v1.0 | 20 12 2017

White Paper HelloID

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INHOUDSOPGAVE

SAMENVATTING

In uw bedrijf worden verschillende applicaties gebruikt. Sommigen daarvan beheert u wellicht zelf, maar steeds vaker zijn het cloud-based oplossingen. Belangrijk is dat al die applicaties en de data goed zijn beveiligd. Dat alleen uw medewerkers er toegang toe hebben en er op geen enkele manier misbruik kan worden gemaakt van bedrijfsinformatie of klantgegevens. Ook de wet- en regelgeving wordt daarin steeds strikter.

Tegelijkertijd wilt u voorkomen dat dit uw personeel hindert bij hun werk. U wilt niet dat ze steeds opnieuw moeten inloggen en voor iedere applicatie een andere gebruikersnaam en password moeten onthouden. U wilt voor uw medewerkers één geïntegreerde en veilige web-based werkplek waarin ze naadloos gebruik kunnen maken van zowel cloud-based apps als Windows applicaties. U wilt IT beveiliging en gebruiksvriendelijkheid optimaal combineren.

HelloID is een cloud-based Identity en Access Management (IAM) oplossing die uw medewerkers via één portal toegang geeft tot al uw bedrijfsapplicaties. Uw medewerkers hebben genoeg aan één username en wachtwoord. HelloID zorgt vervolgens dat ze toegang krijgen tot de applicaties en data die ze nodig hebben om hun werk te doen. Met de uitgebreide Single Sign-On functionaliteit integreert u alle bedrijfsapplicaties – van online cloud apps tot intern gehost webapplicaties - in HelloID. Ook is 2 Factor Authenticatie beschikbaar als extra beveiliging.

HelloID geeft u volledige controle over wie er toegang heeft tot welke applicaties en data. En op welk moment en vanaf welke plek of device. Via het Self-Service portal kunnen medewerkers zelf toegang vragen tot de benodigde applicaties en data. Managers en ‘data-owners’ kunnen deze toestemming zelf met één klik geven. Daarmee vergroot u niet alleen het gebruikersgemak voor medewerkers en managers, u ontlast ook de IT afdeling en helpdesk.

HelloID is een moderne, cloud-based IAM oplossing. De installatie verloopt snel en eenvoudig en u heeft geen dure specialisten nodig voor het beheer. Met HelloID is uw organisatie op een gebruiksvriendelijke manier voorbereid op de toekomstige eisen op het gebied van applicatie- en databeveiliging.

INLEIDING

Het belang van Identity en Access Management (IAM) binnen organisaties neemt sterk toe. Met name de snelle veranderingen op IT infrastructuurgebied en de sterk veranderende wet- en regelgeving dragen daaraan bij:

- De meeste bedrijven beheerden nog niet zo lang geleden hun eigen lokale infrastructuur en richtten zich vooral op het efficiënter maken van IT- en bedrijfsprocessen. De afgelopen jaren hebben veel bedrijven echter de transitie naar de cloud gemaakt. Andere bedrijven bereiden zich daarop voor. Ze hanteren veelal een 'cloud, tenzij' beleid. Het eigen datacenter wordt nog een paar jaar aangehouden, maar de infrastructuur wordt heroverwogen zodra de afschrijvingstermijn voorbij is. De keuze voor gangbare infrastructuurcomponenten als Citrix, Exchange, Active Directory en lokale opslag staat ter discussie.

- Parallel vraagt de sterk veranderende wet- en regelgeving op het gebied van databeveiliging en privacy om maatregelen. De EU General Data Protection Regulation (GDPR) wordt in Nederland geïmplementeerd binnen de Algemene Verordening Gegevensbescherming (AVG) en al eerder werd de meldplicht datalekken van kracht. Voor bedrijven is de impact groot. De gele kaarten uit de auditrapporten moeten serieus worden opgepakt en in veel organisaties is een security officer aangesteld voor alle informatiebeveiliging vraagstukken.

Via Identity en Access Management (IAM) beheren organisaties user account informatie en de toegang van gebruikers tot hun infrastructuur, applicaties en data. IAM verzorgt gestroomlijnde indienst-, door- en uitdienstprocessen en een rol-gebaseerde toegang tot applicaties. Die toegang verloopt via een dashboard en voor een optimale gebruikerservaring biedt IAM veelal ook Single Sign-On, Self Service en workflow management functionaliteit.

