Ministerie van Volksgezondheid,
Welzijn en Sport

Koppelvlakspecificatie
Dezi-Online

Koppelvlak 2: Middelenleverancier

Colofon

Projectnaam	Dezi-online
Organisatie	iRealisatie
Datum:	april 2024
Versie:	1.1

Inhoudsopgave

1. Inleiding

Met het nieuwe Dezi-stelsel is het doel om gezondheidsdata gericht toegankelijker te maken voor zorgmedewerkers en -professionals. Dit betekent dat zorgmedewerkers en -professionals alleen medische informatie kunnen zien die relevant is voor hun functie. Deze functie specifieke informatie wordt vrijgegeven op basis van drie attributen die worden opgestuurd:

Wie ben je? (UZI-nummer)
Waar werk je? (URA-nummer)
Welke bevoegdheden heb je? (rolcode)

Een van de nieuwe functionaliteiten van het nieuwe Dezi-stelsel is de integratie van zorgspecifieke middelen. Dit betekent dat men in staat is om zich te identificeren en authenticeren door middel van een ziekenhuispas, telefoon, tablet, token, etc. Door meer inlogmiddelen toe te voegen, wordt het toegang krijgen tot een zorgplatform makkelijker en gebruiksvriendelijker via het Dezi-stelsel.

Om aan te sluiten op de technische omgeving, maakt een leverancier verbinding met het ontkoppelpunt. Dit is een technische voorziening van het CIBG die als OpenID Connect gateway functioneert.

Op dit moment is de functionaliteit voor het gebruiken van een zorgspecifiek inlogmiddel alleen beschikbaar op de Proeftuin, de testomgeving voor het Dezi-stelsel. Op basis van testen met toekomstige gebruikers, platform- en middelenleveranciers is de ambitie om deze functionaliteit te gaan testen in een pilotvorm. De planning hiervoor is afhankelijk van de voortgang van testen op de Proeftuin omgeving.

In deze koppelvlakspecificatie is voor de leveranciers van zorgspecifieke middelen uitgelegd hoe kan worden aangesloten op de technische omgeving ten behoeve van de identificatie en authenticatie in het nieuwe Dezi-stelsel.

Naast dit document met de koppelvlakspecificaties, is er ook een *aansluitdocument.* Hierin wordt stap voor stap beschreven hoe er een aansluiting gemaakt kan worden met de technische omgeving.

2. Gegevensverwerking

Het ontkoppelpunt (OIDC-gateway) verwerkt op de titel van het CIBG de volgende gegevens van een zorgmedewerker:

- Het (versleuteld) BSN
- Het (versleuteld) UZI-nummer
- Het (versleuteld) URA-nummer
- De (versleutelde) rolcode(s)
- De (versleutelde) voorletter(s) van de voornaam / voornamen
- De (versleutelde) achternaam inclusief tussenvoegsel(s)
- Het IP-adres van het apparaat dat wordt gebruikt (computer, telefoon)

3. Onderdeel ‘identiteitsvaststelling’

3.1 Introductie

Een onderdeel van het nieuwe Dezi-stelsel is het vormgeven van een alternatieve oplossing voor de identificatie en authenticatie van zorgprofessionals en -medewerkers. Hiertoe worden bestaande en toekomstige authenticatiemiddelen ingezet. Dit betreft de middelen die onder de Wet Digitale Overheid (wDO) beschikbaar zullen komen en erkende Europese middelen (eIDAS-1) van andere Europese lidstaten.

Daarnaast is er behoefte in het zorgveld om ook eigen authenticatiemiddelen te kunnen gebruiken. Deze middelen worden zorgspecifieke middelen genoemd. Kenmerkend voor deze authenticatiemiddelen is dat deze onder de verantwoordelijkheid van een zorgaanbieder worden verstrekt aan zorgmedewerkers. De eisen aan een zorgspecifiek middel worden beschreven in de NEN-7518 (op dit moment in ontwikkeling).

Om een beeld te krijgen van de koppelvlakken die een rol spelen bij het onderdeel ‘identiteitsvaststelling’, is in onderstaande afbeelding de samenhang abstract weergegeven.

