



Vereenvoudigd gebruik UZI-pas (VGU)

Netwerkdag XIS-leveranciers

Agenda

- Aanleiding
- AORTA Tokens
- Proces m.b.t. VGU
- Specifieke uitwerking triggers
- Verdieping tokens en processen
- Self assessment
- Implementatie-ervaring



Gebruik UZI-pas bij voorschrijven is probleem

Uit 'Vooronderzoek authenticatie via UZI-pas in polikliniek ziekenhuizen – NVZ' blijkt het volgende

UZI-pas: huidig gebruik remmend

"Het huidige gebruik van de UZI-pas remt het gebruik van het LSP in de polikliniek."

Gebruiksonvriendelijk, duur,
beperkt toepasbaar

"Hoewel de UZI-pas als sterk authenticatiemiddel wordt gezien, vinden ziekenhuizen het ook gebruiks-onvriendelijk, technisch lastig en duur, dat voor slechts één doel (opvragen LSP) wordt gebruikt. Dit leidt tot bureaucratische en ongewenste werkwijzen"

Veel praktische bezwaren

"Als bezwaren tegen de UZI-pas worden vaak genoemd: de extra handelingen voor de gebruiker (insteken, pincode intoetsen) om de pas te gebruiken bij opvragen van patiëntgegevens via het LSP; de trage respons in een aantal gebruikssituaties; de extra investering door het ziekenhuis voor de technische integratie met het EPD en andere systemen; de extra kosten voor de kaart."

Sluit niet aan op werkwijze

"In het algemeen sluit de UZI-pas onvoldoende aan op de werkwijze van de medisch specialist in de poliklinische situatie."

Uitdaging VZVZ

Genoemde belemmeringen oplossen, zonder concessies te doen aan de waarborgen die nodig zijn om tot veilige gegevensuitwisseling te komen

Bevraging LSP met gebruik UZI-pas

noodzaak en drempel



UZI-pas waarborgt veilige gegevensuitwisseling

- identificeert en authenticceert wie u bent, welke functie u heeft (rolcode)
- en welke zorgaanbieder u vertegenwoordigt



Gebruik in de praktijk

- UZI-pas is nodig bij iedere bevraging
- UZI-pas wordt als lastig ervaren in het gebruik in het zorgproces



Kosten en beheer

Per gebruiker: € 255,- voor 3 jaar
Beheer van de UZI-passen en mandaten



Ontwikkeling vereenvoudigd gebruik UZI-pas

Belemmeringen gebruik UZI-pas wegnemen
Zonder concessies te doen aan de waarborgen die nodig zijn voor veilige gegevensuitwisseling

Grondslagen van de tokens, wanneer mag je welke gebruiken?

