TOOLS4EVER

Whitepaper V2.0 / 22 07 2022

HelloID Security

How Tools4ever secures (personal) data and ensures the privacy of users within HelloID

Table of contents

Carefree and secure management of users and authorisations

Tools4ever is a Dutch software company and market leader in the field of Identity & Access Management (IAM). Since 1999, Tools4ever has been helping organisations to efficiently and securely manage their users and authorisations. Tools4ever develops software for both small companies with about 300 employees and large multinationals with more than 200,000 users. Nowadays, more than 5,000 clients, accounting for at least 10 million users, rely on Tools4ever's IAM solutions.

From on-premise to cloud-based

Tools4ever has translated over 20 years of knowledge and expertise with two generations of on-premise IAM solutions into a modern and secure cloud-based IAM platform: HelloID. HelloID has been available as Identity-as-a-Service (IDaaS) in the cloud since 2015. Traditional IAM solutions are complex and require specialist consultants for every change, but HelloID puts the power of Identity & Access Management in the hands of our clients and partners. Thanks to user account provisioning, self-service workflows, single sign-on and multi-factor authentication, your users gain quick and secure access to their applications and data, wherever they are in the world. The service is always available, regularly updated with new functionalities, and the security is top-tier at all times.

Focus on privacy, information security and compliance

Stricter laws and regulations (GDPR, mandatory data breach notification) and information security guidelines (ISO 2700x, BIO, NEN 7510, IBP) require organisations to implement measures in terms of privacy and information security. IAM is a discipline within cybersecurity that helps organisations provide the right people with the right authorisations and access at the right time. To achieve this result, the IAM solution itself also works with a lot of sensitive data. When selecting security software, it is therefore important to ask the following questions:

- How can we determine who can get access, what they can access, and how they can gain access?
- How are connections established with other systems and applications? What data is shared through the connections? How are the connections secured?
- Which data are stored and how? How are they encoded? What control do we have over our data? How do we ensure that this data cannot leak outside the organisation?
- How do we determine and control who performs which actions? How do we respond quickly if suspicious activity occurs?

Tools4ever highly values the security of our software and the security of the storage of (personal) data. That is why we have invested in appropriate resources and controls to protect our clients. With our software, you can rest assured that:

- **Your information is protected** – Tools4ever protects the confidential information of our clients. We aim to deliver the best customer experience.
- **You can continuously access our services** – Our services are available uninterrupted, and Tools4ever proactively minimises security risks that threaten continuity.
- **Your information security complies with standards and legislation** – Tools4ever adheres to legislation, best practices and industry standards.

These three principles guide everything we do: we continuously focus on refining existing controls and implementing new risk-minimising measures.

In this document, you will learn in more detail how Tools4ever guarantees the security of data and the safeguarding of privacy within HelloID's modules Provisioning, Service Automation and Access Management.

HelloID cloudplatform

HelloID is a cloud platform that consists of three modules which can function both independently and integrated with one another. Based on the needs for user, authorisation and access management and self-service, modules can be enabled and disabled in a flexible way.

