TOOLS4EVER

Whitepaper V2.0 / 22 07 2022

HelloID Security

Hoe Tools4ever (persoons)gegevens beveiligt en privacy van gebruikers waarborgt binnen HelloID

Inhoudsopgave

Zorgeloos en veilig beheer van gebruikers en autorisaties

Tools4ever is een Nederlands softwarebedrijf en marktleider op het gebied van Identity & Access Management (IAM). Sinds 1999 helpt Tools4ever organisaties bij het efficiënt en veilig beheren van hun gebruikers en autorisaties: Tools4ever ontwikkelt software voor zowel kleine bedrijven van zo'n 300 werknemers als voor grote multinationals met meer dan 200.000 gebruikers. Inmiddels vertrouwen al meer dan 5.000 klanten voor zeker 10 miljoen gebruikers op de IAM-oplossingen van Tools4ever.

Van on-premise naar cloud

Tools4ever heeft ruim 20 jaar aan kennis en expertise met twee generaties van on-premise IAM-oplossingen vertaald naar een modern en veilig cloud-gebaseerd IAM-platform: HelloID. HelloID is als Identity-as-a-Service (IDaaS) sinds 2015 beschikbaar in de cloud. Traditionele IAM-oplossingen zijn complex en vereisen voor elke wijziging specialistische consultants, maar HelloID legt de kracht van Identity & Access Management in de handen van onze klanten en partners. Met user account provisioning, self-service workflows, single sign-on en multi factor authenticatie krijgen je gebruikers snel en veilig toegang tot hun applicaties en gegevens, waar ze ook zijn in de wereld. De dienst is altijd beschikbaar, wordt regelmatig geüpdatet en uitgebreid met nieuwe functionaliteiten, en de beveiliging is te allen tijde van het hoogste niveau is.

Focus op privacy, informatiebeveiliging en compliancy

Verscherpte wet- en regelgeving (AVG/GDPR, meldplicht datalekken) en informatiebeveiligingsrichtlijnen (ISO 2700x, BIO, NEN 7510, IBP) vereisen dat organisaties maatregelen nemen op het gebied van privacy en informatiebeveiliging. IAM is een discipline binnen de cyberbeveiliging die organisaties helpt om de juiste personen op het juiste moment van de juiste autorisaties en toegang te voorzien. Om dit resultaat te kunnen realiseren werkt de IAM-oplossing zelf ook met veel privacygevoelige data. Bij de selectie van beveiligingssoftware is het dan ook belangrijk om de volgende vragen te stellen:

- Hoe kunnen wij bepalen wie toegang kan krijgen, waartoe zij toegang kunnen krijgen, en hoe zij toegang kunnen krijgen?
- Hoe worden koppelingen met andere systemen en applicaties gemaakt? Welke gegevens worden via de koppelingen gedeeld? Hoe worden de verbindingen beveiligd?
- Hoe en welke gegevens worden opgeslagen? Hoe worden ze gecodeerd? Welke controle hebben wij over onze gegevens? Hoe zorgen wij ervoor dat deze gegevens niet buiten de organisatie kunnen lekken?
- Hoe bepalen en controleren we wie welke handelingen uitvoert? Hoe reageren we snel als er verdachte activiteit plaatsvindt?

Beveiliging van onze software en de veiligheid van de opslag van (persoons)gegevens vinden we bij Tools4ever heel belangrijk. Daarom hebben we geïnvesteerd in passende middelen en controles om onze klanten te beschermen. Met onze software ben je er zeker van dat:

- **Je informatie is beschermd** – Tools4ever beschermt vertrouwelijke informatie van onze klanten. We gaan voor de beste klantervaring.
- **Je kunt continu over onze dienstverlening beschikken** – Onze diensten zijn ononderbroken beschikbaar en Tools4ever minimaliseert proactief veiligheidsrisico's die de continuïteit bedreigen.
- **Je informatiebeveiliging voldoet aan normen en wetgeving** – Tools4ever conformeert zich aan wetgeving, best practices en industriestandaarden.

Deze drie principes zijn voor ons leidend: wij richten ons continu op het verfijnen van bestaande controles en implementeren van nieuwe risico minimaliserende maatregelen.

In dit document lees je in meer detail hoe Tools4ever de veiligheid van gegevens en waarborging van de privacy binnen de modulen Provisioning, Service Automation en Access Management van HelloID garandeert.

HelloID cloudplatform

HelloID is een cloudplatform dat uit drie modulen bestaat die zowel los van elkaar als geïntegreerd met elkaar functioneren. Op basis van de behoefte(n) aan gebruikers-, autorisatie- en toegangsbeheer en self-service, kunnen modulen flexibel in- en uitgeschakeld worden.

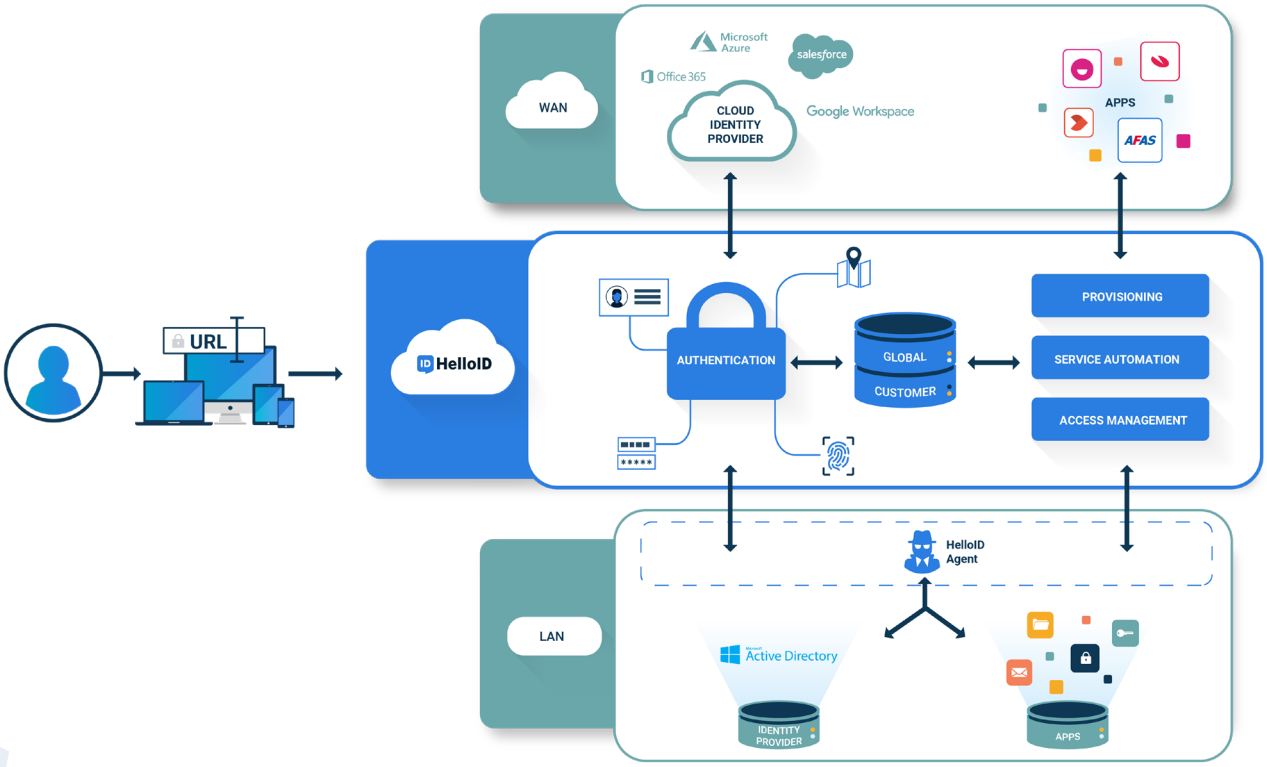
- **Provisioning**
  Geautomatiseerd beheer van gebruikersaccounts en rolgebaseerd autorisatiebeheer op basis van de identity lifecycle middels een koppeling tussen bron- en doelsystemen.