Rollen



= Patiënt



= Zorgverlener



= Ondersteuner

Tokens



= Transactietoken



= Mandaattoken



= Inschrijftoken

UZI-middelen



= zorgverlenerspas



= medewerkerspas



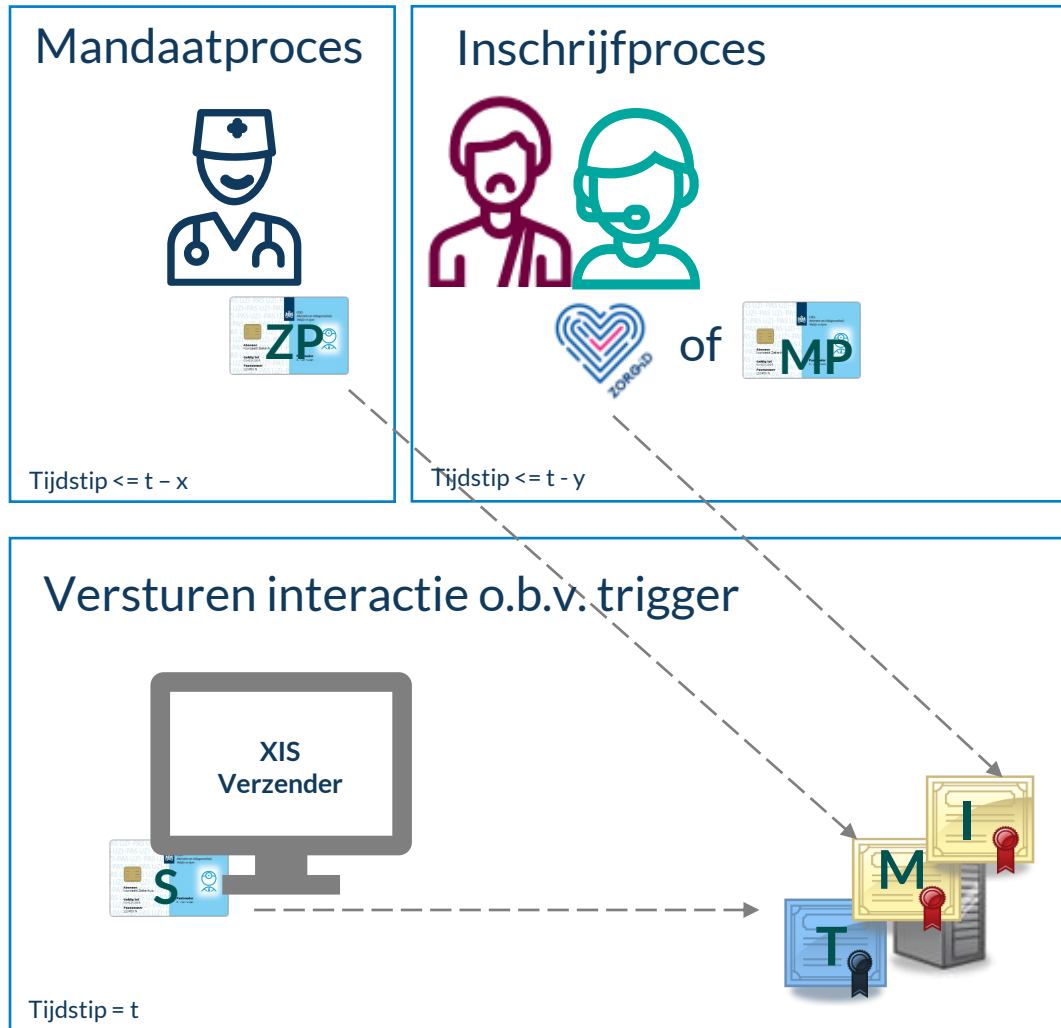
= servercertificaat

Mandaattoken: bewijs dat de zorgverlener die het mandaattoken heeft aangemaakt, toestemming heeft gegeven aan bepaalde zorgverleners en/of systemen om onder zijn verantwoordelijkheid een LSP-bevraging te doen;

