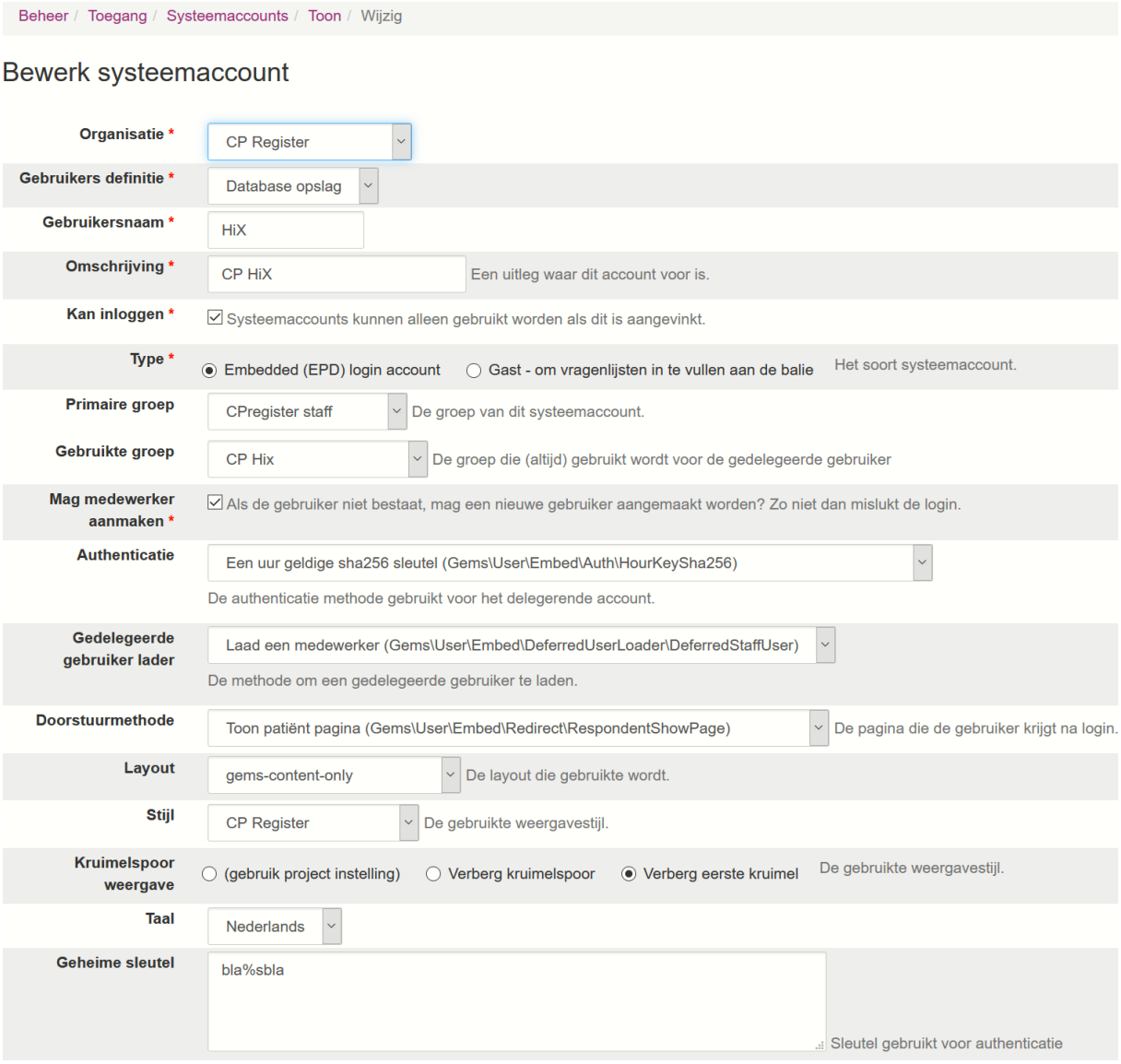
Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

De {systemUser} aanmaken

Ook onder Beheer => Toegang is het sinds 1.8.7 voor super administratoren oftewel applicatie beheerders mogelijk om Systeem gebruikers aan te maken.

Er zijn op dit moment 2 types systeem gebruiker: een “Gast” account dat gebruikt wordt om een patiënt op te zoeken en vervolgens vragenlijsten in te laten vullen zonder dat deze toegang tot het systeem heeft na het invullen. Het andere type is een Embedded (EPD) login account, hetgeen hier gebruikt wordt.

Hieronder een voorbeeldscherm van zo’n gebruiker.



De **Organisatie** is de organisatie waaronder een nog onbekende **{epdUser}** toegevoegd wordt indien deze niet bestaat. Deze gebruikers zijn, nadat ze aangemaakt zijn, te vinden onder Beheer => Toegang => Medewerkers.

Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

Normaal gesproken is “Database opslag” de enige optie bij **Gebruikers definitie.** Maar als een ziekenhuis LDAP of Radius authenticatie gebruikt voor centraal wachtwoord management, worden deze keuzes hieraan toegevoegd. Als één van de waarden ingesteld zijn, dan kan elke EPD gebruiker die toegevoegd is aan GemsTracker inloggen op de web interface met zijn of haar eigen wachtwoord. Wordt dat niet gebruikt dan moet een beheerder eerst deze login mogelijk maken door de gebruikers instelling aan te passen.

De **Gebruikersnaam** is de **{systemUser}** code uit de URL.

De **Primaire groep** is de groep voor elke nieuwe **{epdUser}**.