Daarmee speelt IAM een centrale rol bij de migratie naar de cloud en de implementatie van nieuwe wet- en regelgeving. Een goede en toekomstvaste IAM-oplossing maakt access management niet alleen efficiënter. De oplossing moet de organisatie ook ontzorgen op het gebied van wet- en regelgeving, cloud applicaties ondersteunen en zelf in de cloud beschikbaar zijn. IAM is daarmee een onderwerp dat tegenwoordig op de agenda van de directie of raad van bestuur staat.

De traditionele, grote IAM-enterprise oplossingen blijken niet meer geschikt voor de meeste organisaties. Die oplossingen zijn duur, niet flexibel en vereisen gespecialiseerd personeel om beheerd te worden. IAM-oplossingen in de cloud kunnen daarentegen eenvoudig en snel geïmplementeerd worden. Ze zijn eenvoudig te wijzigen, te beheren en up-to-date te houden volgens de laatste beveiligingsstandaarden. Er is een aanzienlijke kostenbesparing mogelijk omdat niet langer gespecialiseerd personeel nodig is.

HelloID IDENTITY AND ACCESS MANAGEMENT AS A SERVICE

Het HelloID platform van Tools4ever biedt organisaties de mogelijkheid om volledig de transitie te maken van on-premise naar de cloud en een “cloud-tenzij” beleid ook op het gebied van Identity Management te realiseren. HelloID biedt organisaties een volledig cloud-gebaseerd IDaaS-platform waarmee ze klaar zijn voor de toekomst.

HelloID bestaat uit drie componenten:

1. **Access Management** beheert de toegang van medewerkers tot de verschillende applicaties en gegevens.
2. **Self Service en Workflow Management** maken het mogelijk dat medewerkers zonder tussenkomst van de helpdesk automatisch wijzigingen in het netwerk kunnen aanbrengen.
3. **Data Management** zorgt dat de toegang van medewerkers tot bestanden en andere bedrijfsgegevens op eenvoudige wijze kan worden beheerd.

Deze componenten vormen samen een basis voor organisaties om vanuit de huidige situatie snel en veilig de identiteit van gebruikers te beheren. Met beperkte investeringen kan een volwaardige Identity oplossing worden gerealiseerd. Bovendien worden op korte termijn aanvullende cloud-based modules toegevoegd, waaronder Provisioning en Self Service Wachtwoord Reset. Deze modules zijn nu al beschikbaar in de on-premise producten van Tools4ever (UMRA en IAM) die ook naadloos integreren met HelloID.

Een belangrijke voorwaarde van een IAM oplossing in de cloud is dat de oplossing veilig is en dat de oplossing voldoende beveiligd is. Als leverancier van HelloID kan Tools4ever dit aantonen middels periodiek uitgevoerde intrustion en penetration tests. Organisaties die HelloID gebruiken kunnen hiermee aantonen dat Tools4ever voldoende maatregelen heeft genomen en dit aan te kunnen tonen aan externe en interne auditors.

ACCESS MANAGEMENT

INLEIDING

De snelle opkomst van cloudapplicaties zorgt dat steeds meer data buiten de eigen netwerkomgeving zijn opgeslagen. Dat stelt organisaties voor flinke uitdagingen op het gebied van toegangsbeheer en beveiliging. Uiteraard wil men eindgebruikers eenvoudig toegang tot IT-resources bieden. Tegelijkertijd moet die toegang goed gecontroleerd en beheersbaar zijn om data ook buiten het bedrijfsnetwerk optimaal te beveiligen. Vanzelfsprekend om de eigen bedrijfsgegevens te beschermen, maar ook om compliant te zijn met de steeds striktere wet- en regelgeving op dit gebied.

CENTRAAL TOEGANGSBEHEER

Zonder een Access Management oplossing wordt deze beveiliging decentraal geregeld door de leveranciers van de verschillende cloud applicaties. Om de beveiliging van data te waarborgen en te voldoen aan “strong authentication” ontwikkelen die leveranciers hun eigen authenticatieprocessen. Organisaties willen echter voor toegangsbeheer en beveiliging niet geconfronteerd worden met meerdere en onderling verschillende authenticatieprocessen. Ze willen een uniform inlogproces dat ze zelf kunnen bepalen. Voor de eindgebruiker is het ook niet wenselijk om verschillende gebruikersnamen en wachtwoorden te gebruiken. Ook wil niemand met meerdere two-factor devices rondlopen. Het maakt inloggen onnodig complex, kost extra tijd en kan ten koste van de veiligheid gaan.