- **Service Automation**
  Self-service en gedelegeerde formulieren om gestructureerd, gestandaardiseerd en geautomatiseerd wijzigingen af te handelen die niet op basis van een bronsysteem kunnen worden uitgevoerd.

- **Access Management**
  Veilige en gebruiksvriendelijke toegang tot applicaties en gegevens middels één set inloggegevens, optionele twee factor authenticatie en volgens vooraf gedefinieerde en conditionele toegangsregels.

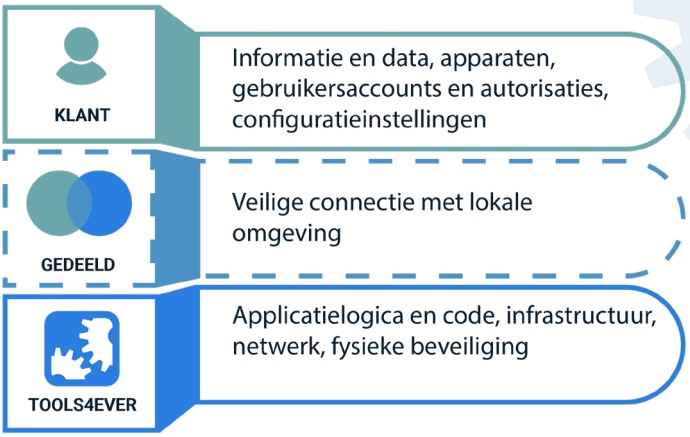
Architectuur

De HelloID-architectuur bestaat uit verschillende gedeelde en separate componenten. In het onderstaande diagram krijg je een overzicht van de belangrijkste componenten en de onderlinge interactie. Informatie wordt altijd versteuteld, of die nu in beweging is of tijdelijk wordt opgeslagen. De mate van beveiliging verschilt per onderdeel en is afhankelijk van de mate van impact, risico en technische toepasbaarheid.



Gedeelde verantwoordelijkheid

In het geval van een SaaS-oplossing als HelloID is het essentieel om de gedeelde verantwoordelijkheid voor de informatiebeveiliging te begrijpen. Het *shared responsibility model* bakent onze verantwoordelijkheden af: van Tools4ever – de SaaS-leverancier – en van jou – als klant, en eindgebruiker van de softwareoplossing.



Verantwoordelijkheid van Tools4ever

Tools4ever is verantwoordelijk voor de beveiliging van het HelloID-platform met inbegrip van de fysieke beveiliging, de beveiliging van de applicatie zelf en de onderliggende infrastructuur. Daarnaast is Tools4ever verantwoordelijk voor de bereikbaarheid van de dienst en voorzien we in mechanismen om de data binnen HelloID te beschermen. De beveiligingsmaatregelen die door Tools4ever zijn geïmplementeerd en beschikbaar worden gesteld vind je in het volgende hoofdstuk: Beveiligingsmaatregelen.

Verantwoordelijkheid van klant

Als klant blijf je altijd eigenaar van je eigen gegevens. Daarmee ben je ook verantwoordelijk om de data die binnen HelloID wordt opgeslagen te beveiligen tegen en te monitoren op ongewenste toegang, de juistheid van de gegevens te waarborgen, en te beschermen tegen kwaadwillenden. Dit omvat onder meer het afdwingen van een sterk authenticatiebeleid, het correct beheren van de gebruikers en hun autorisaties, en het beoordelen van de binnen HelloID beschikbare logging.

Beveiligingsmaatregelen

De manier waarop wij onze oplossingen ontwerpen, ontwikkelen en onderhouden is gebaseerd op tien belangrijke principes. Deze *Security by Design Principles*, zoals gedefinieerd door OWASP, vormen de basis van onze aanpak:

1	**Minimaliseer aanvalsoppervlak**	Ons doel voor veilige ontwikkeling is het verminderen van het totale beveiligingsrisico door het zogeheten 'aanvalsoppervlak' te verkleinen. Elke functie die aan een applicatie wordt toegevoegd, voegt een bepaald risico toe aan de applicatie als geheel.
2	**Veilige standaardinstellingen**	Standaard leveren we een zo veilig mogelijke gebruikerservaring. Het is aan de applicatiegebruiker –met inachtneming van zijn of haar mandaat – om het standaardbeveiligingsniveau te verlagen.
3	**Principe van least-privilege**	Accounts hebben standaard de minimale rechten die nodig zijn om de noodzakelijke bedrijfsprocessen uit te voeren. Dit omvat niet alleen gebruikersrechten, maar ook minimale vereisten aan CPU-limieten, geheugen, netwerk en het bestandssysteem.
4	**Principle of defense in depth**	Zelfs wanneer één controle redelijk zou zijn, geven wij de voorkeur aan meer controles om risico's op verschillende manieren aan te pakken. Dit principe kan ervoor zorgen dat ernstige kwetsbaarheden buitengewoon moeilijk te misbruiken zijn en ze zo onwaarschijnlijker te maken.
5	**Veilig falen**	Een applicatie kan om verschillende redenen falen bij de uitvoer van processen. Het resultaat van zo'n fout bepaalt echter of een toepassing veilig is of niet. Alle HelloID- componenten zijn ontworpen om veilig te falen.

6	**Vertrouw diensten niet standaard**	Derden zullen doorgaans een ander veiligheidsbeleid en andere procedures hebben dan wij. Daarom vertrouwen we externe systemen niet blindelings en behandelen we alle externe systemen op dezelfde manier.
7	**Functiescheiding**	Dit is een essentieel onderdeel van beveiliging van de processtromen. Beheerders mogen normaliter bijvoorbeeld geen gebruikers van de toepassing zijn.
8	**No security by obscurity**	In onze visie moet de veiligheid van belangrijke systemen niet alleen steunen op het verbergen van details. Wij beschouwen dit als een zwakke beveiliging.
9	**Houd beveiliging simpel**	Onze benadering geeft de voorkeur aan eenvoudige code in plaats van overmatig complexe benaderingen. Er worden geen dubbele negatieven of complexe architecturen gebruikt, tenzij absoluut noodzakelijk.
10	**Los beveiligingsproblemen goed op**	Zodra een beveiligingsprobleem is geïdentificeerd, is het belangrijk om er een test voor te ontwikkelen en om de hoofdoorzaak van het probleem te begrijpen. Wanneer ontwerppatronen worden gebruikt, is het waarschijnlijk dat het beveiligingsprobleem wijdverspreid is in alle 'code bases', dus het ontwikkelen van de juiste oplossing zonder terugvallen te introduceren is essentieel.