Figuur 1: Schematische weergave koppelvlakken en ontkoppelpunt

Het ontkoppelpunt biedt twee verbindingsmogelijkheden afhankelijk van de rol als OIDC-provider of OIDC-client. Platformleveranciers maken verbinding via koppeling 1 waarbij het aangesloten platform als OIDC-client fungeert en het ontkoppelpunt als OIDC-provider.

Middelenleveranciers maken verbinding via koppeling 2 waarbij het ontkoppelpunt als OIDC-client fungeert en het aangesloten middel als OIDC-provider.

Dit document betreft alleen informatie die betrekking heeft op koppeling 2 voor middelenleveranciers.

Voor meer informatie betreft koppeling 1 zie het document: *Koppelvlakspecificatie Dezi-Online koppelvlak 1: platformleverancier*

3.2 Architectuur

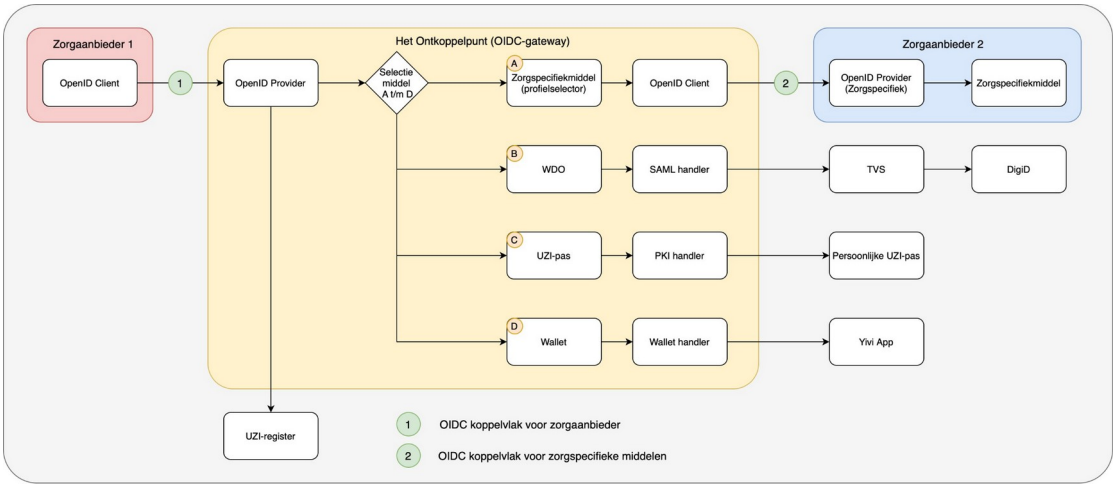
Wanneer een zorgmedewerker zich identificeert en/of authenticeert met een zorgspecifiek middel, treedt het ontkoppelpunt (gele blok, figuur 2) op als een OIDC-client van de Authenticatiedienst van het Zorgspecifieke middel van de zorgaanbieder (blauwe blok, figuur 2). De Authenticatiedienst gedraagt zich hierbij als een OIDC-provider. De afhandeling van de daadwerkelijke autorisatie met behulp van het zorgspecifieke middel is de verantwoordelijkheid van de desbetreffende OIDC-provider.

Deze opzet maakt het mogelijk dat ieder soort authenticatiemiddel dat voldoet aan de NEN 7518 kan worden gebruikt waarbij na de authenticatie de OIDC-provider het resultaat van de authenticatie aan het ontkoppelpunt kan meegeven.

3.3 Het verkrijgen van een zorg identiteit

In de huidige implementatie is het mogelijk om een tijdelijk JWT-token aan te vragen bij het UZI-register van de Proeftuin. Dit JWT token, dat door het UZI-register is ondertekend, kan op het zorgspecifieke authenticatiemiddel geladen worden. Het is aan de leverancier om ervoor te zorgen dat het token op de juiste manier aan de zorgprofessional wordt verstrekt.