GEBRUIKERSERVARING

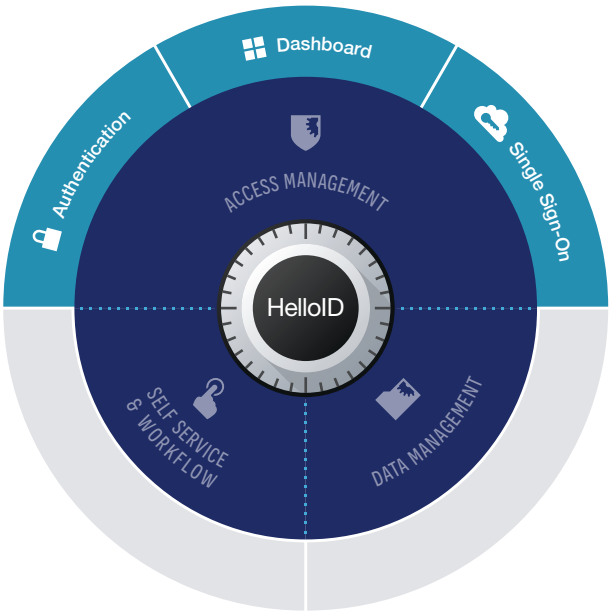
HelloID biedt medewerkers, partners en eventueel klanten eenvoudig en uniform toegang tot cloudapplicaties. De eindgebruiker hoeft maar één webadres te onthouden in plaats van meerdere webadressen voor verschillende applicaties. Bovendien hoeft de eindgebruiker zich maar een keer te identificeren bij de centrale directory. Deze directory kan bijvoorbeeld een Active Directory zijn. De gebruiker identificeert zich met het voor hem of haar bekende gebruikersnaam en wachtwoord. Deze verificatie kan eventueel worden uitgebreid met een two-factor authenticatiestap. Hierna hoeft de eindgebruiker zich niet meer per cloudapplicatie opnieuw in te loggen (SSO).

ONDERDELEN HelloID ACCESS MANAGEMENT

Access Management bestaat uit drie componenten:

1. **Authenticatie**
   Allereerst vindt authenticatie van de eindgebruiker plaats via een login met gebruikersnaam en wachtwoord. Eventueel kan ook nog two factor authenticatie worden ingezet als extra verificatie.

2. **Dashboard**
   Als de identificatie en verificatie succesvol zijn, krijgt de gebruiker toegang tot een dashboard met herkenbare iconen van de relevante cloudapplicaties. Deze vormen de links naar de cloudapplicatie en worden eenvoudig en aantrekkelijk gepresenteerd in het portal of mobiele dashboard.



3. **Single Sign-On (SSO)**
   Afhankelijk van het authenticatieprotocol van de cloudapplicaties gebruikt HelloID het relevante SSO-protocol om eindgebruikers automatisch voor de cloudapplicatie te identificeren en authentiseren. HelloID ondersteunt alle gangbare SSO-protocollen. Voor leveranciers die geen enkel SSO protocol (correct) ondersteunen, heeft HelloID een browser extensie die een ‘catch all’ mogelijk maakt en zorgt dat een eindgebruiker altijd SSO aangeboden kan worden.

Dankzij HelloID logt de eindgebruiker één keer in en heeft hij via een overzichtelijk dashboard toegang tot de applicaties. Dit kan vanaf elke willekeurige plek en vanaf ieder willekeurig apparaat. We lichten de genoemde drie functies hieronder uitgebreider toe.