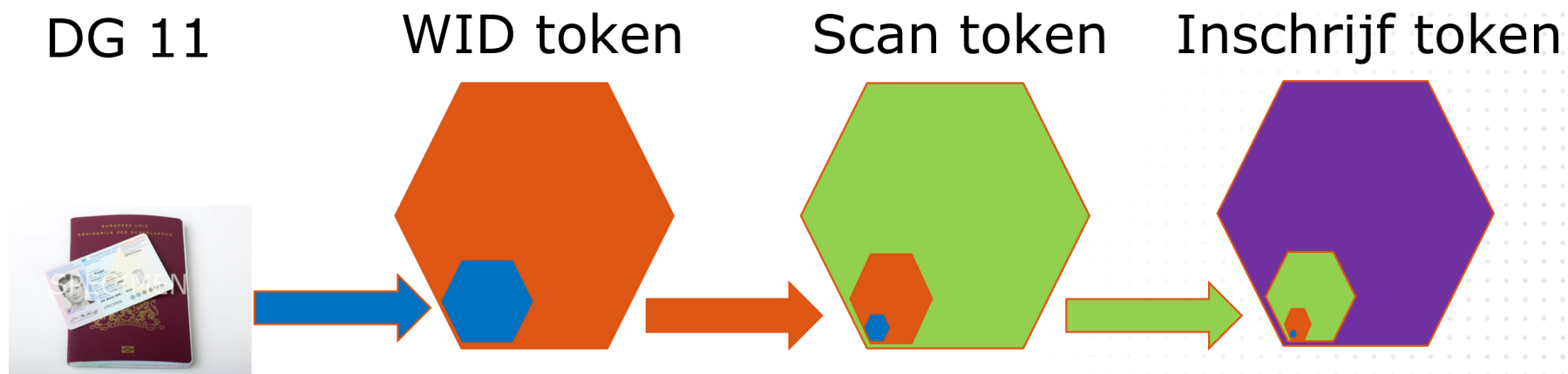
Inschrijftoken: bewijs dat de patiënt is ingeschreven bij de zorgaanbieder;

Transactietoken: koppelt het bericht aan het inschrijf- en het mandaattoken en geeft de waarborg dat het bericht afkomstig is van de applicatie.

Processen m.b.t. VGU



ZORG-ID



		ZORG-ID SDK	Smartphone	XIS
Ondertekend door	Staat der Nederlanden	ZORG-ID	Medewerker	Medewerker

Samenvatting processen m.b.t. VGU

Tijdstip	Proces	Actoren	Token	Duur token	Middel
T-x (x>0)	Mandaatproces	Verantwoordelijke zorgverlener XIS	Mandaattoken	Maximaal de geldigheidsduur van het handtekeningcertificaat waarmee is ondertekend .	UZI-zorgverlenerpas, handtekeningcertificaat
T-y (y>0)	Inschrijfproces	Medewerker Patiënt XIS	Inschrijftoken	Maximaal 1,5 jaar	UZI-medewerkerpas-op-naam, authenticatiecertificaat, of ZORG-ID
T	Genereren transactietoken a.g.v. trigger	XIS	Transactietoken	Richtlijn 5 minuten, maximaal 90 minuten.	UZI-servercertificaat
T+1	Bericht versturen over AORTA	XIS LSP	Mandaattoken Transactietoken Inschrijftoken		UZI-servercertificaat

^[1] Het tijdstip ligt in ieder geval voor het moment dat een transactietoken aangemaakt wordt.

Op welk moment het mandaattoken precies aangemaakt wordt, is afhankelijk van het zorgproces.

^[2] Het tijdstip ligt in ieder geval voor het moment dat een transactietoken aangemaakt wordt.

Op welk moment het mandaattoken precies aangemaakt wordt, is afhankelijk van het zorgproces. Hierbij geldt dat er geen verband is tussen x en y.

Wat verandert er?

Wat verandert er NIET?

- De verantwoordelijkheden van de VZVZ en de zorgaanbieder blijven gelijk
- Zorgaanbieder moet nog steeds voldoen aan vigerend wettelijk kader o.a. de NEN-7510: Informatiebeveiliging --> Eisen Goed Beheerd Zorgsysteem (GBZ), NEN-7512: Zekerheid identiteit zorgaanbieder en maker v.d. tokens, NEN-7513: Traceerbaarheid (logging)
- Logging van het LSP – het LSP logt nog steeds wie verantwoordelijk was voor de opvraging.
- De zorgaanbieder logt wie verantwoordelijk was voor de opvraging en ook wie de informatie heeft ingezien

Wat verandert er WEL?