Wanneer de zorgverlener inlogt met behulp van het zorgspecifieke inlogmiddel moet deze JWT token verstrekt worden als ‘signed_userinfo’ claim van de userinfo endpoint van de OIDC-provider van de ZSM leverancier. Voordat de ZSM leverancier het JWT token teruggeeft om te identificeren moet de ZSM leverancier de identiteit van de zorgmedewerker verifiëren.



Figuur 2: Overzicht van de koppelvlakken en ontkoppelpunt

3.4 Het ontkoppelpunt (OIDC-gateway)

Om aan te sluiten op de technische omgeving maakt een leverancier een verbinding met het ontkoppelpunt. Het ontkoppelpunt laat op basis van het OpenID Connect (OIDC) protocol de gebruiker inloggen. OpenID Connect (OIDC) is, net als SAML, een federatief authenticatieprotocol: het systeem waar de identiteit van de gebruiker is opgeslagen, staat dus los van de online dienst waar de gebruiker op inlogt.
Het OpenID Connect (OIDC) protocol vormt een identificerende laag (identity layer) over het OAuth 2.0 protocol heen. Een external identity provider, in dit geval het CIBG, retourneert een (versleuteld) access token met de gebruikers identiteit.

3.5 Koppelvlakspecificatie

Het zorgspecifieke middel dient aan te sluiten op de technische omgeving op basis van de technische standaard OpenID Connect (OIDC). Dit is een beheerde, open standaard die een technisch koppelvlak biedt dat eenvoudig implementeerbaar is.

Met de OIDC-standaard wordt de PKCE Authorization Code flow gebruikt als extensie op de standaard OIDC specificatie. Daarbij wordt er gebruikgemaakt van de SHA-256 (S256) 'code challenge method' in de authorization code flow. Zie RFC 7636.

3.6 Gebruikte standaarden

Tabel 1: gebruikte standaarden

Standaard		Referentie
OpenID Connect		https://openid.net/specs/openid-connect-core-1_0.html
PKCE Authorization Code Flow (PKCE)	RFC 7636	https://datatracker.ietf.org/doc/html/rfc7636
SHA-256(S256)	RFC 6234	https://datatracker.ietf.org/doc/html/rfc6234
JSON Web Token (JWT)	RFC 7519	https://www.rfc-editor.org/rfc/rfc7519.html
JSON Web Encryption (JWE)	RFC 7516	https://datatracker.ietf.org/doc/html/rfc7516
JSON Web Signature (JWS)	RFC 7515	https://datatracker.ietf.org/doc/html/rfc7515
JSON Web Key (JWK)	RFC 7517	https://datatracker.ietf.org/doc/html/rfc7517

3.7 Message encryption

De ‘userinfo’ zoals gespecificeerd in de OpenID Connect specificaties is versleuteld volgens de JSON Web Encryption (JWE, RFC 7516) specificatie.
Daarbij wordt er gebruikgemaakt van een nested JWT zoals beschreven in RFC 7519.
Voor de versleuteling door de middelenleverancier wordt de public key van de OIDC-Provider gebruikt die bij de registratie bij het ontkoppelvlak aangeleverd wordt.

De implementatie van het koppelvlak is volgens de specificatie zoals beschreven in de OpenID specificatie waarbij de middelen leverancier de rol van OIDC-provider heeft.

Het ontkoppelpunt valideert dat de encrypted en signed JWT daadwerkelijk van de middelenleverancier komt. Dit betekent dat de signature van de ‘inner JWT’ gevalideerd wordt. De middelenleverancier biedt hiertoe een OpenID Connect JWKS Endpoint aan volgens de specificatie van RFC 7515.

De locatie van de JKWS is via de OIDC-configuration van de server te vinden. Voor de validatie van de signature is de public key van de zorgmiddelenleverancier nodig. In de ‘inner JWT’ is een ‘kid’-header (key ID) opgenomen die moet corresponderen met de ‘kid’ van de middelenleverancier dat in de jwks-uri staat.