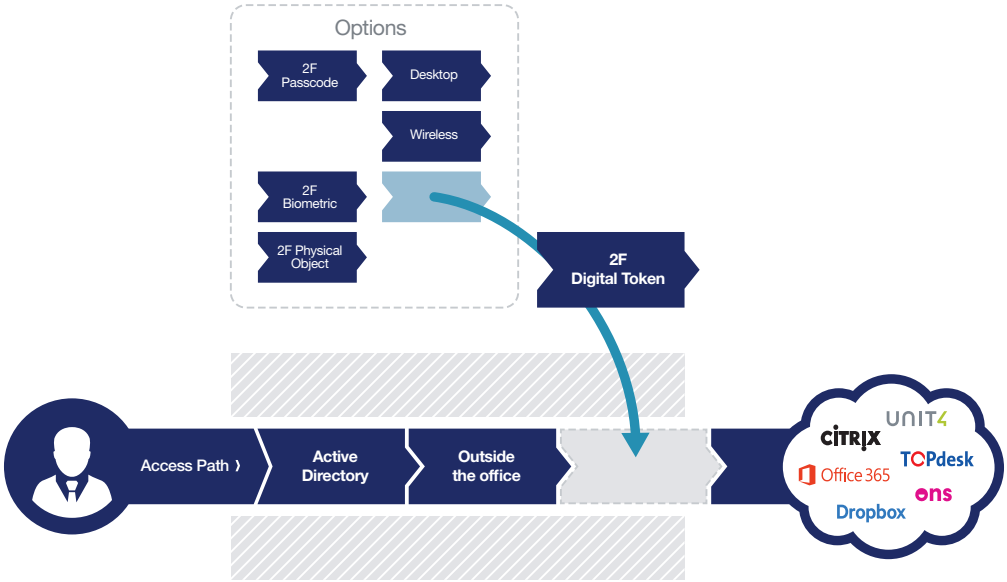
AUTHENTICATIE

Inloggen van een gebruiker op HelloID gaat in veel gevallen via de Active Directory. HelloID ondersteunt ook andere Identity Providers zoals SAML, LDAP en Azure. Ook kan gebruik worden gemaakt van de login van de lokale HelloID-directory. De lokale HelloID-directory kan gebruikt worden om toegang voor bijvoorbeeld klanten of patiënten van de organisatie te beheersen zonder hiervoor deze gebruikers aan te maken in de Active Directory of andere Identity Provider. HelloID biedt daarbij volledige provisioning technologie en is kostentechnisch zeer concurrerend.

Aansluitend kan een tweede verificatieslag noodzakelijk zijn om de gebruiker te authentiseren alvorens toegang kan worden verleend. Deze check gebeurt op basis van 2FA. Naast soft of hard tokens en SMS worden ook verschillende one time passwords (OTP's) als tweede factor ondersteund. Afhankelijk van de behoefte van de organisatie biedt HelloID uiteenlopende integratiemogelijkheden, inclusief Radius cliëntintegratie. Biometrische opties, zoals gezichtsherkenning zijn in ontwikkeling.

Het gehele inlogproces vindt plaats met gebruik van access policies. Het is mogelijk om uitgebreide toegangsregels in te stellen op basis van onder andere netwerktype, locatie, netwerk, tijdstip, device en applicatie. De beheerder van HelloID bepaalt wie onder welke voorwaarden toegang krijgt tot het portal of de achterliggende applicaties. Het is bijvoorbeeld mogelijk de toegang vanaf een extern netwerk of een tablet of smartphone te blokkeren. Maar ook vanuit het buitenland of op specifieke momenten, zoals buiten kantooruren.

Het authenticatieproces wordt automatisch gemonitord. Via rapportages is altijd inzichtelijk wie welke applicaties heeft geraadpleegd, op welk moment en vanaf welke locatie. Dit geeft niet alleen een gedetailleerd beeld van het authenticatietraject, maar toont bijvoorbeeld ook inlogpogingen via verdachte IP-adressen. Daarmee is het authenticatieproces transparant, toetsbaar en aanpasbaar. Mogelijke dreigingen kunnen tijdig worden herkend om tegenmaatregelen te nemen. Iets dat niet alleen gewenst is, maar ook vanuit de nieuwe wet- en regelgeving wordt geëist.