- Alle bezwaren uit het NVZ rapport worden opgelost waarbij het technisch inregelen zo veilig mogelijk op basis van wat er realistisch mogelijk is
- Onweerlegbaarheid t.a.v. de verantwoordelijke in de logging (ondertekenen van mandaattoken op hoogste niveau)
- Vertrouwen op de correcte logging conform NEN-7513 bij de zorgaanbieders (In LSP logging alleen nog de verantwoordelijk medewerker)
- Naast een aangepaste set GBZ eisen is voor de zorginstelling een zelftoetsingsvragenlijst opgesteld (self-assessment). De vragenlijst dient 1 x per drie jaar ingevuld te worden

Aandachtspunten

- Inzage logging door patiënt;
 - Een zorgaanbieder dient te allen tijde uit te kunnen leggen, waarom er een bericht is verstuurd onder het 'mandaat' van een bepaalde zorgverlener.
- Verlopen UZI-passen;
 - Zorgaanbieder dient te zorgen voor voldoende UZI-passen en voor het tijdig verlengen van UZI-passen.
- Verlopen UZI-servercertificaten;
 - Afhankelijk van organisatietype dient er één of twee servercertificaten te worden aangevraagd. Deze dienen beide tijdig vervangen te worden.



Selecteren juiste mandaattoken

- Er dient een behandelrelatie te zijn vastgelegd met de verantwoordelijke zorgverlener en de patiënt waarvan gegevens worden opgevraagd.
- Er kunnen meerdere mandaattokens aanwezig zijn van verschillende zorgverleners met verschillende rolcodes die een behandelrelatie hebben met de patiënt.
- Vraag: Hoe kan het juiste mandaattoken worden geselecteerd?
- Vraag: Moeten we afstappen van een behandelrelatie per zorgverlener en toe naar een behandelovereenkomst tussen patiënt en zorgaanbieder?

Ondertekenen Inschrijftoken

- Hoe ga je om met zelfinschrijfzuilen, waarbij geen medewerker betrokken is?
 - Garanderen dat er géén BSN's toegevoegd kunnen worden aan lijst met BSN's waar een inschrijftoken voor aangemaakt dient te worden.
 - Controle tegen patiëntadministrerend systeem.

Triggers voor versturen van een interactie

- Triggers te bepalen door XIS-leverancier i.o.m. zorgaanbieder.
- Voorbeelden van triggers:
 - Het beschikbaar komen van nieuwe informatie bij een zorgverlener; een zorgverlener heeft nieuwe informatie beschikbaar gesteld via het LSP en het LSP stuurt een signaal naar alle abonneehouders.
 - Een agenda-afspraak met een patiënt; een patiënt heeft die dag een afspraak en het systeem krijgt hiermee het verzoek om de patiëntgegevens van die patiënt op te vragen.
 - Een bepaalde tijdsperiode; elke eerste van de maand bevraagt het systeem bepaalde gegevens t.b.v. bijvoorbeeld een bewakings- of rapportageproces.
 - Het openen van een dossier; een geautoriseerde zorgverlener opent een dossier van een patiënt en het systeem zorgt ervoor dat de zorgverlener de meest actuele gegevens opgeleverd krijgt door alle nieuwe informatie op te vragen.
 - Een handeling door een daarvoor geautoriseerde gebruiker; een zorgverlener kan het systeem actief opdracht geven om een bevraging te doen m.b.t. een specifieke patiënt.
- Diverse triggers voor specifieke interacties

Abonnement- en signaalfunctie

- Abonnement wordt afgesloten op Patiënt/Gegevenssoort of Contextcode/ApplicatieID/Rolcode;
- Geldigheidsduur abonnement is maximaal 1,5 jaar;
- Abonnement dient te worden afgesloten met UZI-Pas;
- LSP stuurt signaal naar abonnementhouders bij verandering in VWI/ACT.