Datacenters van internationaal erkende leiders

HelloID wordt gehost op de cloudplatforms Microsoft Azure en Google Cloud. Onze cloudpartners Microsoft en Google zijn internationaal erkend als wereldwijde leiders op het gebied van Infrastructure-as-a-Service (IaaS). Ze hebben cloud-infrastructuren geïmplementeerd die volledig voldoen aan de wereldwijde en lokale eisen. De dienst is bestand tegen ongeregeldheden en aanvallen van kwaadwillenden, doordat de infrastructuur wordt beschermd op de fysieke, netwerk-, host-, toepassings- en gegevenslagen. Er worden strikte beveiligingsrichtlijnen en operationele processen toegepast. Verder worden de diensten voortdurend proactief gemonitord en worden er penetratietesten uitgevoerd.

Gegevens veilig opgeslagen in de EER

Microsoft Azure en Google Cloud beschikken over de gehele wereld over datacenters die per regio zijn opgesplitst. Het onderscheid in regio's maakt het voor jou als klant mogelijk om elk HelloID-portaal in de gewenste regio te plaatsen. HelloID maakt momenteel gebruik van datacenters in twee regio's: de Europese Economische Ruimte (EER) en het westen van de Verenigde Staten. De data van onze Nederlandse klanten en partners worden standaard enkel in de Europese Economische Ruimte opgeslagen. Hiermee voldoet Tools4ever aan eisen die de AVG stelt aan de locatie van gevoelige data.

Hoge beschikbaarheid en continuïteit

Het HelloID-platform is gegarandeerd tot 99,90% per jaar beschikbaar. Dit is onder meer mogelijk door de maatregelen die onze hostingproviders hebben getroffen omtrent datareplicatie binnen de regio, back-updiensten en redundantie van de stroom-, netwerk- en koelvoorzieningen.

De beschikbaarheid en prestaties van HelloID worden continu gemonitord. Informatie over de actuele en historische beschikbaarheid, (gepland) onderhoud en storingen is publiekelijk toegankelijk via de HelloID-statuspagina. Schrijf je in voor de statusupdates, dan word je bij ongeregeldheden direct per mail op de hoogte gesteld.

Geautomatiseerde back-ups

Tools4ever maakt van alle databases geautomatiseerde back-ups. De gegevens worden 30 dagen bewaard. Het is mogelijk om de database via Point-in-Time-Recovery (PITR) met intervallen van 4 uur te

herstellen. Hierdoor is het mogelijk om data te herstellen tot een willekeurig moment in de afgelopen 30 dagen binnen de gestelde interval. In een geval van een incident kan de database daarom veelal worden hersteld tot vlak voor het moment dat een probleem zich voordeed. De toepassing van PITR betekent dat data met geen tot minimaal dataverlies hersteld kan worden.

HelloID encryptie, verificatie en certificaten

Certificaten waarborgen zowel de identiteit als de veilige encryptie van een website, individu, organisatie, apparaat, gebruiker of server. Binnen de HelloID-software wordt encryptie op verschillende lagen toegepast.

Gescheiden en versleutelde databases

Tools4ever biedt met HelloID een schaalbare multi-tenant SaaS-oplossing. De gebruikersinterface en API's beperken de toegang tot alleen die gegevens waartoe het klantportaal geautoriseerd is. De data is logisch gescheiden in verschillende databases die worden versleuteld met AES 256-bit encryptiesleutels. De algemene HelloID-database bevat globale configuratie-instellingen en portaalgegevens. Alle klantspecifieke configuraties en gebruikersgegevens worden per portaal opgeslagen in een eigen klantendatabase. De gegevens in deze database worden gecodeerd met een eigen encryptiesleutel. Door deze opzet zijn alle tenants van elkaar geïsoleerd en is er geen risico op cross-portal toegang of datavervuiling.

Veilige communicatie over internet

Communicatie over het internet moet te allen tijde op een veilige manier gebeuren. De HelloID-webserver communiceert met componenten via het internet met behulp van HTTPS. Het niveau van encryptie is TLS 1.2, AES met 256-bit encryptie. Bij het gebruik van de third party identity provider (IDP) Active Directory heb je een IIS-webserver nodig.

Gebruik van een eigen URL

Standaard krijgt je organisatie de beschikking over een eigen subdomein: 'organisatienaam.helloid.com', dat toegang geeft tot HelloID. Je kunt ook de HelloID-URL vervangen door een eigen domeinnaam om zo de herkenbaarheid voor je organisatie te vergroten. Veel voorkomende domeinnamen zijn bijvoorbeeld 'login.organisatienaam.nl' of 'helloid.organisatienaam.nl'. Aangezien de communicatie met HelloID via HTTPS plaatsvindt heb je een PFX-certificaat nodig. Dit kan een wildcard- of een domeincertificaat zijn voor de gevraagde URL. De koppeling tussen HelloID en het domein wordt gevalideerd middels een CNAME-record.

Als je een eigen domeinnaam wilt gebruiken, wordt het aanbevolen om die direct na het aanmaken van het portaal te configureren. Als je de URL later wijzigt kan dat invloed hebben op de werking van identity providers, single sign-on, en connecties met de lokale omgeving.

Veilige verbinding met lokale infrastructuur via HelloID Agent

De standaardconfiguratie van HelloID is volledig cloud-to-cloud. Voor organisaties die volledig cloud-gebaseerd werken, werkt HelloID dus ook zonder on-premise componenten. Een optionele on-premise 'agent' is echter wel vereist wanneer HelloID moet interfacen met lokale bronnen zoals een Active Directory, het bestandssysteem of een database. De HelloID Agent is een set van drie lichtgewicht Windows-services die binnen het netwerk van je organisatie worden geïnstalleerd. De Windows-services maken communicatie met de verschillende HelloID-modulen mogelijk.

Je kunt meerdere agents installeren ten behoeve van load balancing en de scheiding van taken. Wanneer er meerdere agents zijn worden ze gegroepeerd in Agent Pools. Als een on-premise taak wordt opgestart, wordt die naar een Agent Pool gestuurd, die dan bepaalt welke HelloID Agent in die pool beschikbaar en geschikt is voor de uitvoering van de taak. Elke Agent Pool heeft minstens één HelloID Agent nodig om te functioneren.

Installatie, verificatie en communicatie

De HelloID Agent is dus een 'broker' die data uitwisselt en lokaal acties uitvoert. Communicatie over het internet moet altijd op een veilige manier gebeuren. Een proces met drie stappen verzekert veilige communicatie tussen HelloID en de agent.

Installatie

De HelloID Agent communiceert met componenten via het internet met behulp van HTTPS. Het niveau van encryptie is TLS 1.2, AES met 256-bit encryptie. De HelloID Agent kan op elke server in het domein worden geïnstalleerd die HTTPS-toegang heeft tot HelloID. Om conflicten met het lokale beveiligingsbeleid te voorkomen is dit in de regel een server die geen domaincontroller is. De services van de agent draaien op een domeinaccount met lokale admin-rechten. Het gebruik van een lokaal account kan leiden tot inlogproblemen voor eindgebruikers en falende synchronisatietaken. Zonder lokale admin-rechten kan de agent niet geautomatiseerd updaten.