3.8 Message signing

De ‘userinfo’ die de het ontkoppelpunt opvraagt bij de middelenleverancier is ondertekend met de sleutel van de middelenleverancier. Hierdoor wordt het ontkoppelpunt in staat gesteld om te valideren dat de ‘userinfo’ onaangepast afkomstig is van de middelenleverancier. Deze validatie moet uitgevoerd worden door het ontkoppelpunt om de betrouwbaarheid van de ‘userinfo’ te kunnen garanderen.

Voor de technische omgeving moet een minimale sleutellengte van 4096 bits RSA worden gebruikt om de private key te maken.
Voor productie omgevingen is een PKI-O certificaat vereist. Voor niet productie omgevingen kan er gebruik gemaakt worden van publieke CA’s of van self-signed certificaten.

3.9 Geen single sign-on (SSO) en logout

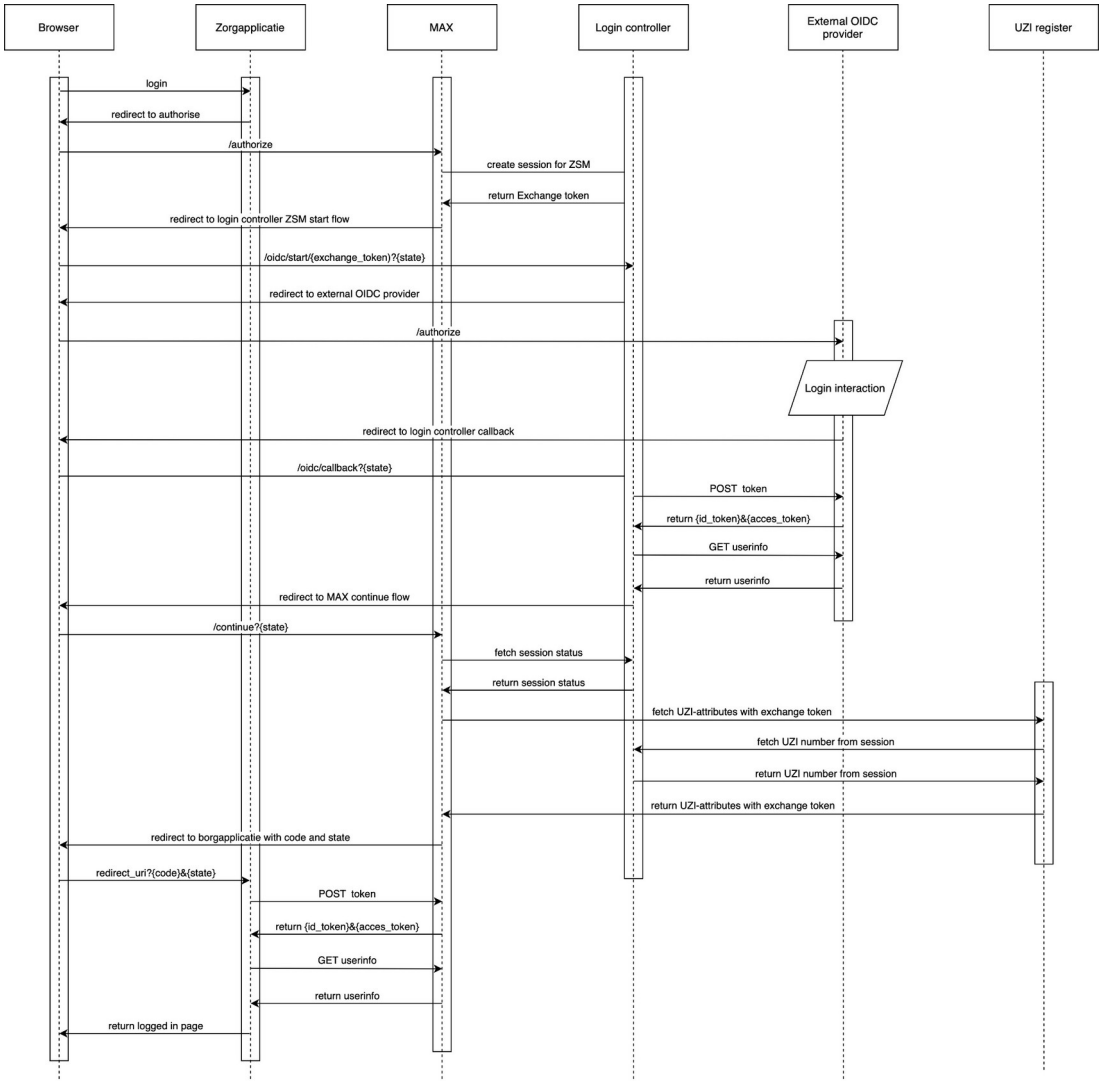
Er wordt door het ontkoppelpunt geen single sign-on functionaliteit geleverd. Deze functionaliteit behoort te worden geleverd door de authenticatiemiddelen/-diensten. De kaders waar de erkende middelen en authenticatiediensten aan moeten voldoen zijn bepalend of SSO mag worden ondersteunend. Doordat het ontkoppelpunt geen (inlog) sessie bewaard, wordt er ook geen logout functionaliteit aangeboden.

