govroam

WHITEPAPER

Soevereiniteit van de digitale identiteit

Hoe een Nederlandse federatie helpt om de toegang tot het IT-landschap veilig te stellen.

Erik Dobbelsteijn,
Technisch directeur Stichting govroam

Juni 2025

Soevereiniteit van de digitale identiteit

Hoe een Nederlandse federatie helpt om de toegang tot het IT-landschap veilig te stellen.

Soevereiniteitsbeleid is een strategie, geen product. De basis van zo'n beleid is besef van de kerndata en functionaliteit in het IT-landschap en het nastreven van flexibele inzet van IT.
Waarschuwingen worden frequenter en indringender[1] en meer en meer organisaties in de publieke sector worden zich bewust van hun afhankelijkheid van buitenlandse leveranciers en de politieke invloed daarop. De mogelijkheden om los te komen van Big Tech zijn er, maar moeten zich in de praktijk nog bewijzen. Twee essentiële zwaartepunten van het IT-landschap moeten snel en volledig verplaatst kunnen worden: de data en de identiteiten van de organisatie. Aan de data wordt veel aandacht besteed door leveranciers en organisaties, maar hoe zit het met de identiteiten van de medewerkers?

Inhoudsopgave

Digitale soevereiniteit en databescherming: belangrijker dan ooit

Wanneer gesproken wordt over digitale soevereiniteit, is het hoofdthema vooral de continuïteit van de bedrijfsvoering. Hoe waarborgen we deze als er problemen optreden bij 'Big Tech' leveranciers. Hoe kunnen medewerkers in dat geval nog steeds werken, communiceren, en veilige toegang tot hun data krijgen?

Dat de data al tijden in handen is van een (of meer) buitenlandse partijen is een feit dat – als het goed is – benoemd wordt in een Data Protection Impact Analyse (DPIA).
Een significant aantal overheidsorganisaties heeft gekozen voor een of meerdere cloudproviders. En steeds meer toepassingen zijn zelfs 'cloud only' waarbij de provider bepaalt waar de data opgeslagen wordt en waarbij veel gebruik gemaakt wordt van AWS, Google Cloud of Azure. In technisch opzicht is de data van de organisatie in te zien door de provider, en is daarmee in feite ook opvraagbaar door de overheid door wetgeving waar de provider aan te gehoorzamen heeft. Dat geldt zelfs voor Nederlandse toepassingen, omdat die vaak ondergebracht zijn bij AWS, Google Cloud of Azure.

Dit risico werd vooralsnog geaccepteerd op basis van allerlei afwegingen, zoals uitbesteden versus zelf doen, de gevoeligheid van de data of vertrouwen dat een bondgenootschap de data van de organisatie beschermt. Providers proberen zorgen weg te nemen door termen als 'end-to-end encryptie', 'opslag in Europese datacenters', en hanteren inmiddels ook zelf het begrip 'soevereiniteit', maar de naakte waarheid is dat bijvoorbeeld de Amerikaanse regering toegang tot data op Europese servers kan afdwingen. Dat kan zelfs zonder enig digitaal spoor van deze activiteiten achter te laten. En indien 'auditing' daadwerkelijk actief is, is het maar de vraag of deze zichtbaar is voor de klant.

Recent heeft de Amerikaanse overheid laten zien dat ze succesvol invloed kan uitoefenen op de strategie van Big Tech, zoals dat al bekend is van andere naties. Alleen organisaties die hier verregaande maatregelen tegen nemen, kunnen de data afschermen, wat op haar beurt ook leidt tot beperkte functionaliteiten.

Exit-strategie en soevereiniteitsbeleid: werkbaar?