Verificatie

Het verificatieproces zorgt ervoor dat je HelloID-portaal alleen de juiste instantie van de agent vertrouwt. Tijdens de installatie van de agent genereert HelloID een OTP-ticketnummer. Dit nummer kan maar één keer worden gebruikt, en alleen binnen 10 minuten na de creatie ervan. De HelloID-beheerder verstrekt dit nummer aan de agent. Op basis van een combinatie van de OTP, de portal URL, en de agent GUID wordt een gedeeld certificaat gegenereerd. Dit certificaat valideert vervolgens elke communicatiepoging tussen HelloID en de agent. Als het certificaat niet overeenkomt of als de agent GUID is veranderd, is communicatie onmogelijk. Als het certificaat of de agent wordt gekopieerd of verplaatst, wordt het vertrouwen onmiddellijk herroepen. Deze verificatieprocedure kan alleen worden uitgevoerd door HelloID-beheerders met de permissie om agents toe te voegen. Voor maximale beveiliging worden geen andere scenario's toegestaan.

Communicatie

De HelloID Agent werkt uitsluitend in één richting waarbij communicatie enkel van het lokale netwerk naar het HelloID-portaal plaatsvindt en nooit andersom. Hij voert alleen acties uit die door het HelloID-portaal worden klaargezet en kan zelf geen opdrachten naar het portaal sturen. Wanneer de agent reageert op een verzoek, controleert HelloID het afkomstige IP-adres. Als dit niet overeenkomt met het IP-adres dat gebruikt is tijdens de verificatie, wordt het commando afgewezen en wordt het vertrouwen onmiddellijk opgezegd. Er is geen speciale firewall poortopening of DMZ-configuratie nodig. De agent communiceert via de standaard TCP-poort 443. Alle events en verzoeken aan de agent worden opgeslagen in de logfiles. De agent ondersteunt verder onder meer load balancing, failover, en monitoring.

Directory Agent

De Directory Agent is een service die verantwoordelijk is voor on-premise taken die gerelateerd zijn aan het authenticeren op HelloID via Active Directory:

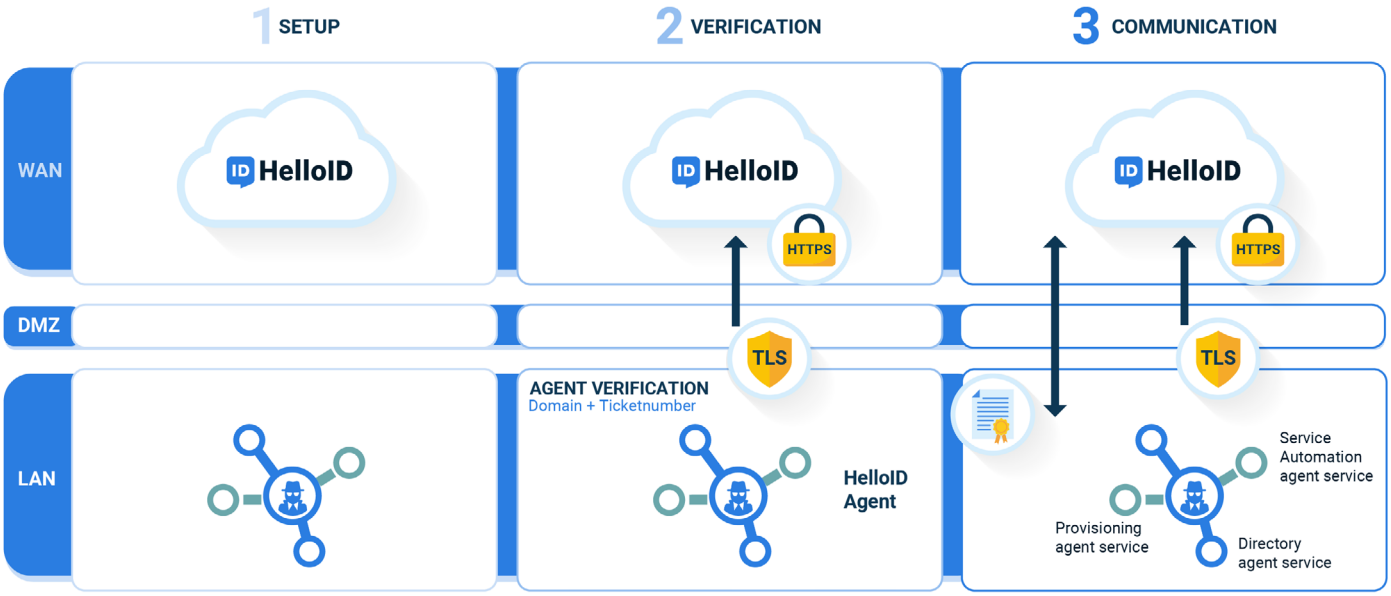
- authenticeren van gebruikers in HelloID bij gebruik van Active Directory als identity provider
- synchroniseren van gebruikersaccounts van Active Directory naar HelloID

De Directory Agent gebruikt HTTPS met *long polling*. Elk verzoek blijft 30 seconden open. Gedurende dit interval antwoordt de dienst elke vijf seconden met vijf processen die gelijktijdig pollen. De meeste verzoeken worden beantwoord in minder dan een seconde. Alle communicatie wordt versleuteld met behulp van HelloID-certificaten via TLS 1.2. Elk verzoek wordt geverifieerd aan de hand van het certificaat en de GUID van agent.

Provisioning Agent

De Provisioning Agent is een service die verantwoordelijk is voor on-premise taken die te maken hebben met de Provisioning-module van HelloID, zoals:

- het ophalen van gegevens uit lokale bronsystemen zoals HR- en SIS-databases
- het beheren van gebruikersaccounts en rechten in lokale doelsystemen zoals Active Directory en NTFS, maar ook in CSV-bestanden, SQL en Oracle-databases



De Provisioning Agent maakt gebruik van beveiligde WebSockets om open, bijna realtime communicatie met HelloID te onderhouden. Een initieel HTTPS-verzoek aan het HelloID-portaal wordt geüpgraded naar een beveiligde WebSocket. De WebSocket wordt elke drie uur gerecycled en heeft een 60 seconden heartbeat om te controleren of de verbinding open moet blijven. Alle communicatie wordt versleuteld met via HelloID-certificaten via TLS 1.2. Elk verzoek wordt geverifieerd op basis van het Agent-certificaat en de GUID. Deze dienst is geoptimaliseerd voor bijna realtime communicatie, stabiliteit en prestaties bij bulkverzoeken.

Service Automation Agent

De Service Automation Agent is een service die verantwoordelijk is voor alle taken die te maken hebben met de Service Automation module van HelloID. Denk aan de:

- uitvoer van PowerShell-scripts in het kader van het vullen van gegevensbronnen
- uitvoer van on-premise acties voor geplande taken, goedgekeurde self-service verzoeken en gedelegeerde formulieren

De Service Automation Agent deelt de beveiligingskenmerken van de Provisioning Agent. Deze service is geoptimaliseerd voor een snelle reactietijd ten behoeve van een vlotte gebruikerservaring. Taken die vanuit self-service en gedelegeerde formulieren worden klaargezet worden vrijwel direct opgepakt en uitgevoerd.