Authenticatiedienst	De rol van een partij die op basis van een identificatiemiddel een authenticatieverklaring afgeeft. Naast de generieke authenticatiedienst (voor generieke authenticatiemiddelen) kunnen ook zorgspecifieke authenticatiediensten worden opgenomen in het stelsel (voor zorgspecifieke authenticatiemiddelen).
BSN	Burger Service Nummer, waarmee een dienstafnemer zich initieel kan identificeren in het stelsel, die omgewisseld wordt in het UZI-nummer van de dienstafnemer in het zorgregister.
CIBG	Uitvoeringsorganisatie van VWS verantwoordelijk voor o.a. het zorgregister, en daarmee een partij binnen dit stelsel.
Digitaal ondertekenen	Het proces waarmee een digitaal document wordt voorzien van een elektronische handtekening.
JWE	JSON Web Encryption (JWE) is directe encryptie met een symmetrische AES-sleutel volgens een open standaard (RFC-7516).
JWT	JSON Web Token (JWT) is een open standaard (RFC-7519) die een compacte en op zichzelf staande manier definieert voor het veilig verzenden van informatie tussen partijen als een JSON-object
OIDC-gateway	Technische oplossing die op basis van de OIDC-standaard authenticatiemiddelen ontsluit (via een ander technisch koppelvlak) en met behulp van de identiteitsverklaring een zorgidentiteit samenstelt vanuit het Dezi-register. Zie ook Zorgtoegangsdienst.
Ontkoppelpunt	Werktitel voor het systeem dat de functionaliteit implementeert die de OIDC-gateway biedt.
OpenID Connect	OpenID Connect 1.0 is een open standaard voor gedecentraliseerde authenticatie. Het biedt applicaties de mogelijkheid de identiteit van de gebruiker vast te laten stellen door een vertrouwde server, als ook attributen van de gebruiker op te vragen.
proeftuin omgeving	Een technische omgeving waarin leveranciers en zorgaanbieders kunnen aansluiten op de technische infrastructuur die in het kader van het project Toekomstbestendig Dezi wordt gerealiseerd. De proetuin omgeving en bepaalde implementatie-keuzes die daar worden toegepast kunnen nog veranderen. In