Abonneren



Trigger voor afsluiten abonnement

Mandaatproces



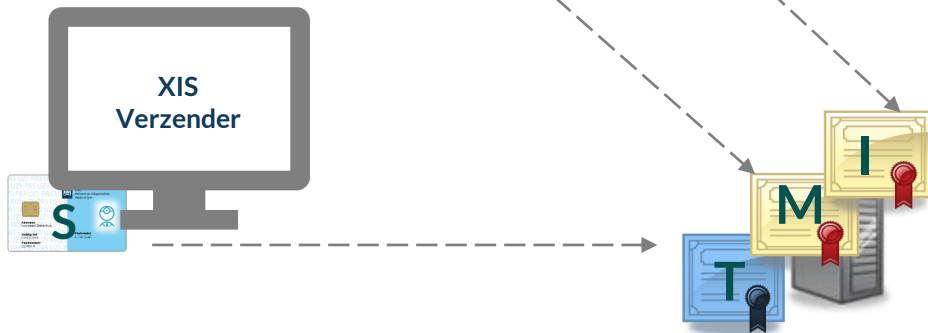
Tijdstip $< t - x$

Inschrijfproces



Tijdstip $= t - x$

Versturen interactie o.b.v. trigger



Tijdstip $= t$

Trigger voor afsluiten abonnement:

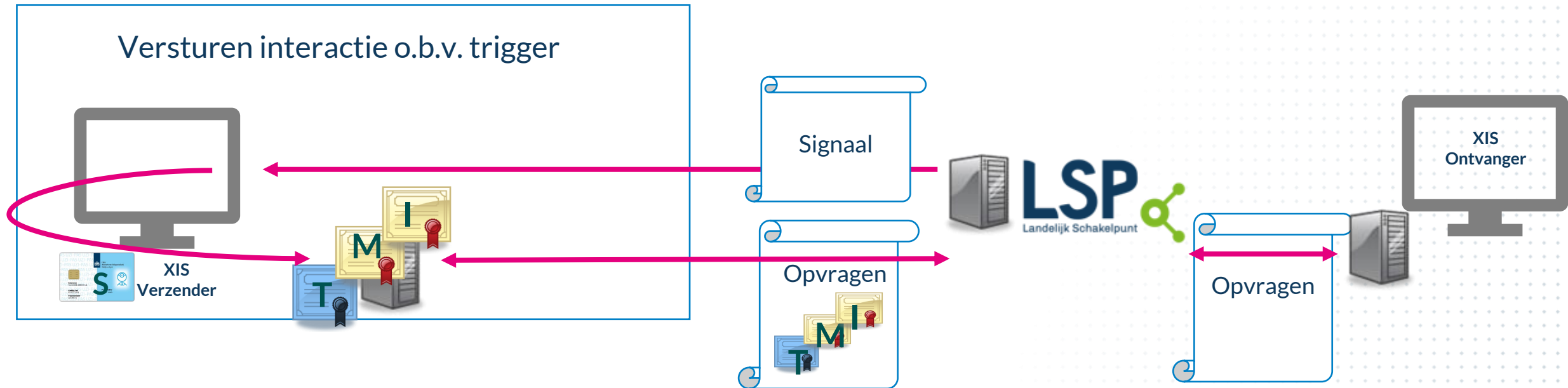
- Aanmaken van een inschrijftoken.

Preconditie:

- Aanwezigheid mandaattoken;
- Ondertekend inschrijftoken.



VGU i.c.m. Abonnementsignaal als trigger



Preconditie:

- Aanwezigheid geldig mandaattoken van een behandelend en/of verantwoordelijke zorgverlener;
- Aanwezigheid geldig inschrijftoken;
- Afgesloten abonnement op patiënt.

Geen menselijk actie en dus UZI-pas benodigd tijdens opvraagproces.