De roep om meer aandacht voor soevereiniteit en autonomie neemt toe. De praktijk is echter zeer weerbarstig. De huidige fase van bewustwording leidt tot de formulering van 'exit-strategieën' en 'soevereiniteitsbeleid'. Het risico bestaat dat dergelijke plannen papieren tijgers oplevert en geen waterdichte en praktische oplossing bieden als de nood aan de man is. Bijvoorbeeld wanneer de exit-strategie bestaat uit overstappen naar een andere cloudprovider. Daar zitten nogal wat haken en ogen aan, en de ene cloudprovider is de andere niet. Verschillende dataformaten en uiteenlopende functionaliteiten zijn belangrijke barrières. Bovendien zullen ze in geval van een calamiteit bij de vaste cloudprovider heel druk zijn met het 'onboarden' van vele andere organisaties en is maar zeer de vraag of een migratie snel genoeg kan worden afgerond.

Het startpunt van een mitigatie-maatregel begint met de kern van de IT-dienstverlening: welke data en welke functionaliteit is het meest cruciaal voor de organisatie? Hoe lang kan deze functionaliteit gemist worden? Deze antwoorden zijn nodig om de alternatieven in kaart te kunnen brengen.

De oplossing is niet eenvoudig; IT-managers zitten al snel klem. De alternatieven zijn namelijk niet een kwestie van simpelweg uploaden van de back-up. Bovendien kosten ze flink wat tijd om op te zetten en te koppelen. Er is een grotere en meer ervaren IT-afdeling voor nodig, in tijden van schaarste van deze expertise. Vervolgens moeten de eindgebruikers omschakelen naar de nieuwe manieren van werken. Een gewenningsproces maar ook meer inspanning in het dagelijkse werk omdat er minder hechte integratie is tussen de verschillende applicaties en functionaliteiten.

Sommige functionaliteit zal zelfs helemaal niet overgezet kunnen worden. Bijvoorbeeld de gedigitaliseerde kennisopbouw in het AI-model van de vorige leverancier die niet over te dragen is naar een andere cloudprovider. Efficiëntere zoekfuncties, datamining met AI en allerlei andere hulpmiddelen waar een cloudprovider zijn AI-model mee getraind heeft, zijn niet zijn niet compatibel of beschikbaar bij een andere cloudprovider. Dit is een fundamentele uitdaging van AI: de kennis die het neurale netwerk heeft geleerd is niet deterministisch te isoleren en aan te passen in het model, net zoals een menselijke herinnering niet in specifieke hersencellen is opgeslagen

Al deze aspecten moeten geregeld worden voor de operationele en kantoordata die van belang is voor de 'core business', maar vooral ook voor de digitale identiteit van de medewerkers. Zolang de gebruikersdatabase niet soeverein is, bestaat het risico dat in één klap het hele applicatielandschap ontoegankelijk wordt indien die gebruikersdatabase niet beschikbaar is.

Om de doelmatigheid van alternatieven te kunnen bepalen, moeten we eerst een aantal cruciale vragen beantwoord zien. Zijn deze alternatieven grondig onderzocht vóórdat de nood aan de man is? Zijn alle betrokken afdelingen zich bewust van het plan? Is het plan getest en aangepast? Moet de geselecteerde oplossing niet al parallel draaien om snel over te kunnen schakelen? Is dat niet kostbaar? Is het dan niet verstandig om maar helemaal te switchen naar het alternatief?

We naderen het kernpunt van dit betoog. Alle IT-handelingen die medewerkers verrichten beginnen bij hun eigen digitale identiteit. De interne database met identiteiten, de interne 'Identity Provider' of 'IdP' is het startpunt van alle IT die door medewerkers wordt gebruikt. De borging van die identiteiten, en de uitwijkmogelijkheden voor het onderbrengen en adequaat beschermen ervan, is de start van elk migratieplan.
Hoe heeft uw organisatie dit geregeld? Is er nog geen on-premise gebruikersdatabase meer? En bevindt zich ook geen actuele kopie in een andere cloud? Dan is er waarschijnlijk geen goede 'backup' van de user accounts. En zonder user accounts is elk IT-landschap onbereikbaar voor de gebruikers.