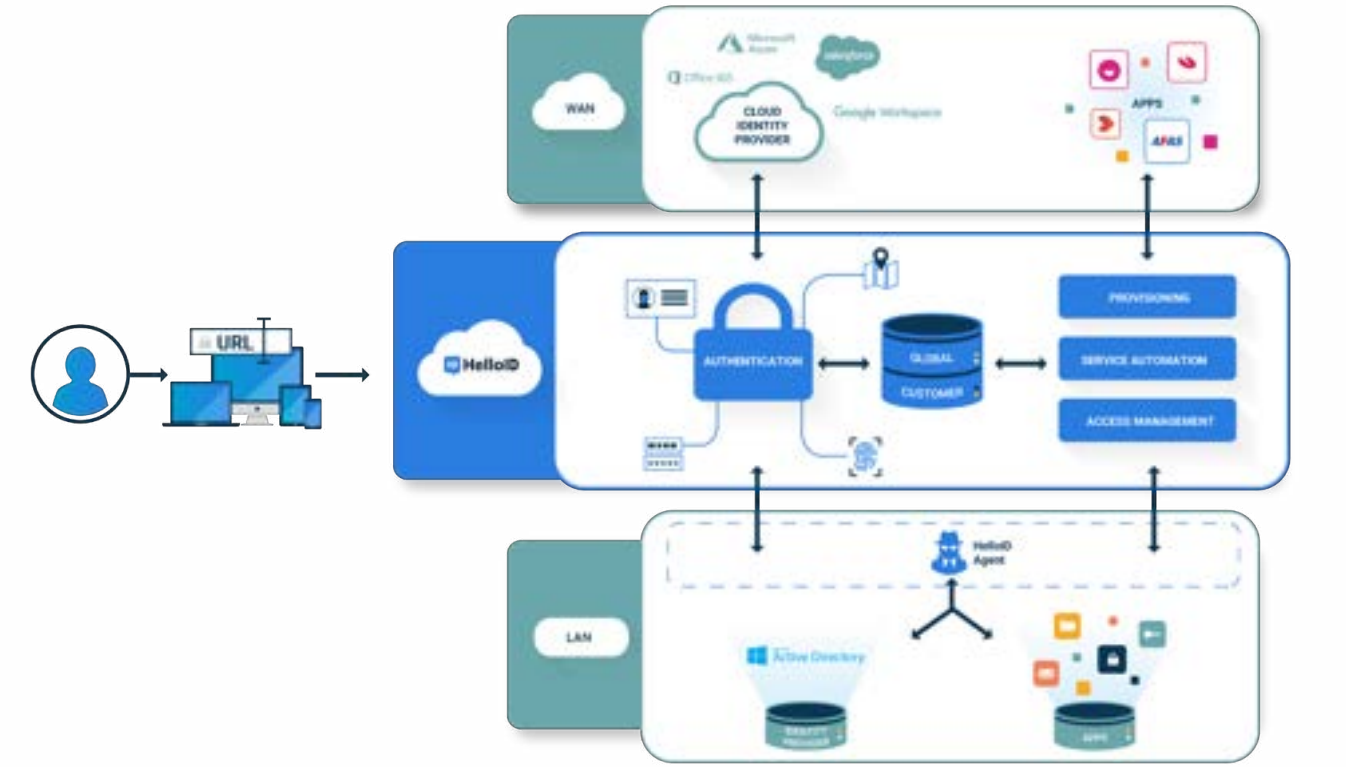
- **Provisioning**
  Automated management of user accounts and role-based authorisation management based on the identity lifecycle, through a link between source and target systems.

- **Service Automation**
  Self-service and delegated forms to handle structured, standardised and automated changes that cannot be executed based on a source system.

- **Access Management**
  Secure and user-friendly access to applications and data via a single set of login credentials, optional two-factor authentication, and according to predefined and conditional access rules.

Architecture

The HelloID architecture consists of various shared and segregated components. The diagram below provides an overview of the key components and how they interact. Information is always encrypted, whether it is in transit or temporarily stored. The level of security varies by component and depends on the extent of impact, risk and technical applicability.

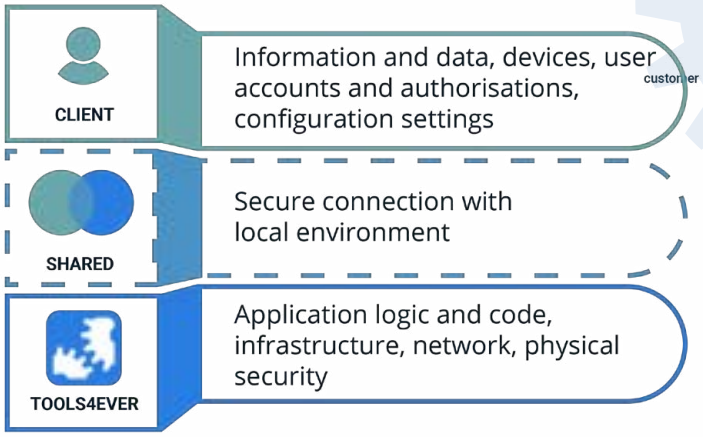


Shared responsibility

In the case of a SaaS solution such as HelloID, it is essential to understand the shared responsibility for information security. The shared responsibility model delineates our responsibilities: those of Tools4ever – the SaaS provider – and yours – as the client and end-user of the software solution.