Aandachtspunten m.b.t. abonnementsignaal als trigger

- Afmelden abonnement
 - Wat is het gevolg m.b.t. het geautomatiseerde opvraagproces?
- Verlengen abonnement
 - Indien aanwezigheid geldig inschrijftoken en mandaattoken, dan een geautomatiseerd proces
 - Geautomatiseerd bij aanmaken nieuw inschrijftoken en bij aanwezigheid geldig mandaattoken
- Rolcode abonnementhouder
 - Rolcode van abonnementhouder wordt opgeslagen in ABR
 - Rolcode bepaalt of er een signaal wordt verstuurd o.b.v. opvraagautorisatie
 - Is dit werkbaar?
- Signaal per bouwsteen, bevraging met contextcode
 - Één bevraging voor een specifieke contextcode per x-tijd
- Bevraging op later tijdstip om keten niet onnodig te belasten



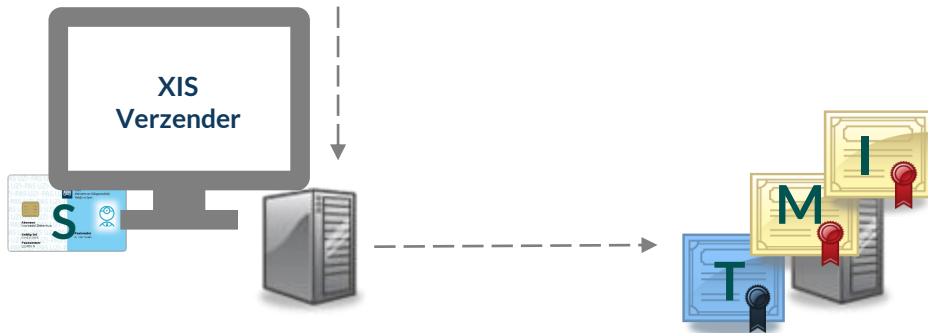
Trigger voor bevraging na openen patiëntdossier

Openen dossier



Tijdstip = $t - 1$

Versturen interactie o.b.v. trigger



Tijdstip = t

Trigger voor opvragen gegevens:

- Openen patiëntdossier.

Preconditie:

- Aanwezigheid mandaattoken;
- Ondertekend inschrijftoken;
- Juiste autorisatie voor zorgverlener/medewerker.



Aandachtspunten bevraging na openen patiëntdossier

- Autorisatie goed inregelen
 - Welke zorgverleners mogen dossier openen?
- Eén keer bevragen in x-tijd
- Mogelijk bevraging met meerdere contextcodes nodig



Initiële aanmaken inschrijftokens bestaande patiënten

- Elk inschrijftoken dient ondertekend te worden met UZI-pas (medewerkerpas of zorgverlenerspas) die daarvoor geautoriseerd is
- Niet tijdsefficiënt!
- Vergelijkbaar proces met het verlengen van het inschrijftoken

Verlengen Inschrijftoken

- Inschrijftoken is maximaal 1,5 jaar geldig en dient tijdig verlengd te worden
 - Indien patiënt ingeschreven staat en in behandeling is of weer in behandeling komt
 - Verlengen ook met UZI-Pas
 - Verlengproces is niet bepaald en kan worden afgestemd tussen XIS-leverancier en klant
-
- Voorkom dat een kwaadwillende een BSN kan toevoegen aan de lijst met te verlengen inschrijftokens!

Mandaattoken

Bewijs dat de zorgverlener die het mandaattoken heeft aangemaakt, toestemming heeft gegeven aan bepaalde zorgverleners en/of systemen om onder zijn verantwoordelijkheid een LSP-interactie te doen.



Vastgelegd in autorisatieregel

Voor VGU dient een applicatieID te zijn opgenomen in de autorisatieregel

Voor gebruik i.c.m. UZI-pas op moment van versturen interactie dient een zorgverlener o.b.v. een kenmerk opgenomen te zijn

Het is mogelijk om één mandaattoken aan te maken voor VGU en regulier gebruik i.c.m. UZI-Pas op moment van versturen interactie.