Authenticatie en autorisatie

Authenticatie omvat het proces waarbij de identiteit van een gebruiker wordt geverifieerd om na te gaan of de gebruiker is wie hij of zij beweert te zijn. Het als gebruiker of beheerder authenticeren op het HelloID-platform verloopt via één of meerdere zogenoemde *identity providers*. Een identity provider (IDP) is een systeem waarin identiteitsinformatie wordt beheerd. Voor de primaire authenticatie tot de HelloID-appllicatie ondersteunt HelloID twee typen identity providers:

- HelloID cloud directory
- Third party identity provider

Er kunnen meerdere identity providers tegelijkertijd actief zijn. In de praktijk wordt HelloID veelal gekoppeld met een third party IDP zoals (Azure) Active Directory of Google Workplace. De cloud directory geeft je organisatie dan aanvullend de mogelijkheid om toegang te bieden aan bijvoorbeeld klanten of patiënten zonder dat hiervoor een gebruikersaccount in Active Directory aangemaakt hoeft te worden.

Authenticatie via cloud directory

Bij authenticatie wordt de gebruiker geïdentificeerd via de in HelloID geïntegreerde cloud directory.Die identificatie gebeurt met een gebruikersnaam en gebruikers authenticeren zich met een wachtwoord. Deze accountgegevens worden opgeslagen in de cloud, waarbij het wachtwoord encrypted is opgeslagen. HelloID-beheerders in je organisatie kunnen de complexiteit en veiligheid van de lokale HelloID-gebruikersaccounts bewaken door een wachtwoordbeleid voor je organisatie te configureren. Ze kunnen bijvoorbeeld eisen stellen aan de wachtwoordsterkte op onder meer de lengte en complexiteit, of veel voorkomende wachtwoorden uitsluiten. Als extra beveiligingslaag kan naast het wachtwoord, al dan niet conditioneel, ook een tweede worden vereist. HelloID biedt ondersteuning voor twee factor authenticatie (2FA) via SMS, e-mail, one time passwords (OTP) via zowel soft- als hardtokens, en kan integreren met Radius clients.

Authenticatie via third parties

In veel gevallen loggen gebruikers in op HelloID via een third party identity provider zoals Active Directory. Bij het gebruik van een lokale Active Directory zijn er ook lokale componenten nodig in de vorm van een HelloID Agent en een IIS-webserver. HelloID ondersteunt echter ook cloud-to-cloud authenticatie via identity providers zoals Azure, Google Workforce en Salesforce. Bij deze identity providers worden geen inloggegevens gesynchroniseerd, maar verloopt de authenticatie via een ‘shared secret’ met industriestandaarden als SAML, WS-Federation en OpenID Connect. Gebruikers kunnen inloggen met de binnen de IDP beheerde inloggegevens en de derde partij valideert deze per authenticatieverzoek op juistheid.

Fijnmazige rechten en rollen

Nadat een gebruiker is geauthenticeerd bepalen zijn of haar rollen tot welke onderdelen van HelloID de gebruiker toegang mag hebben. Een rol is een verzameling van rechten en privileges die kunnen worden toegekend aan een of meerdere gebruikers. Standaard zijn er binnen HelloID enkele basisrollen beschikbaar, maar er kunnen ook organisatiespecifieke gebruikersrollen worden gedefinieerd. De acties die uitgevoerd mogen worden per rol zijn fijnmazig in te stellen op basis van het CRUD-systeem (Create, Read, Update, Delete).

Enerzijds bepaalt dit welke acties een bepaalde gebruiker mag uitvoeren. Zo kan geconfigureerd worden dat iemand met een beheerdersrol een rapportage mag bewerken en verwijderen, terwijl iemand met een managersrol deze enkel kan bekijken. Anderzijds kan hiermee ook bepaald worden welke onderdelen zichtbaar zijn voor de gebruikers binnen een rol. Elk onderdeel binnen de gebruikersinterface

van HelloID kan per rol aan- en uitgezet worden zodat je organisatie zelf kan bepalen welke functionaliteiten er kunnen worden gebruikt. De toekenning van een rol kan handmatig door een beheerder worden uitgevoerd, maar rollen kunnen ook worden toegekend op basis van groepen binnen de lokale HelloID-directory of de gekoppelde identity provider.

Koppelen met doelsystemen

Met HelloID Provisioning wordt de aanmaak en het beheer van user accounts en rechten in het netwerk en applicaties zoveel mogelijk geautomatiseerd op basis van een koppeling met een bronsysteem. De module HelloID Service Automation sluit naadloos aan op HelloID Provisioning. Naast de geautomatiseerde provisioning vanuit het HR-systeem zullen er altijd incidentele 'maatwerk'-serviceverzoeken blijven. Incidentele wijzigingen kunnen met de module Service Automation worden geautomatiseerd. De HelloID Agent verzorgt de synchronisatie met lokale bron- en doelsystemen. Met cloudapplicaties vindt de connectiviteit volledig vanuit de cloud plaats. HelloID beschikt over de mogelijkheid om te interfacen met de API's en webservices van bron- en doelapplicaties via protocollen als SOAP/XML, REST/JSON, SCIM en ODBC. Verbindingen over het internet worden tot stand gebracht via HTTPS.

Single sign-on tot gekoppelde applicaties

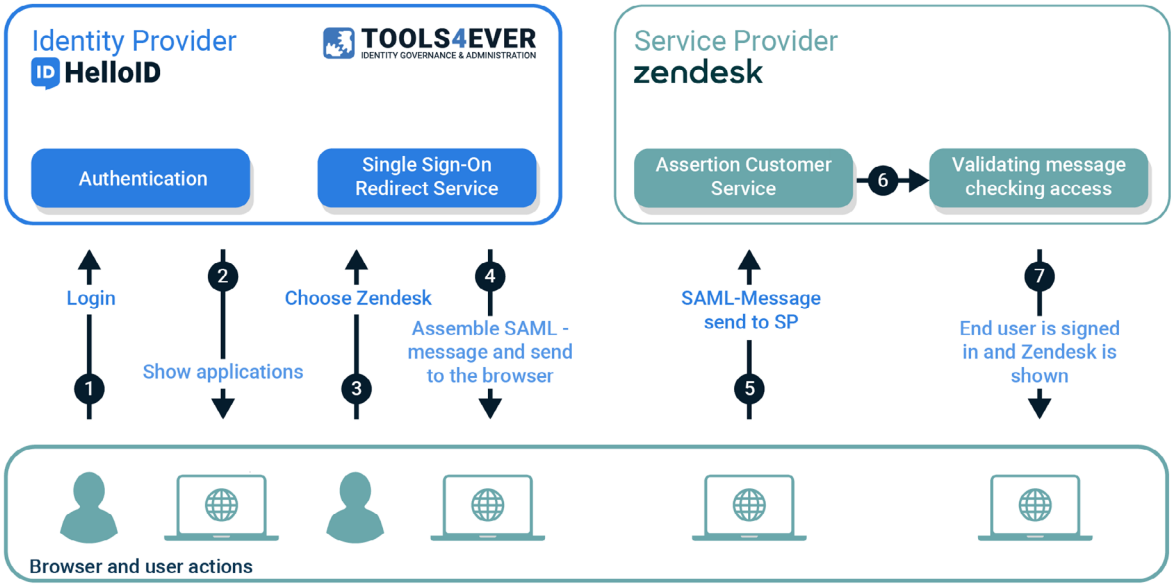
Wanneer de gebruiker is geauthenticeerd tot het HelloID portaal is het mogelijk om middels de optionele module Access Management de authenticatie tot andere applicaties via single sign-on (SSO) geautomatiseerd te laten verlopen. De eindgebruiker hoeft dan niet nogmaals in te loggen op de aan HelloID gekoppelde applicaties. Dit betekent dat HelloID de identity provider van de desbetreffende applicaties wordt. Om SSO mogelijk te maken ondersteunt HelloID alle gangbare SSO-protocollen zoals SAML, WS-Federation, en OpenID Connect. Voor applicaties die uit zichzelf geen SSO ondersteunen kan daarnaast worden teruggevallen op HTTP(S) Post, basic authentication en de HelloID plug-in.