Responsibility of Tools4ever

Tools4ever is responsible for the security of the HelloID platform, including the physical security, the security of the application itself and the underlying infrastructure. Additionally, Tools4ever is responsible for the availability of the service and we provide mechanisms to protect the data within HelloID. The security measures implemented by Tools4ever that we have made available are discussed in the following chapter: Security measures.



Client responsibility

As a client, you always remain the owner of your data. This means you are also responsible for securing and monitoring the data stored within HelloID against unauthorised access, ensuring the accuracy of the data and protecting it from malicious parties. This includes enforcing a strong authentication policy, correctly managing users and their authorisations, and reviewing the logging available within HelloID.

Security measures

The way in which we design, develop and maintain our solutions is based on ten key principles. These 'security by design' principles, as defined by OWASP, form the basis of our approach:

1	**Minimise attack surface**	Our goal for secure development is to reduce the total security risk by minimising the so-called 'attack surface'. Each function that is added to an application introduces a certain risk to the application as a whole.
2	**Secure default settings**	By default, we deliver the safest possible user experience. It is up to the application user – taking into account his or her mandate – to lower the standard level of security.
3	**Principle of 'least privilege'**	Accounts are granted only the minimum rights necessary to perform the essential business processes. This includes not only user rights but also minimal requirements for CPU limits, memory, network and the file system.
4	**Principle of defense in depth**	Even when one control would seem reasonable, we prefer putting multiple controls in place to address risks in different ways. This principle can ensure that serious vulnerabilities are exceedingly difficult to exploit, making them less likely to occur.
5	**Safe failure**	When executing processes, an application can fail for various reasons. However, the result of such an error determines whether an application is safe or not. All HelloID components are designed to fail safely.
6	**Do not inherently trust services**	Third parties will generally have different security policies and procedures than us. That is why we do not blindly trust external systems and treat all external systems in the same manner.
7	**Segregation of duties**	This is an essential part of the security of process flows. Administrators, for example, should not normally be users of the application.
8	**No security by obscurity**	In our view, the security of important systems should not rely solely on hiding details. We consider this to be a weak form of security.

9	**Keep security simple**	Our approach favors simple code over excessively complex approaches. We do not use double negatives or complex architectures unless absolutely necessary.
10	**Properly resolve security issues**	Once a security issue has been identified, it is important to develop a test for it and to understand the root cause of the problem. When design patterns are used, it is likely that the security issue is widespread across all 'code bases', so developing the correct solution without introducing regressions is essential.

Data centres of internationally recognised leaders

HelloID is hosted on the cloud platforms Microsoft Azure and Google Cloud. Our cloud partners Microsoft and Google are internationally recognised as global leaders in the field of Infrastructure-as-a-Service (IaaS). They have implemented cloud infrastructures that fully comply with global and local requirements. The service is resistant to irregularities and attacks from malicious actors, as the infrastructure is protected across the physical, network, host, application and data layers. Strict security guidelines and operational processes are applied. Furthermore, the services are continuously proactively monitored, and penetration tests are conducted.

Data securely stored in the EEA

Microsoft Azure and Google Cloud have data centres around the world that are divided by region. The distinction in regions makes it possible for you as a customer to place each HelloID portal in the desired region. HelloID currently uses data centres in two regions: the European Economic Area (EEA) and the western United States. The data of our Dutch clients and partners are standardly stored only in the European Economic Area. In doing so, Tools4ever meets the requirements set by the GDPR regarding the location of sensitive data.

High availability and continuity

The HelloID platform is guaranteed to be available up to 99.90% per year. This is made possible by the measures our hosting providers have taken concerning data replication within the region, backup services, and redundancy of power, network and cooling facilities.

The availability and performance of HelloID are continuously monitored. Information about the current and historical availability, (planned) maintenance and outages is publicly accessible via the HelloID status page. If you subscribe to the status updates, you will be notified directly by email in the event of irregularities.