Federatie als oplossing: govConext

In grote organisaties zwerven accountgegevens rond in diverse systemen: het personeelsysteem, de Active Directory, de EntraID, het CRM, een integraal IAM-middlewaresysteem etc. Interne applicaties zijn gekoppeld aan de AD of EntraID, externe applicaties worden ontsloten via EntraID of via een IAM-broker.
Het is verleidelijk om accounts te kopiëren naar andere systemen, al dan niet bij andere cloudleveranciers. Dat veroorzaakt onmiddellijk synchronisatie-uitdagingen en een vergroting van de datafootprint. Hetzelfde risico is er bij het kopiëren naar een leverancier buiten Nederland.

De simpelste, meest overzichtelijke en veilige manier om accounts veilig te houden, is om de login-gegevens ('credentials') op slechts één plek op te slaan. Andere systemen zullen wel gebruikers*profielen* bevatten met daarin applicatie-specifieke autorisaties en eigenschappen. Maar de login moet liefst altijd maar via één login-scherm met dezelfde credentials en multi-factor (MFA) plaatsvinden. Dat is de enige manier om te voorkomen dat verlopen of geblokkeerde credentials nog gebruikt kunnen worden. Een uitdaging die in omvangrijke en ingewikkelde IAM-projecten aangegaan wordt.

Om eenduidige aanmelding ook voor externe (cloud-)applicaties voor elkaar te krijgen, is een single sign-on-koppeling met elk van die externe applicaties nodig. Tijdrovend, onderhoudsgevoelig en erg onoverzichtelijk.

Hoe aangenaam zou het zijn om met een vinkje een dienst van een alternatieve leverancier te kunnen activeren? Flexibiliteit die een fundament van het soevereiniteitsbeleid mogelijk maakt in de praktijk.
In het onderwijs is hiervoor al geruime tijd een belangrijke bouwsteen beschikbaar. SURF – de ICT-coöperatie van onderwijs en onderzoek – heeft zo'n 10 jaar geleden een platform ontwikkeld onder de naam SURFconext. Hierop zijn de meest onderwijsinstellingen en ca. 2.000 serviceproviders aangesloten. Stichting govroam biedt deze dienst sinds eind vorig jaar aan voor de publieke sector onder de naam govConext.

De govConext-dienst van Stichting govroam biedt een eenvoudige oplossing voor de wildgroei aan koppelingen met dienstenleveranciers en de locaties waar identiteitsgegevens rondzwerven. Stichting govroam is federatief georganiseerd. De federatie vormt inmiddels een groeiende verzameling van gebruikersorganisaties (Identity Providers) enerzijds, en dienstverleners (Service Providers) anderzijds.

Wat is govConext?

GovConext is een open source modulair platform, ontwikkeld en gehost in Nederland, dat universeel en op open standaarden koppelt met alle mogelijke IAM-oplossingen, inclusief EntraID.

Aan de ene kant koppelen organisaties in de publieke sector hun gebruikers via het SAML-protocol. Dat maakt het mogelijk om gebruikers te laten inloggen op andere websites via de loginpagina van de eigen organisatie zonder dat deze website weet heeft van de logingegevens. GovConext levert alleen die informatie aan de Serviceprovider die strikt noodzakelijk is en toegestaan wordt door de beheerder en de gebruikers zelf.

Aan de andere kant koppelen serviceproviders, hiermee bedienen zij een grote groep organisaties als potentiële klant. Via een web interface kunnen beheerders eenvoudig aanvinken welke groepen gebruikers bij welke diensten mogen, en eenvoudig nieuwe diensten en online applicaties aanvinken zonder deze technisch te hoeven koppelen.

In feite is govConext een ecosysteem waaraan zowel gebruikers als applicaties gekoppeld zijn, dat IT-beheerders de mogelijkheid geeft om eenvoudig applicaties toe te voegen aan hun landschap, op een voor hun gebruikers laagdrempelige manier. De dienstverleners die aansluiten hebben toegang tot een groot en groeiend potentieel van mogelijke klanten.

Door deze architectuur:

1. blijven alle identiteitsgegevens bij de gebruikersorganisatie. Eindgebruikers kunnen precies zien welke informatie er met een leverancier uitgewisseld wordt. Veilig en privacy vriendelijk, inclusief de mogelijkheid het recht om vergeten te worden.
2. zijn authenticatie, autorisatie, groepsbeheer en afspraken over privacy en beveiliging bij govConext centraal geregeld.
3. wordt bespaard op het beheer; Er is slechts één koppeling nodig, in plaats van een koppeling met serviceprovider.