SAML en WS-Federation

SAML is een van de meestgebruikte standaarden voor het uitwisselen van authenticatiegegevens en maakt single sign-on (SSO) mogelijk. Het SAML-protocol regelt authenticatie en autorisatie van een gebruiker tussen een identity provider (IDP) en service provider (SP). WS-Federation is een protocol dat primair door Microsoft en IBM wordt gehanteerd, maar een vergelijkbare flow kent. Binnen de gebruikelijke combinatie met ADFS wordt daarbij ook gebruikgemaakt van SAML-berichten.

Binnen HelloID werkt SAML-authenticatie en autorisatie als volgt:

1. Een gebruiker stuurt een verzoek om in te loggen en HelloID valideert het verzoek.
2. HelloID toont een overzicht van applicaties die de gebruiker mag gebruiken.
3. De gebruiker selecteert een applicatie.
4. HelloID maakt een SAML-bericht aan om de authenticatie uit te voeren bij de SP. HelloID ondertekent en versleutelt het bericht met behulp van een certificaat en stuurt dit naar de browser.
5. Het SAML bericht wordt verstuurd naar de betreffende SP.
6. De SP controleert het SAML-bericht aan de hand van het certificaat en valideert de toegang.
7. De gebruiker is zonder tussenkomst van een inlogpagina ingelogd bij de SP.

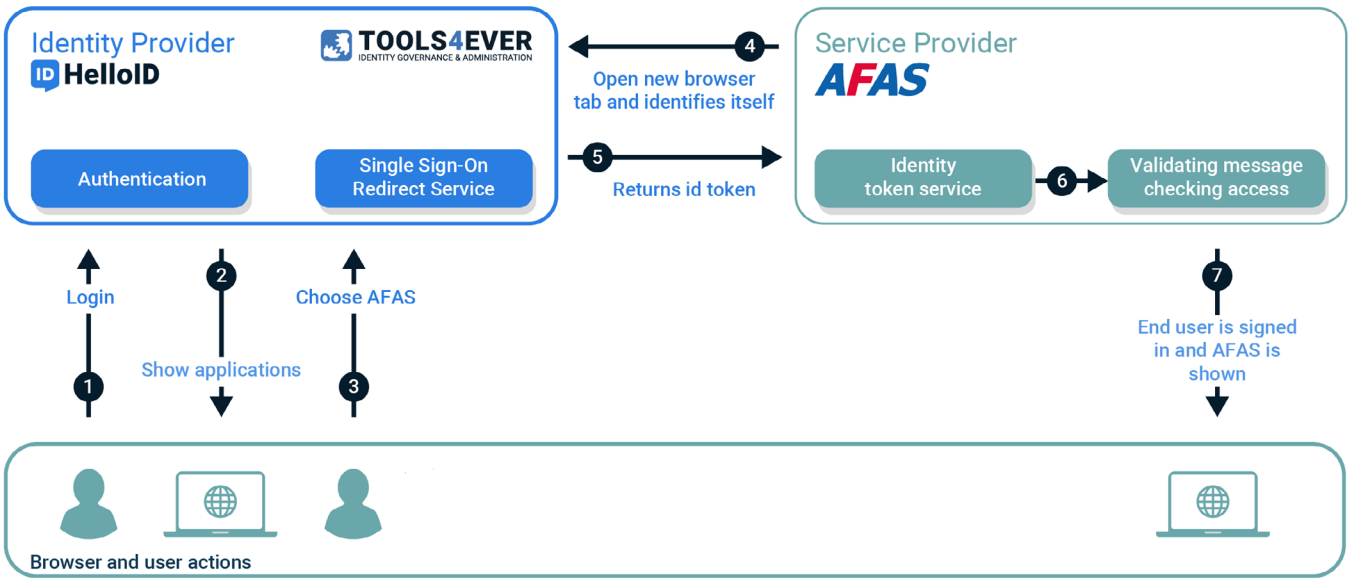


OpenID Connect

OpenID Connect (OIDC) is een open standaard gebouwd op het OAuth 2.0 protocol. Authenticatie werkt via een ID-token, ook wel JSON Web Token (JWT) genoemd.

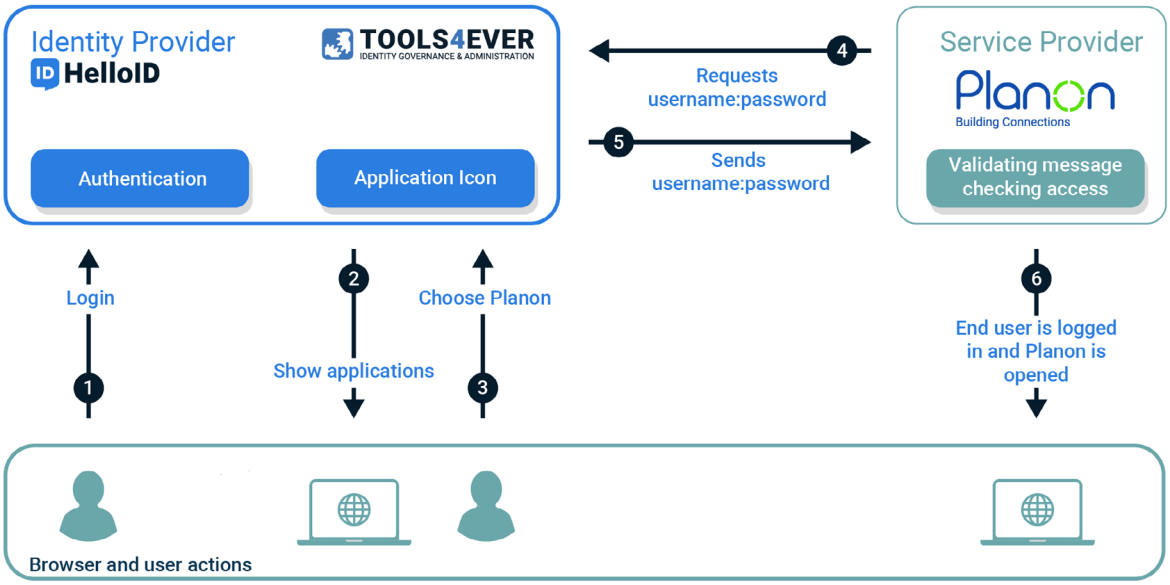
De authenticatie via OpenID Connect werkt als volgt:

1. Een gebruiker stuurt een verzoek om in te loggen en HelloID valideert het verzoek.
2. HelloID toont een overzicht van applicaties die de gebruiker mag gebruiken.
3. De gebruiker selecteert een applicatie.
4. Generate authorization code and request token
5. HelloID valideert de gebruiker en stuurt de gebruiker terug naar de applicatie met een token.
6. De applicatie valideert het token maakt een sessie aan voor de gebruiker.
7. De gebruiker is zonder tussenkomst van een inlogpagina ingelogd bij de applicatie.