Automated backups

Tools4ever creates automated backups of all databases. The data is kept for 30 days. It is possible to restore the database via Point-in-Time Recovery (PITR) at 4-hour intervals. This makes it possible to restore data to any point in the past 30 days within the set interval. In the event of an incident, the database can often be restored to just before the problem occurred. The application of PITR means that data can be restored with little to no data loss.

HelloID encryption, verification and certificates

Certificates guarantee both the identity and the secure encryption of a website, individual, organisation, device, user or server. Within the HelloID software, encryption is applied to various layers.

Segregated and encrypted databases

Thanks to HelloID, Tools4ever offers a scalable multitenant SaaS solution. The user interface and APIs restrict access to only those data to which the client portal is authorised. The data is logically separated into different databases that are encrypted with AES 256-bit encryption keys. The general HelloID

database contains global configuration settings and portal data. All client-specific configurations and user data are stored in their own client database per portal. The data in this database are encoded with their own encryption key. This setup isolates all tenants from each other and there is no risk of cross-portal access or data contamination.

Secure communication over the internet

Communication over the internet must always occur in a secure manner. The HelloID web server communicates with components over the internet using HTTPS. The level of encryption is TLS 1.2, AES with 256-bit encryption. When using the third-party identity provider (IDP) Active Directory, an IIS web server is required.

Use of a custom URL

By default, your organisation is provided with its own subdomain: 'organisationname.helloid.com', which gives access to HelloID. You can also replace the HelloID URL with your own domain name to increase recognisability for your organisation. Common domain names are, for example, 'login.organisationname.nl' or 'helloid.organisationname.nl'. Since communication with HelloID occurs over HTTPS, you will need a PFX certificate. This can be a wildcard or a domain certificate for the requested URL. The link between HelloID and the domain is validated using a CNAME record.

If you want to use your own domain name, it is recommended to configure it immediately after creating the portal. If you change the URL later, it may affect the operation of identity providers, single sign-on and connections with the local environment.

Secure connection with local infrastructure via HelloID Agent

The standard configuration of HelloID is entirely cloud-to-cloud. For organisations that operate entirely cloud-based, HelloID also works without on-premise components. However, an optional on-premise

'agent' is required when HelloID needs to interface with local resources such as an Active Directory, the file system or a database. The HelloID Agent is a set of three lightweight Windows services that are installed within your organisation's network. The Windows services enable communication with the various HelloID modules.

You can install multiple agents for the purpose of load balancing and task separation. When there are multiple agents, they are grouped into Agent Pools. When an on-premise task is initiated, it is sent to an Agent Pool, which then determines which HelloID Agent in that pool is available and suitable for performing the task. Each Agent Pool requires at least one HelloID Agent to function.

Installation, verification and communication

The HelloID Agent thus acts as a 'broker' that exchanges data and performs local actions. Communication over the internet must always happen in a secure manner. A three-step process ensures secure communication between HelloID and the agent.

Installation

The HelloID Agent communicates with components via the internet using HTTPS. The level of encryption is TLS 1.2, AES with 256-bit encryption. The HelloID Agent can be installed on any server within the domain that has HTTPS access to HelloID. To avoid conflicts with local security policy, this is usually a server that is not a domain controller. The agent's services run on a domain account with local admin rights. Using a local account can lead to login problems for end-users and failing synchronisation tasks. Without local admin rights, the agent cannot update automatically.

Verification

The verification process ensures that your HelloID portal only trusts the correct instance of the agent. During the installation of the agent, HelloID generates an OTP ticket number. This number can only be used once, and only within 10 minutes of its creation. The HelloID administrator provides this number to the agent. Based on a combination of the OTP, the portal URL, and the agent GUID, a shared certificate is generated. This certificate then validates every attempt at communication between HelloID and the agent. If the certificate does not match or if the agent GUID has changed, communication is impossible. If the certificate or the agent is copied or moved, trust is immediately revoked. This verification procedure can only be performed by HelloID administrators with the permission to add agents. No other scenarios are allowed to ensure maximum security.