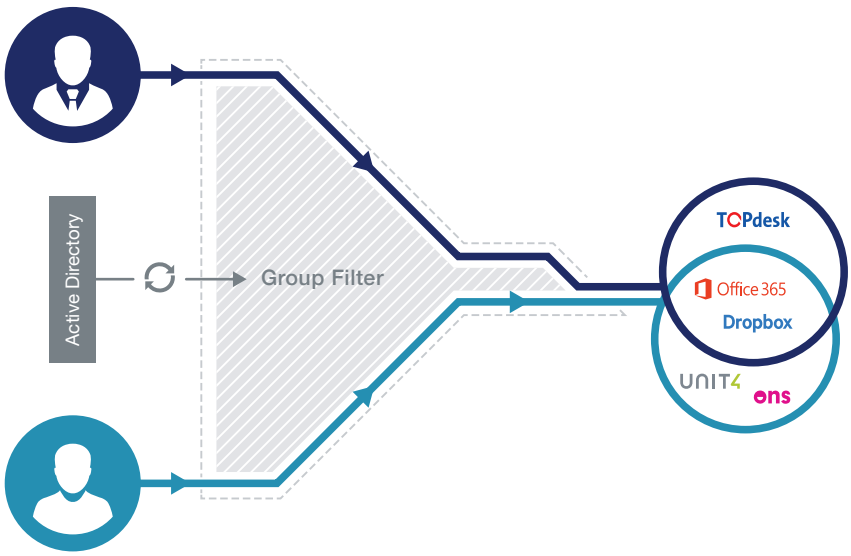


DASHBOARD

Na succesvol inloggen krijgen eindgebruikers toegang tot een onlinedesktop of -dashboard. Via iconen heeft men direct toegang tot de gekoppelde cloudapplicaties. Welke cloudapplicaties getoond worden, kan afhankelijk gemaakt worden van de rol van de medewerker binnen de organisatie. Medewerkers kunnen op basis van hun afdeling, functie, locatie, etc. aan een bepaalde groep binnen HelloID worden gekoppeld. Iedere groep is geautoriseerd voor bepaalde applicaties. Op die manier heeft de beheerder controle over wie toegang krijgt tot welke cloudapplicatie.

Door de integratie met bijvoorbeeld Active Directory kan de plaatsing van gebruikers in groepen worden gesynchroniseerd met de groepen in de Active Directory. Dit scheelt de beheerders veel werk. Zo bepaalt het lidmaatschap van een AD-groep bijvoorbeeld of een medewerker toegang krijgt tot een cloudapplicatie en/of daarvoor een 2FA vereist is. Zonder extra beheerhandelingen op HelloID.

De lay-out van het dashboard is verder volledig af te stemmen op de specifieke wensen van de organisatie. Naast een standaardopmaak biedt HelloID mogelijkheden om eigen stylesheets, CSS-koppelingen of links te integreren. Door de end user API is het dashboard eenvoudig te integreren in social intranet toepassingen als TripTic, Embrace, Google Sites of Sharepoint Online.



SINGLE SIGN-ON (SSO)

Zodra de gebruiker is geauthentiseerd op het HelloID-dashboard is het mogelijk de authenticatie tot andere applicaties automatisch te laten verlopen. Op het HelloID-dashboard heeft de gebruiker een overzicht van beschikbare cloudapplicaties. De authenticatie op de applicatie verloopt middels het centrale HelloID-managementportal. Hierbij is het voor de eindgebruiker niet nodig nogmaals in te loggen op de geselecteerde applicatie. Het HelloID-portal onthoudt de gebruiker en verifieert de identiteit van de gebruiker automatisch op het andere systeem (automated login).

Om deze Single Sign-On (SSO) automatisch mogelijk te maken voor de verschillende applicaties ondersteunt HelloID alle bestaande SSO-protocollen zoals: SAML, HTTP(S) Post, OpenID connect, Oauth, WS Federation, Basic Authentication. Maar ook als een leverancier geen enkel SSO protocol (correct) ondersteunt, zorgt HelloID toch voor het SSO gebruiksgemak. Daarvoor heeft HelloID een browser extensie die een ‘catch all’ mogelijk maakt en uiteindelijk garandeert dat een eindgebruiker altijd SSO aangeboden kan worden.

In het HelloID-portal wordt de link tussen de HelloID-identiteit en de verschillende applicaties vastgelegd. De authenticatie tot het portal en de authenticatie op de verschillende applicaties worden gescheiden. Dit houdt in dat alleen wanneer de toegang gevraagd wordt deze tokens opgehaald worden. Doordat de gebruiker eenvoudig de sessie kan sluiten zonder opnieuw in te hoeven loggen, worden applicaties sneller afgesloten. Dit minimaliseert de risico’s op onjuist gebruik. De organisatie heeft controle over wie toegang kan krijgen tot welke applicaties.