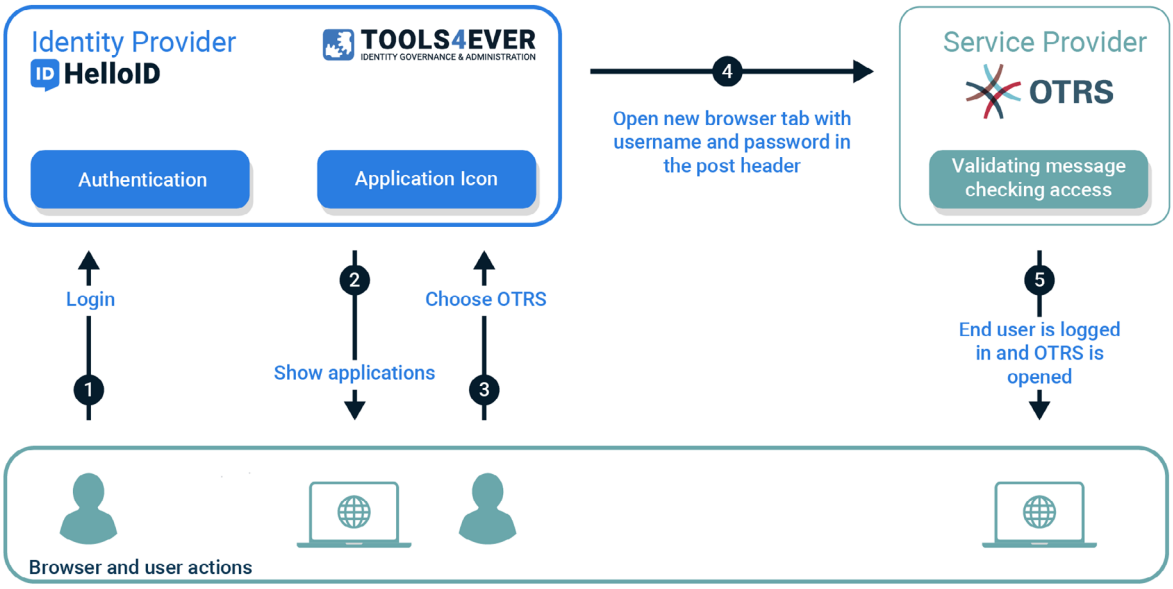
Basic authentication

Basic authentication is een eenvoudig authenticatie-schema gebouwd op het HTTP(S)-protocol. HelloID stuurt een HTTP-verzoek met een autorisatie-header dat het woord 'Basic' en een base64-encoded string met de gebruikersnaam en het wachtwoord bevat. De applicatie ontvangt het authenticatieverzoek, decodeert de autorisatie-header, split de gebruikersnaam en het wachtwoord, en gebruikt deze vervolgens om de gebruiker te valideren.



Form post

Het '*form post*'-mechanisme plaatst de gebruikersnaam en het wachtwoord in de HTTP(S) POST-header die naar de webapplicatie wordt gestuurd. Dit mechanisme wordt ook gebruikt als een gebruiker toegang krijgt tot de applicatie via de gebruikelijke inlogpagina van de website. De loginpagina plaatst de gebruikersgegevens in de header (client-kant), en de applicatie (server-kant) leest deze gegevens, verifieert ze en verifieert de gebruiker. Voor applicaties die geen SSO-protocollen ondersteunen kan HelloID dit mechanisme gebruiken om hierop toch geautomatiseerd in te loggen. HelloID ondersteunt zowel HTTP als HTTPS. Tools4ever raadt HTTPS sterk aan vanwege de aanzienlijke verhoging van de veiligheid via encryptie.

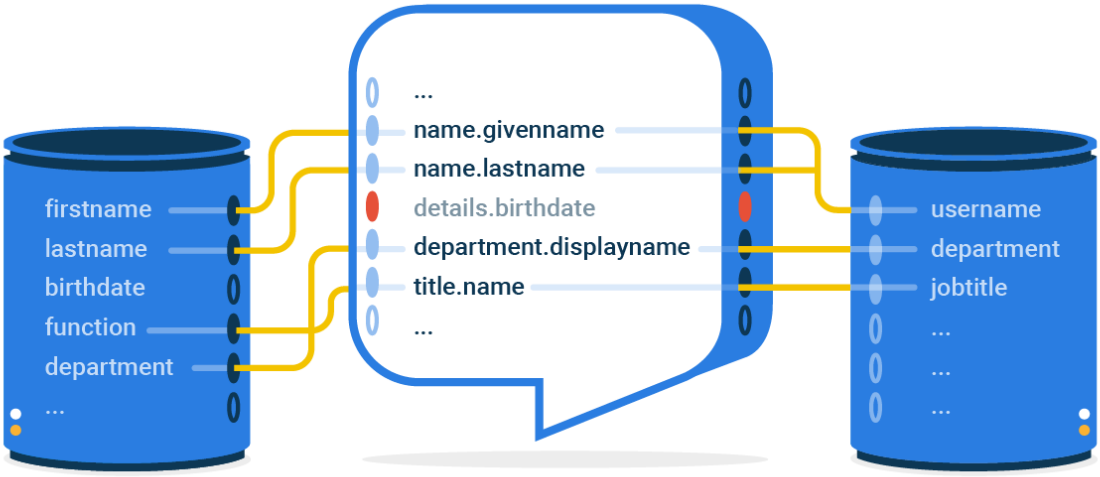


Plug-in authenticatie

Voor applicaties die geen van eerdergenoemde methoden ondersteunt kun je gebruikmaken van de HelloID browser plug-in. Binnen HelloID wordt vastgelegd welke applicaties en welke URL's de plug-in moet afhandelen. De plug-in gebruikt een beveiligde SSL-verbinding met het HelloID-platform om authenticatiegegevens als een gebruikersnaam en wachtwoord te verkrijgen. De inloggegevens worden niet door de plug-in opgeslagen, maar direct gebruikt voor SSO. De plug-in herkent de invoervelden van het inlogformulier van de webapplicatie op basis van onder meer de unieke identifiers. Vervolgens vult de plug-in de velden geautomatiseerd met de inloggegevens van de gebruiker. Afhankelijk van de wijze waarop het inlogformulier werkt kan HelloID de inloggegevens automatisch verzenden of moet de gebruiker zelf nog even op de inlogknop drukken.

Opslag van persoonsgegevens

Tools4ever verwerkt persoonsgegevens van opdrachtgevers om de te leveren diensten te kunnen uitvoeren. We maken onderscheid tussen persoonsgegevens die minimaal benodigd zijn voor de functionering van de afgenomen HelloID-modulen én persoonsgegevens die je als klant wenst te verwerken. Standaard verwerkt HelloID geen gegevens die zijn aangemerkt als 'bijzondere persoonsgegevens'.



Hieronder zie je per module welke gegevens minimaal benodigd zijn:

- **Provisioning** - vereist minimaal de naam (initialen, roepnaam, tussenvoegsel, achternaam, voorkeursnaam) en contractgegevens (personeelsnummer, functie, afdeling, organisatie, in- en uitdienstdatum) om gebruikers en autorisaties te kunnen beheren.