Communication

The HelloID Agent operates exclusively in one direction, where communication only occurs from the local network to the HelloID portal and never the other way around. It only performs actions that are prepared by the HelloID portal and cannot send commands to the portal itself. When the agent responds to a request, HelloID checks the originating IP address. If this does not match the IP address used during verification, the command is rejected and trust is immediately revoked. No special firewall port opening or DMZ configuration is needed. The agent communicates via the standard TCP port 443. All events and requests to the agent are saved in the log files. The agent further supports load balancing, failover and monitoring.

Directory Agent

The Directory Agent is a service responsible for on-premise tasks related to authentication on HelloID via Active Directory:

- authenticating users in HelloID when using Active Directory as the identity provider
- synchronising user accounts from Active Directory to HelloID

The Directory Agent uses HTTPS with long polling. Each request remains open for 30 seconds. During this interval, the service responds every five seconds with five processes polling simultaneously. Most requests are answered in less than a second. All communication is encrypted using HelloID certificates via TLS 1.2. Each request is verified based on the agent's certificate and GUID

Provisioning Agent

The Provisioning Agent is a service responsible for on-premise tasks related to the Provisioning module of HelloID, such as:

- retrieving data from local source systems such as HR and SIS databases
- managing user accounts and rights in local target systems such as Active Directory and

NTFS, but also in CSV files, SQL and Oracle databases

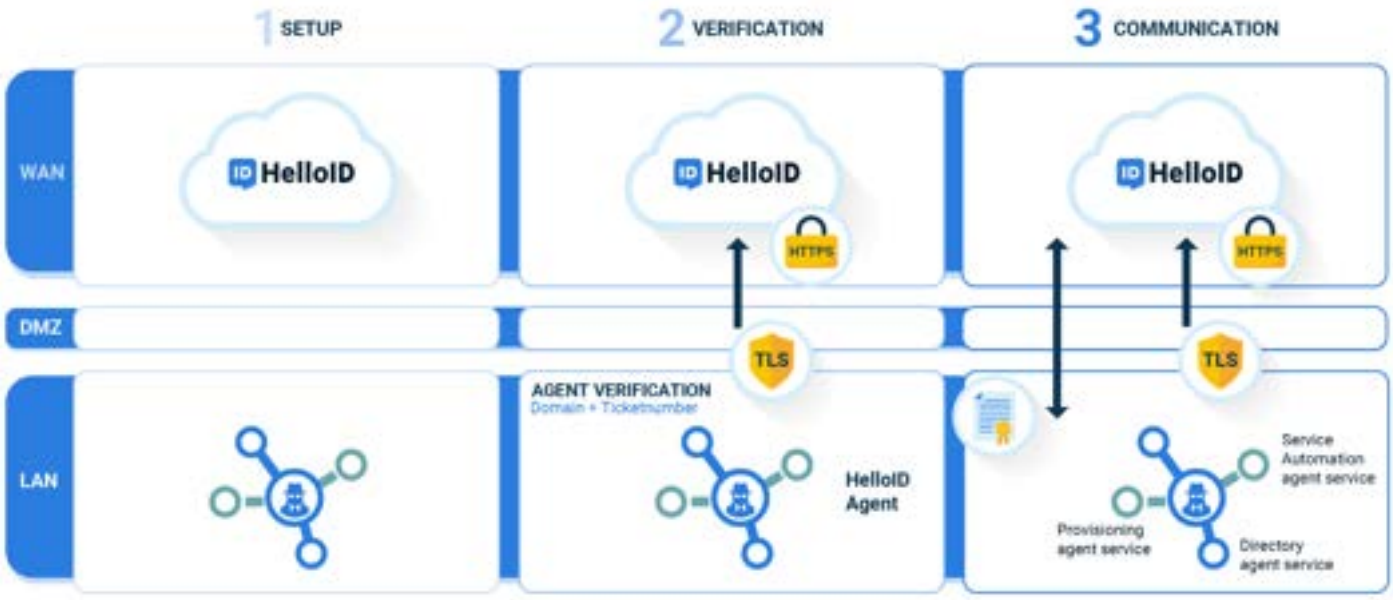
The Provisioning Agent uses secure WebSockets for open, near real-time communication with HelloID. An initial HTTPS request to the HelloID portal is upgraded to a secure WebSocket. The WebSocket is recycled every three hours and has a 60-second heartbeat to check if the connection should remain open. All communication is encrypted using HelloID certificates via TLS 1.2. Each request is verified based on the Agent certificate and the GUID. This service is optimised for near real-time communication, stability and performance during bulk requests.