	de technische omgeving wordt niet gewerkt met echte data van echte zorgmedewerkers (gebruikers).
Rolcode	Kenmerk(en) van een zorgmedewerker vastgelegd in het zorgregister of een attribuutregister, gerelateerd aan de functie bij de zorgaanbieder (o.b.v. het URA-nummer). Een rolcode drukt de bevoegdheid van een zorgmedewerker uit zoals deze in het UZI-register bekend is. Deze is gebaseerd op erkende beroepen van de wet BIG.
Signeren, signen	Zie digitaal ondertekenen
URA-nummer	Het abonneenummer zoals deze bekend is in het UZI-register. Het is een identificerend nummer die een zorgorganisatie aanduidt.
Dezi-nummer/UZI-nummer	Uniek identificerend nummer voor een zorgmedewerker (natuurlijk persoon) zoals deze bekend is in het UZI-register. Een UZI-nummer is in het UZI-register te relateren aan een BSN.
WetDO / wDO	Wet Digitale Overheid
Zorgaanbieder	Het unieke identificatie-attribuut van een zorgaanbieder binnen het zorgregister (UZI Register Abonneenummer).
Zorgidentiteit	De digitale representatie van de identiteit van een zorgmedewerker in de context van de zorgaanbieder. De zorgidentiteit bestaat uit een aantal kenmerken. Dit zijn ten minste: UZI-nummer + URA-nummer + rolcode(s)
Zorgmedewerker	Een natuurlijke persoon die functie matig zorg verleent in dienst van een zorgaanbieder.
Zorgprofessional	Professionals die taken verrichten in de zorg, dit is (dus) een bredere doelgroep dan de zorgverlener.
Zorgtoegangsdienst	De generieke authenticatie-voorziening voor de zorg, vastgelegd in het stelsel, waarvan het doel is het leveren van een betrouwbare, veilige en interoperabele verstrekking van identiteitsinformatie van de zorgmedewerker aan de zorgaanbieder. Zie ook OIDC-gateway.
Zorgspecifiek middel	Een authenticatiemiddel waarmee zorgprofessionals zich authentiseren, verstrekt door een zorgaanbieder en in overeenstemming met de NEN-7518 norm. De conformiteit kan worden aangetoond met een certificaat van een bevoegde Certificerende Instantie.

Bijlage 2: Sequentiediagram Zorgspecifiek middel

Het sequentiediagram van het koppelvlak voor een Zorgspecifiek middel volgens RFC7636.