Voor gemeentes, die veelal gebruik maken van EntraID, is het goed om te weten dat de federatieve logindienst govConext complementair is aan Common Ground. Beiden vormen bouwstenen in het gemeentelijk applicatielandschap. Daar waar Common Ground de ontsluiting van data richting applicaties beveiligt en standaardiseert, zorgt govConext ervoor dat de gebruikersinterface veilig en gestandaardiseerd ontsloten wordt.

Vormt het inschakelen van een extra component in het IT-landschap niet een additioneel risico? Dat is slechts beperkt zo.

- GovConext is volgens alle regelen der kunst zodanig opgetuigd dat de beschikbaarheid geen bottleneck zal vormen (uiteraard meervoudige redundantie op basis van containerisatie, geografische scheiding etc.).
- Bovendien is het gebruik van de browser-gebaseerde SAML-standaard essentieel: govConext leidt alleen om, de login vindt altijd plaats bij de IdP van de eigen organisatie waarvan de beschikbaarheid het meest op het kritieke pad van het inlogproces ligt.

Doordat govConext (of feitelijk de onderliggende open source code) als universele kroonsteen is ontwikkeld, biedt deze juist mogelijkheden om redundantie in het loginproces toe te voegen. Daarover hieronder meer.

De voordelen van govConext

- **Veilig en privacy vriendelijk**: informatiebeveiliging en privacy-bescherming zijn geborgd in de techniek. Identiteitsgegevens blijven bij de identity-provider, AVG proof, met ondersteuning voor verschillende betrouwbaarheidsniveaus. Dataminimalisatie en security by design. Implementatie van het recht vergeten te worden.
- **Toekomstbestendige oplossing**, gebaseerd op innovatieve SURF-technologie. Architectuur en dienstverlening, wordt gezien als een robuuste en bewezen oplossing, met een sterke voetafdruk in zowel de onderwijssector als de rijksoverheid.
- GovConext ondersteunt **selfservice-functionaliteiten** voor gebruikers, zoals het zelf beheren van multi-factor authenticatie, wat de operationele efficiëntie verhoogt en de druk op de servicedesk vermindert.
- GovConext zorgt voor **lagere operationele kosten** door centrale governance, sneller schakelen en minder koppelingen aan te leggen en te beheren. Het is een geïntegreerde oplossing die is afgestemd op de behoeften van de organisatie, door gedelegeerd beheer naar IdP's en SP's (Identity Providers en Service Providers).
- **Hosting in Nederlandse datacenters** dus betere aansluiting bij zorgvereisten en privacy- en databeveiligingswetten, hulpmiddel bij het bereiken van digitale soevereiniteit.

Naast deze voordelen biedt govConext een aangesloten dienstenleverancier (serviceprovider) nog een aantal pluspunten:

- Versterking van de **positie als overheidsleverancier**. De aansluiting op govConext helpt leveranciers en publieke organisaties om te voldoen aan aanbestedingseisen, wet- en regelgeving én versterkt hun rol als betrouwbare partner voor overheidsdiensten.
- GovConext wordt breed ingezet in de publieke sector. Het is de **'default' oplossing voor SSO** in de publieke sector

Maar govConext biedt meer dan single sign-on:

- Centraal punt voor operationele aanpassingen
- Inzicht in en controle over privacyaspecten
- Account life cycle management: zodra IdP account deactiveert kan gebruiker niet meer inloggen
- Self Service Portalen voor Service Providers, Identity Providers en Eindgebruikers: centraal beheer van de autorisaties en toegestane applicaties, inclusief benodigde beveiligingsniveaus
- Versterking van authenticatiemiddelen (MFA) op diverse niveaus, eIDAS compliant (laag, substantieel en hoog) door middel van de 'govSecureID'-module (die FIDO2 tokens en de govSecureID app als extra authenticatiefactor kan toevoegen)
- Gasttoegang voor niet-IdP gebonden personen mogelijk (met de 'Invite' module)
- Beveiligen van API-toegang op basis van OIDC
- Bouwsteen voor digitale soevereiniteit (met de 'govID'-module als alternatieve IdP die gasttoegang kan bieden maar ook overloop in geval van problemen met de eigen IdP)