SSO Protocols

- SAML 2.0
- OAuth
- OpenID Connect
- WS Federation
- HTTP(S) Post
- Basic Authentication
- Plugin/Extension

RADIUS – HARDWARE EN SOFTWARE TOKENS

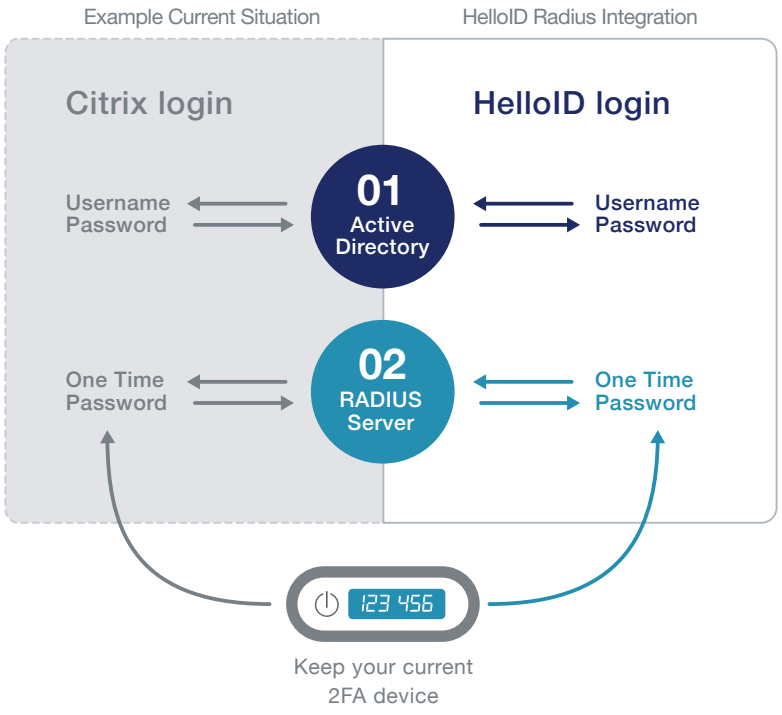
Voor integratie met hardware- en softwaretokens (ook wel One-Time-Passwords genoemd) is Radius de industriestandaard. Om organisaties de mogelijkheid te geven om reeds aangeschafte tokens te blijven gebruiken, biedt HelloID de Radius integratie aan. Hiermee is het eenvoudig om multi-factor van bestaande leveranciers te integreren binnen HelloID. Investeringen in bestaande 2FA blijven zo behouden en medewerkers hoeven niet een nieuwe 2FA te leren.

Hardware- en softwaretokens worden veel ingezet als medewerkers vanaf thuis of een remote locatie via een Remote, VPN of RDP-toegang inloggen op het bedrijfsnetwerk. Eindgebruikers zijn dan ook vaak al bekend met deze tokens. De toegang tot HelloID en de data moet veilig zijn en deze tokens dragen bij aan het authentiseren van de gebruiker. In veel gevallen wordt sterke authenticatie ook verplicht vanuit wet- of regelgeving.

Het authenticatie proces in HelloID verloopt in twee stappen:

1. Zodra een gebruiker toegang wil krijgen, voert HelloID eerst de initiële authenticatie uit.

2. Vervolgens stuurt de geïntegreerde HelloID Radius cliënt een toegangsverzoek naar de Radius server. De Radius server voert verschillende controles uit die door de organisatie zijn ingesteld. Zodra de aanvraag is goedgekeurd wordt het one-time-token gevraagd. Indien deze correct is, krijgt de gebruiker toegang tot het portal.



SELF-SERVICE & WORKFLOW

SELF-SERVICE

Het is inmiddels gewoon geworden om allerlei diensten via portals beschikbaar te stellen aan medewerkers in de organisatie. Waar je vroeger nog via de post je salarisstrook ontving, kun je deze tegenwoordig online bekijken in het eHRM portal. En op dezelfde manier zijn er self service portals voor Facility Management, Planning en andere bedrijfsprocessen.

Ook voor ICT diensten wordt steeds vaker gebruik gemaakt van self service. In plaats van een email of te bellen, kan men zelf een verzoek aanmaken in TOPdesk of een ander ICT portal. Wel is de verdere afhandeling vaak nog handmatig. Het verzoek leidt tot een ticket bij de ICT helpdesk waar vervolgens iemand actie moet ondernemen. De wijzigingen moeten immers worden doorgevoerd in de infrastructuur.