Bijlage 3: Voorbeeld userinfo JWT Zorg Middelen Leverancier

eyJhbGciOiJSDezi1NiIsImtpZCI6IjhqSzBHN3pvL3lpNTdaVDhqQUtSVzJIODZyNUJ4OUFzYXU2VXMyR284ejg9IiwieDV0IjoieWpjQm96bkFIb
mJwQnFScG11RWFqM3YzUXN2WExjS3ZJNkd3WlhHYklwZyJ9.eyJleHAiOjE3MTExMDM5MTUsIm5iZiI6MTcxMTEwMzg0NSwic2lnbmVkX3Vz
ZXJpbmZvIjoiZXlKaGJHY2lPaUpTVXpJMU5pSXNJbXRwWkNJNkltUk1VMlZJUkVWaVdrYzFTVGx5Ym5NMFFtZDFlRUl5U0c1amFuZG9XVk5yZU
dOdVdIY3ZVVFppTmtrOUlpd2llRFYwSWpvaUxYVnhaMlJXVUdadFlYbHFhMlppUkZCMlFXaE5UbGhYUzNST01HNW5kamQxZGpjeExUQTJab
WhpWXlKOS5leUpoZFdRaU9pSnlaV2RwYzNSbGNpNXNZV0p6TG5WNmFTNXdjbTlzYjJOaGRHbHZiaTV1WlhRaUxDSmxlSEFpT2pFM01USX
pNVE0wTlRVc0ltbHVhWFJwWVd4eklqb2lVaTVOTGtFdUlpd2lhWE56SWpvaWJXRjRMbkJ5YjJWbWRIVnBiaTUxZW1rdGIyNXNhVzVsTG5Ka2Iy
SmxhR1ZsY2k1dWJDSXNJbXh2WVY5aGRYUm9iaUk2SW1oMGRIQTZMeTlsYVdSaGN5NWxkWEp2Y0dFdVpYVXZURzlCTDJocFoyZ2lMQ0pzYj
JGZmRYcHBJam9pYUhSMGNEb3ZMMlZwWkdGekxtVjFjbTl3WVM1bGRTOU1iMEV2YUdsbmFDSXNJbTVpWmlJNk1UY3hNVEV3TXpnME5Td
2IjbVZzWVhScGIyNXpJanBiZXlKbGJuUnBkSGxmYm1GdFpTSTZJa1JsSUZwcFpXdGxibUp2WldjaUxDSnliMnhsY3lJNld5SXdNUzR3TVRBaVhTd
2lkWEpoSWpvaU5ESTBNalF5TkRJaWZTeDdJbVZ1ZEdsMGVWOXVZVzFsSWpvaVZscFdXaUJZYVcxMWJHRjBiM0l4TWlJc0luSnZiR1Z6SWpwYkl
qQXhMakF4TUNKZExDSjFjbUVpT2lJMU1EQXdNRFV6TlNKOVhTd2IjbVYyYjJOaGRHbHZibDkwYjJ0bGJpSTZJaIF3Wm1ObU1XSTBMVE0wT0d
NdE5HUmpZeTA0WWpFM0xXUmpNV0ZtTjJGall6VTFPU0lzSW5OMWNtNWhiV1VpT2lKTVlXRnlJaXdpYzNWeWJtRnRaVjl3Y21WbWFYZ2lPaU
oyWVc0aUxDSjFlbWxmYVdRaU9pSTVPVGs1T1RFM056SWlmUS5kbkRyQUJma2ZzMWo5QVBaY2ZRUFFvTWxfS01PNDBQd2hQeHNnOWF6
ZTJTRkZzWmJEeUpteHk2aDlyMkk2M2w3Z3NxdEtielpydlRuUFN3UFBFY1UxdHBTVFFTVndjZktmckRXNk5HdmlTdWJFZzBtWVM4czRTQ1hw
SmxTTGNHdjcyeTJrUW9GSnNLMDN3RHY1MGlTZ053XzhVTFoxaU5xS0pSVzR3eXkyUy05N0tRYmI3SDZlcVNHY0dHSVhTaVlCRFYxa29wVlp
5ZnNELVkzdEkyNzlNN0hNX2s4MDh4SlVfNEVkN1ZYN3YxdGJkQU9pNWpoWUpHMS02R0ZKS2Y3VlBQcTBRdWVGaEJfYkJFakxmb1dFWmFv
cE44NTFuQjEtVUpTcnd5eV8yeHNHNkJUVERnR3Rfc1FVWEZKRVVfelhGZ2hzSHZEMGZpSmhDcTVXTlZqWmlmT2RpT3RyYXpaQUs1Vk5zUV
NSeFM2blczS1VNeGRpTzduQk1nbGlQU0JxdkJZUUppZS16bzIxSjNfUXJ2RXZ0WldPUnpkVl8wUURWMnRubEc1MXNDeEx1cFFSalpGeGx1R
mpqT2ZaTUtWLXpSOUdCVXR3QnBGbWN2dzNZaGQ2MVJzZjA2N0JlNkdmVGNzZGFMZHJaQlhiM3BQOUd6VzVOeDByYW5obnFvU29RaGJ
BeHJ0YXN0dVFoUFFabFpPaWloZFRzTWpIVTRHRkxJNkhDNTFFR1VuQjJjV29hZ09CTExRaHV6bmFzeHdjTTNNZ054MDhJUkxMQlRMd3FBS0
01b0w4OTUwbXZGZXNxZmVLcExxieTdWZ1ZkWVU3R01VaEFtaVlPa1c2bzhmOC0wMTMtSFFjRnZ3QWdydWswOWp6XzF0bFdqOTFMUG0w
c1IzbmZ1TWozQSJ9.Bpifv2Kf4v4VRexhaMq369XVi_s36y5D9nvVCrSzjAOmthimAiz9-vUCuCAuKj2bYl5vxVTTbuWvy8YnM-0AqJyfTlyWY-
OIXnqJRSK1YzyZlQRjjUnTL560Re88Ga2QzGIsot2zjZDTu7nYhKZqR8ngVDhCNp_zqC17YJ5xeXMdXxSaWtVy6Rzk6gSp8dms738jHtoZ9RN3P
67bWx_pYr_OQ3nH5Z6zaVE5XP3uq2niFIS06ktIhQZTJqAU7GEClWjMThI2-_IXlQh4QRTpWxoVtGvp6Et84ZymQDfmx6sJTItIByUk6-
R5qd7rLe1I7s_g44SYLV0tFq1i90eywA