Doorslaggevende meerwaarde voor eindgebruikers:

- Veilige toegang
- Met één account overal online (één wachtwoord, één MFA type)
- Aanpassingen (wachtwoord, naamswijziging) bij eigen organisatie
- Inzicht in en controle over privacy-aspecten, zoals recht om vergeten te worden
- Eenvoudig aanvragen nieuwe dienst (na verificatie door beheerder)
- Eenvoudig toegang tot govroam-diensten zoals getgovroam, govguest, govVPN die de beleving van toegang tot govroam-wifi vergemakkelijken.

Soeverein scenario:
digitale identiteiten veiligstellen via govConext

Naast de eenvoudig en beveiliging van govConext voor het dagelijks gebruik van applicaties op het internet, kan govConext dus een rol spelen in een uitwijkscenario. Daarvoor is niet veel méér nodig dan een standaard aansluiting.

Om voorbereid te zijn op een scenario waarin de gebruikersdatabase niet meer bereikbaar is, kunnen medewerkers vlot en veilig een govID-account aanmaken. Wanneer de noodsituatie zich voordoet, is door mogelijk om door middel van een beleidsregel in govConext deze medewerkers op basis van hun govID (tijdelijk) alsnog toegang te bieden tot alle applicaties die ze al via govConext gebruikten.

Of beter: de alternatieve IAM-oplossing die de organisatie kiest om haar soevereiniteit te waarborgen kan parallel aan de primaire IdP aan govConext verbonden worden waardoor het hele applicatielandschap in noodgevallen op dezelfde manier ontsloten blijft. Heel eenvoudig.

Samengevat: koppel de primaire en secundaire gebruikersdatabase beiden aan govConext en wees gegarandeerd van toegang tot dezelfde applicaties. Met als bonus extra functionaliteit zoals gastgebruik, de mogelijkheid om sterkere authenticatiefactoren af te dwingen, autorisatiegroepen dynamisch in te regelen en nog veel meer.

Conclusie

Het IT-landschap voor lagere overheden leeft al grotendeels in de cloud en ook in de andere geledingen van de publieke sector wordt hier volop gebruik van gemaakt. Alhoewel het bewustzijn bestaat dat hiermee een grote (geopolitiek gevoelige) afhankelijkheid is ontstaan van Big Tech, liggen volwaardige en compatibele alternatieven niet voor het oprapen. Het kost veel tijd om 'om te schakelen' en gebruikers te laten wennen aan potentieel minder functionaliteit.
Door de IAM-componenten van de enterprise-architectuur te koppelen met de govConext-federatie van Stichting govroam wordt een veilige, leveranciersonafhankelijke en gestandaardiseerde beveiliging van applicatie-toegang realiteit. De eindgebruikers, maar ook hun management, voeren weer zelf de regie over privacygevoelige gegevens. Zodra de organisatie is aangesloten, kunnen voordelen zoals AVG-compliancy, snel onboarden van nieuwe applicaties en eenvoudiger life cycle management van identiteiten ('uit diensttreding') verzilverd worden.
Als bonus biedt de govConext-federatie de mogelijkheid om snel te schakelen mocht zich om welke reden dan ook een probleem bij een cloudprovider voordoen.

Meer informatie: www.govroam.nl

1)
https://www.ft.com/content/956ccaa6-0537-11ea-9afa-d9e2401fa7ca
https://deingenieur.nl/artikelen/doorbreek-de-afhankelijkheid-van-big-tech
https://www.binnenlandsbestuur.nl/digitaal/natuur-en-milieu/waarschuwing-voor-stille-verhuizing-overheids-ict
https://www.rekenkamer.nl/binaries/rekenkamer/documenten/rapporten/2025/01/15/het-rijk-in-de-cloud/Het+Rijk+in+de+cloud.pdf