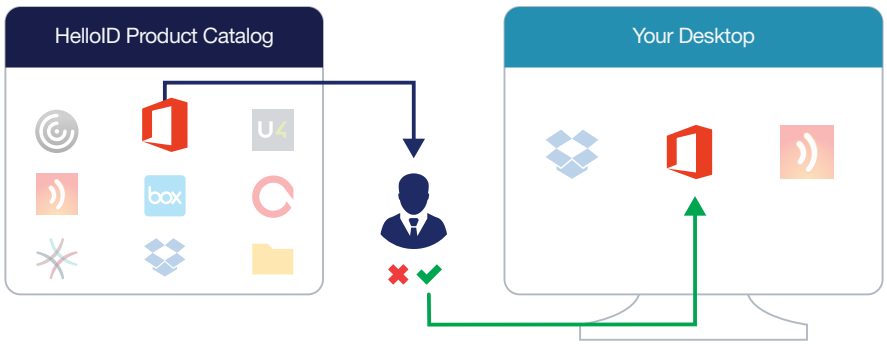
De volgende stap is dan om ook deze acties te automatiseren. Daar valt enorme winst te behalen voor de helpdesk en de verdere organisatie. De HelloID Self-Service functionaliteit verzorgt deze automatisering. Met HelloID Self-Service is het mogelijk om bijvoorbeeld binnen TOPdesk self service en service automation aan te bieden. Omdat beide portals cloud-gebaseerd zijn, is dit zeer eenvoudig en snel te realiseren.

HelloID maakt het mogelijk om een product catalogus samen te stellen en beschikbaar te stellen aan de organisatie. Het beheer van deze product catalogus is bijzonder eenvoudig. En de aantrekkelijke gebruikersinterface zorgt voor een brede acceptatie bij de gebruikers. De product catalogus wordt opgebouwd en onderhouden op basis van geautomatiseerde regels binnen HelloID. Die regels zorgen ervoor dat wijzigingen in de infrastructuur automatisch worden verwerkt.

Als bijvoorbeeld een nieuwe share wordt aangemaakt, wordt deze automatisch getoond in de productcatalogus. Ook wordt op basis van de netwerkinstellingen direct aan medewerkers getoond wie toegang heeft tot de betreffende share. Medewerkers kunnen toegang aanvragen en verantwoordelijke managers kunnen aanvragen goedkeuren. HelloID biedt daarbij extra mogelijkheden als goedkeuring via email, of een tijdelijke goedkeuring om rechtenaccumulatie te voorkomen.

Voor de interface naar het netwerk zijn verschillende powershell commando's beschikbaar. Naast de standaard meegeleverde set kunnen commando's worden aangepast of toegevoegd door de ICT afdeling of een implementatie consultant. HelloID verzorgt de GUI inclusief de uitvoering van de powershell commando's.

Op deze manier kunnen medewerkers en managers snel en eenvoudig - zonder tussenkomst van de ICT afdeling - toegang en rechten beheren. De manager heeft daarbij direct inzicht in welke medewerkers actief zijn op de afdeling en welke licenties, applicaties, shares, etc. deze medewerkers in gebruik hebben. Wijzigingen worden op een uniforme manier standaard afgehandeld en geregistreerd. De werklast voor de helpdesk vermindert enorm en het draagt bij aan een professionele en moderne uitstraling van de ICT afdeling en het bedrijf.



DATA MANAGEMENT

DATA MANAGEMENT

Een van de meest tijdrovende taken voor de helpdesk is het toegangsbeheer tot folders. Om effectief te kunnen samenwerken moeten medewerkers bestanden met elkaar kunnen delen. Om een medewerker toegang tot bepaalde folders of subfolders te geven moet een helpdesk medewerker een reeks van handmatige acties uitvoeren in het filesysteem en in de Active Directory. Hierbij worden snel fouten gemaakt. Dat varieert van fouten in de naamgeving, medewerkers aan wie nooit meer de toegang ontzegd wordt, noodzakelijk AD groepen die niet zijn aangemaakt etc.

HelloID Data Management automatiseert dit proces volledig. Een projectleider, afdelingsmanager of assistent kan als data owner zonder tussenkomst van de helpdesk zelfstandig de toegang tot folders en subfolders beheren. Ook kunnen andere medewerkers direct toegang aanvragen bij de data owner. Via HelloID worden groepen aangemaakt, medewerkers automatisch lid gemaakt van de juiste groepen, folders aangemaakt, Access Control Lists (ACL's) op de folder gezet en alle verdere noodzakelijke handelingen.