De **Gebruikte groep** daarentegen is de groep waarmee de gebruiker ingelogd wordt in GemsTracker. Dit wijkt vaak af, bijvoorbeeld om een iets beperktere interface met minder knoppen te bieden of om bepaalde informatie niet te tonen omdat die al in het EPD te zien is. Ook kan hierdoor gekozen worden voor een andere patiënt toon of wijzig scherm.

Mag medewerker aanmaken bepaald wat er gebeurt als de EPD gebruiker niet bekend is bij GemsTracker. Als toegang tot de patiënt in het EPD niet automatisch betekend dat de gebruiker toegang heeft in GemsTracker dan moet dit niet aangevinkt worden. Betekent toegang in het EPD wel dat de gebruiker ook in GT mag kijken, dan wordt automatisch een nieuwe gebruiker in GT aangemaakt met de primaire groep en taal van deze systeemgebruiker.

Authenticatie is de methode die gebruikt wordt voor het genereren van de **{key}**. Standaard is een sha256 sleutel die een uur geldig is. Andere opties zijn het gebruik van md5 of van een dag geldige sha256 sleutel. Er zijn nog een paar andere mogelijkheden, waaronder het wachtwoord van de gebruiker zelf. Dit lijstje kan eenvoudig uitgebreid

Op dit moment is er nog maar 1 **Gedelegeerde gebruiker lader**, namelijk om een medewerker te laden. In de nabije toekomst verwachten we extra opties, bijvoorbeeld om vragenlijsten in een patiënt portaal te tonen.

De **Doorstuurmethode** bepaald wat de medewerker te zien krijgt na de inlog, standaard het GT Toon patiënt scherm, maar toon of voer een nieuwe in wordt ook veel gebruikt.

De **Layout** bepaald de grove structuur van wat weergegeven wordt en wat niet. “gems-content-only” is de standaard en laat de menu’s, logo’s en kop en voet onderdelen van GT weg. Hiermee worden alleen de patiënt gegevens getoond en kan de gebruiker niet naar andere onderdelen van GT navigeren. “gems-responsive” daarentegen toont wel de menu’s en biedt dus volle navigatie mogelijkheden.

De **Stijl** bepaalt de gebruikte fonts en kleuren. Standaard worden dezelfde fonts en kleuren gebruikt als voor de organisatie ingesteld zijn; maar het is mogelijk dat we in de toekomst een stijl te maken die de fonts en kleuren gebruikt uit HiX om de scherm integratie minder opvallend te maken.

Kruimelspoor weergeven is (wederom) bedoelt om te voorkomen dat een medewerker naar andere gegevens kan browsen. Het kruimelspoor staat bovenaan het scherm; in de afbeelding begint die met Beheer en eindigt die met Wijzig. Bij het Toon patiënt scherm is het kruimelspoor “Patiënten / Toon”. De link naar Patiënten maakt het mogelijk het zoekscherm te openen. Door “Verberg eerste kruimel” te kiezen wordt deze optie afgesloten.

Oostzeedijk 314
3063 CC Rotterdam
T 010 8910902
E mjong@magnafacta.nl

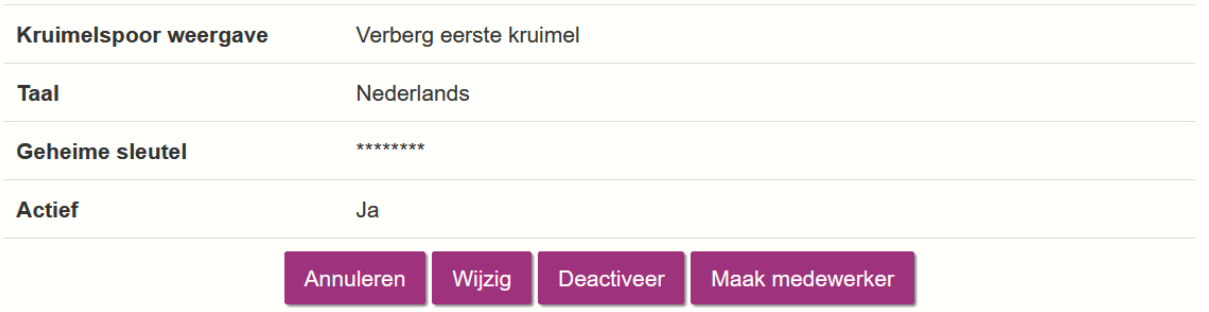
De **taal** is de taal die ingesteld wordt voor eventuele nieuwe gebruikers.

Tot slot is de geheime sleutel de basis voor de **{key}** sleutel waarmee ingelogd wordt. Als deze sleutel de tekst “%s” bevat, word op deze plek de **{YYYYMMDDHH}** code geplaatst (of **{YYYYMMDD}** bij de dag sleutel). Zo niet dan wordt de tijd-code aan het eind van de sleutel toegevoegd.

(Deze sleutel wordt versleuteld opgeslagen in de database, maar wordt hier altijd ontsleutelt weergegeven omdat hij anders kwijt raakt.)

EPD account testen

Om het testen eenvoudig te maken is een voorbeeld login URL generator toegevoegd onderaan het “Toon systeemaccount” scherm. Hier kan een medewerker en een patiënt gekozen worden. Daarmee wordt een url gegenereerd waarmee op dat moment de EPD login in een (andere of private mode) browser geopend kan worden.



De standaard query optie genereerd de url op een manier die in alle browser / server combinaties werkt – en die aan het begin van het document voorgeschreven is. Zonder deze check is de URL iets beter te lezen, maar werkt deze niet met sommige Windows servers.