- **Service Automation** - vereist minimaal de inlognaam en weergavenaam, om te kunnen authenticeren op het portaal.

- **Access Management** - vereist net als Service Automation minimaal de inlognaam en weergavenaam, om te kunnen inloggen op het portaal.

Als klant kun je zelf beoordelen of Tools4ever extra gegevens mag verwerken. Via de HelloID 'attribute mapper' kunnen beheerders consultants van Tools4ever en partners laten configureren welke gegevens uit gekoppelde systemen wel en niet verwerkt en/of bewaard zullen worden in de HelloID-database. Deze configureerbare mapping zorgt ervoor dat de HelloID-database altijd volledig in overeenstemming blijft met het privacy- en beveiligingsbeleid van je organisatie.

Rapportering en logging

Rapportering en logging zijn basiscomponenten van elk beveiligingsbeleid en worden vereist vanuit zowel wet- en regelgeving als richtlijnen voor informatiebeveiliging. HelloID logt alle belangrijke gebeurtenissen. De logging geeft in de vorm van een 'audit trail' inzicht in het gebruik van de HelloID-omgeving. Je kunt er potentiële beveiligingsrisico's mee identificeren. Alle binnen en door HelloID uitgevoerde acties worden opgeslagen in Elastic reporting, dat uitgebreide mogelijkheden biedt om hierover te rapporteren. Hieronder zie je per module verschillende voorbeelden van de data die wordt gelogd:

- **Provisioning**
  Per systeem en persoon worden alle uitgevoerde acties gelogd omtrent het creëren, enablen, updaten, verplaatsen, disablen, en verwijderen van accounts, en het toekennen en intrekken van permissies.

- **Service Automation**
  Voor self-service producten wordt informatie opgeslagen over de aanvraag, workflow en goedkeuring. Bij gedelegeerde formulieren worden alle gegevens opgeslagen over aanvragen, formulierdata en auditinformatie ten behoeve van configuratiewijzigingen.

- **Access Management**
  Vastgelegde gebeurtenissen omvatten succesvolle en mislukte aanmeldingen, de geografische locatie van de gebruiker, gebruikte apparaten, geïnitieerde wachtwoordresets, toegangspogingen voor applicaties en mislukte toegangspogingen als gevolg van het toegangsbeleid.

Ontsluiten van logging data

De data vanuit Elastic kan via de ingebouwde rapportagevoorzieningen worden weergegeven of worden gebruikt in combinatie met eigen business intelligence (BI) tooling zoals PowerBI. Alle logging data binnen Elastic is bijna realtime beschikbaar en uit te lezen via REST API's. Door de toepassing van authenticatie via een HelloID API key ben je er van verzekerd dat enkel geautoriseerde personen de logging data kunnen inzien.

Bewaartermijnen van gegevens

Binnen HelloID worden de bewaartermijnen onderscheiden in gegevens die door de klant in het platform worden opgeslagen en de (audit)logging. Gebruikers- en configuratiegegevens blijven gedurende de gehele contractperiode bewaard. Bij het beëindigen van het HelloID-contract worden de gegevens nog maximaal 3 maanden bewaard en hierna automatisch verwijderd.

HelloID slaat de interne audit logging 30 dagen op. Na het verstrijken van deze bewaarperiode worden de logs inclusief de back-up verwijderd. De audit logging die via het rapportageplatform Elastic wordt ontsloten, wordt een jaar bewaard. Daarna worden deze gegevens inclusief de back-ups gewist. Indien het gewenst of vanuit wet- en regelgeving vereist is om gegevens langer te bewaren kun je ze via de hiervoor beschikbare API's exporteren naar een eigen rapportage/archief/auditing-tool. Op deze manier heeft je organisatie de volledige controle over de retentieperiode van de (audit)logging.

Datalek protocol

In het geval van een datalek treedt het datalek protocol in werking om ervoor te zorgen dat klanten op de hoogte zijn van incidenten. Na het ontdekken van een beveiligingsincident of datalek, stelt Tools4ever haar klanten daarvan binnen 24 uur op de hoogte. Dat schrijft het protocol voor. Tools4ever doet deze melding per e-mail aan de contactpersoon binnen je organisatie. Tools4ever doet zelf geen directe melding aan de AP of betrokkenen.

Fysieke beveiliging en autorisatiebeleid Tools4ever

Het kantoor van Tools4ever wordt op verschillende manieren beveiligd. In en rondom het pand is onder meer camerasurveillance en toegang tot het pand wordt beperkt met RFID-tokens die aan individuele personen zijn gekoppeld. Voor onder meer server-, opslag- en elektriciteitsruimten passen we daarnaast aanvullende vormen van toegangsbeveiliging toe.

Voor het werken met gegevens van klanten hanteert Tools4ever een strikt beleid. Met medewerkers zijn geheimhoudingsverklaringen overeengekomen en zij hebben enkel toegang tot de data die strikt noodzakelijk is voor hun functie. Er wordt gewerkt met twee-factor-authenticatie voor toegang tot systemen en applicaties. Tools4ever stimuleert bewustzijn, opleiding en training ten aanzien van privacy en informatiebeveiliging. Getrainde security managers informatiebeleid en IT-security zien toe op de naleving van het beleid en actualiseren de beveiligingsmaatregelen regelmatig.

Standaarden en certificeringen

Het HelloID-platform wordt gehost op de Infrastructure-as-a-Service (IaaS)-oplossingen van Microsoft en Google. Beide leveranciers zijn internationaal erkend om de zeer hoge beveiligingsstandaarden waar zij aan voldoen en op basis van de *service level agreement* met beide partijen wordt de veiligheid van ons platform gegarandeerd. Daarnaast helpt HelloID als IDaaS-oplossing jou, als klant, te voldoen aan verschillende (sectorspecifieke) informatiebeveiligingsnormen en certificeringen. Tools4ever vindt we het ook belangrijk dat er wordt voldaan aan standaarden die door de softwareindustrie worden gesteld en dat er structureel door andere partijen naar onze systemen, processen en procedures wordt gekeken.

OWASP

De Security-by-Design-principes zoals gedefinieerd door OWASP vormen de basis van onze aanpak.

Microsoft Gold Partner

Tools4ever heeft een langdurig Microsoft Gold Partnership en heeft specifieke beveiligingservaring in het werken met de Microsoft-productsuite.

ISO 27001

Tools4ever is ISO 27001-gecertificeerd. Dat houdt in dat Tools4ever het managementsysteem voor informatiebeveiliging goed op orde heeft. Concreet betekent dit dat wij op een veilige en gecontroleerde manier software ontwikkelen, maar ook dat we adequaat handelen bij mogelijke risico's of beveiligingsincidenten. In 2022 komt daar de SOC 2-certificering nog bij.

Deloitte.

Deloitte Risk Services voert twee keer per jaar penetratietesten uit. Het rapport met bevindingen dat Deloitte verstrekt wordt door onze development afdeling met hoge prioriteit opgepakt en geïmplementeerd en/of Tools4ever reageert er inhoudelijk op.

TOOLS4EVER

Adres	Amalialaan 126c 3743 KJ Baarn Nederland
Telefoon	+31 (0) 35 54 832 55
Website	Tools4ever.nl
Mail	info@tools4ever.com
Sales	sales@tools4ever.com
Support	tools4ever.nl/support