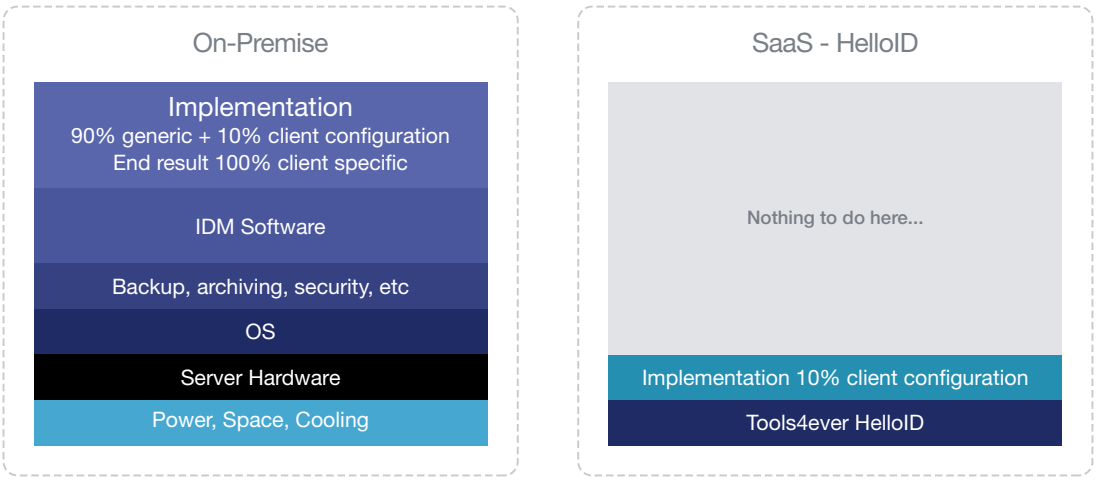
TOOLS4EVER

IAM IN THE CLOUD

Steeds meer organisaties profiteren van services in de cloud. Ook Identity & Access Management (IAM) kan uitstekend vanuit de cloud worden verzorgd. De keuze voor Identity as a Service of IDaaS biedt organisaties verschillende voordelen.

Zo hoeft de organisatie niet langer te investeren in een eigen infrastructuur met hardware, storage, security en identity managementsoftware. Een andere belangrijke kostenpost bij een On-Premise-oplossing is configuratie en beheer. Dit vraagt lokaal veel capaciteit en expertise van de eigen organisatie of partners. Daarbij is de vuistregel dat 90 procent van de implementatie standaard en slechts 10 procent klant specifiek is. Desondanks moet de organisatie dit doen of laten doen om een complete oplossing te krijgen. Ook is de organisatie zelf verantwoordelijk voor zaken als versiebeheer en updates.

De implementatie van HelloID IDaaS is letterlijk een kwestie van uren. De installatie van een lichtgewicht agent volstaat. Tools4ever verzorgt vervolgens automatisch updates van de functionaliteit. Er wordt gebruik gemaakt van een wereldwijd gedeelde configuratie die ook automatisch wordt bijgewerkt. Deze verregaande standaardisatie zorgt dat de organisatie alleen verantwoordelijk is voor het beheer van 10 procent organisatie-specifieke zaken en dat is door de opzet van HelloID zeer eenvoudig. De lagere kosten en minimaal beheer gaan niet ten koste van de controle en veiligheid. Integendeel, IDaaS van Tools4ever draait in een maximaal beveiligde Azure-omgeving die bovendien iedere zes maanden grondig gecontroleerd wordt door Deloitte Risk Services. Hiermee is compliance aan de strengste securityeisen gewaarborgd.



OVER TOOLS4EVER

Met meer dan 1,5 miljoen beheerde user accounts is Tools4ever in Nederland marktleider op het gebied van Identity Governance & Administration. Sinds 1999 ontwikkelt en levert Tools4ever hiervoor verschillende softwareproducten en consultancy diensten, waaronder Identity & Access Manager (IAM) en HelloID (IDaaS).

Tools4ever heeft veel koppelingen en strategische partnerships met software leveranciers. De software van Tools4ever wordt toegepast bij deze leveranciers en vice versa. Tools4ever werkt bijvoorbeeld met de software van TOPdesk en werken AFAS en TOPdesk ook met onze software.

Tools4ever's Identity Governance & Administration oplossingen worden geïnstalleerd bij organisaties uit diverse sectoren variërend in grootte, van 300 tot meer dan 200.000 user accounts.

TOOLS4EVER

IDENTITY GOVERNANCE & ADMINISTRATION

TOOLS4EVER BV

Amalialaan 126c
3743 KJ Baarn
Nederland

T +31 (0) 35 54 832 55
F +31 (0) 35 54 327 36

Informatie info@tools4ever.com
Sales sales@tools4ever.com
Support isupport@tools4ever.com