Autorisatieregel

- Voor VGU dient een applicatieID te zijn opgenomen in de autorisatieregel
- Voor gebruik i.c.m. UZI-pas op moment van versturen interactie dient een zorgverlener o.b.v. een kenmerk opgenomen te zijn
 - Kenmerk kan van alles zijn, als het maar te herleiden is naar de persoon
 - Kenmerk hoeft niet uniek gekoppeld te zijn aan één persoon, maar kan ook een 'groep' beslaan
 - Autorisatiebeheerder koppelt een kenmerk aan een persoon

Het is mogelijk om één autorisatieregel aan te maken voor VGU en regulier gebruik i.c.m. UZI-Pas op moment van versturen interactie. Er is dan dus ook maar één mandaattoken van die specifieke mandaterende zorgverlener.

Mandaatproces

- Verplicht voor:
 - VGU (Opnemen ApplicatieID);
 - Versturen interactie onder mandaat (Opnemen zorgverlenerkenmerk).
- Optioneel voor:
 - Intern gebruik voor bijvoorbeeld toekennen autorisaties voor het VGU met als trigger het openen van een dossier

Verlengen Mandaattoken

- Mandaattoken heeft een maximale geldigheidsduur die afhankelijk is van de maximale geldigheid van het UZI-certificaat, waarmee het mandaattoken is ondertekend.
- Zorgverlener verantwoordelijk voor verlengen mandaattoken

Behandelrelatie

- Niet randvoorwaardelijk voor inschrijftoken en/of verlengen inschrijftoken
- Wel randvoorwaardelijk voor gebruik van een mandaattoken
 - Gebruik van juiste rolcode; welke zorgverlener en welke UZI-pas?

Self-assessment

Waarom?

- Uit risico analyse zijn aanvullende GBZ eisen gesteld die geaudit moeten worden
- Audit bij elke zorgaanbieder niet haalbaar, dus gekozen voor het self-assessment
- Self-assessment is zelftoetsing op deze aanvullende GBZ eisen

Hoe?

- https://www.formdesk.com/vzvz/selfassesment_zorgaanbieders_vereenvoudigd_gebruik_uzi_pas
- Invullen, ondertekenen en opsturen aan het VZVZ Service- en Informatiecentrum (SIC)

Implementatie ervaring (1)

Aanmaken inschrijftoken bij registratie of inclusie van de patiënt

- Dit vindt automatisch plaats als de gebruiker is ingelogd met een UZI-pas of er wordt om verzocht door de applicatie als de UZI-pas geplaatst moet worden

Verlengen inschrijftoken

- Indien de patiënt na 1,5 jaar (geldigheidsduur inschrijftoken) nog in zorg is, zal een nieuw inschrijftoken aangemaakt moeten worden. De leverancier biedt hier functionaliteit voor.

Maken van een Mandaattoken

- Tijdens het registreren van de nieuwe UZI-pas of van een gewijzigde toegang tot de zorgapplicatie van een zorgverlener wordt eenmalig een mandaattoken aangemaakt

Implementatie ervaring (2)

Opvragen van gegevens – medicatieverstrekkingen en CiO's

Tijdens patiëntcontact 'controleert' het systeem of de benodigde waarborgen (tokens) aangemaakt zijn en zal automatisch het LSP bevragen voor de benodigde medische gegevens. Indien er onvoldoende waarborgen zijn, dan wordt de gebruiker de mogelijkheid gegeven om die alsnog aan te maken of ad hoc met een UZI-pas het LSP te bevragen (oude situatie).

Opvragen van gegevens – LSP Ketenzorg

- Het KIS neemt op iedere patiënt een abonnement
- Bij wijziging in het HIS ontvangt het KIS een signaal
- 's nachts worden de signalen verwerkt (om de bronsystemen niet te veel te belasten) OF
- Als het dossier wordt geopend en er is nog een onverwerkt signaal
- Geactualiseerd HIS en KIS systeem

Medicatieoverdracht

- Wordt verder uitgewerkt tijdens hackathon op 25 jan '23



Dank voor jullie aandacht!

Vragen?