Service Automation Agent

The Service Automation Agent is a service responsible for all tasks related to the Service Automation module of HelloID. Examples include:

- execution of PowerShell scripts in the context of populating data sources
- execution of on-premise actions for scheduled tasks, approved self-service requests and delegated forms

The Service Automation Agent shares the security features of the Provisioning Agent. This service is optimised for a quick response time to facilitate a smooth user experience. Tasks set up via self-service and delegated forms are picked up and executed almost immediately.



Authentication and authorisation

Authentication refers to the process through which a user's identity is verified to ascertain if the user is who they claim to be. Authenticating as a user or administrator on the HelloID platform is done via one or more so-called identity providers. An identity provider (IDP) is a system in which identity information is managed. For primary authentication to the HelloID application, HelloID supports two types of identity providers:

- HelloID cloud directory
- Third party identity provider

Multiple identity providers can be active at the same time. In practice, HelloID is often linked with a third-party IDP such as (Azure) Active Directory or Google Workplace. The cloud directory then gives your organisation the additional ability to offer access to, for example, clients or patients without the need for a user account to be created in Active Directory.

Authentication via cloud directory

During authentication, the user is identified through the cloud directory integrated into HelloID. This identification is done using a username, and users authenticate themselves with a password. These account details are stored in the cloud, with the password being encrypted. HelloID administrators in your organisation can monitor the complexity and security of the local HelloID user accounts by configuring a password policy for your organisation. They can, for instance, set requirements for password strength based on length and complexity, or exclude common passwords. As an additional layer of security, a second factor, whether conditional or not, may also be required. HelloID supports two-factor authentication (2FA) via SMS, email, one-time passwords (OTP) through both soft and hard tokens, and can integrate with Radius clients.

Authenticatie via third parties

Often, users log into HelloID via a third-party identity provider such as Active Directory. Using a local Active Directory also requires local components in the form of a HelloID Agent and an IIS web server. However, HelloID also supports cloud-to-cloud authentication via identity providers such as Azure, Google Workforce and Salesforce. With these identity providers, login details are not synchronised, but authentication occurs through a 'shared secret' with industry standards like SAML, WS-Federation and OpenID Connect. Users can log in with the login details managed within the IDP, and the third party validates these for accuracy per authentication request.

Fine-tuned rights and roles

Once a user is authenticated, their roles determine which parts of HelloID the user may access. A role is a collection of rights and privileges that can be assigned to one or more users. Basic roles are available within HelloID by default, but organisation-specific user roles can also be defined. The actions that can be performed per role are precisely adjustable based on the CRUD system (Create, Read, Update, Delete).

On one hand, this determines which actions a specific user is allowed to perform. For example, it can be configured so that someone with an administrator role may edit and delete reports, while someone with a manager role can only view them. On the other hand, you can also define which components are visible to users within a role. Each component within the HelloID user interface can be enabled or disabled per role, allowing your organisation to decide which functionalities can be used. The assignment of a role can be performed manually by an administrator, but roles can also be assigned based on groups within the local HelloID directory or the linked identity provider.

Connecting with target systems

With HelloID Provisioning, the creation and management of user accounts and rights in the network and applications are automated as much as possible based on a link with a source system. The HelloID Service Automation module seamlessly integrates with HelloID Provisioning. In addition to automated provisioning from the HR system, there will always be incidental 'custom' service requests. Incidental changes can be automated with the Service Automation module. The HelloID Agent takes care of the synchronisation with local source and target systems. With cloud-based applications, connectivity is entirely from the cloud. HelloID has the capability to interface with the APIs and web services of source and target applications through protocols such as SOAP/XML, REST/JSON, SCIM and ODBC. Connections over the internet are established via HTTPS.

Single sign-on to connected applications

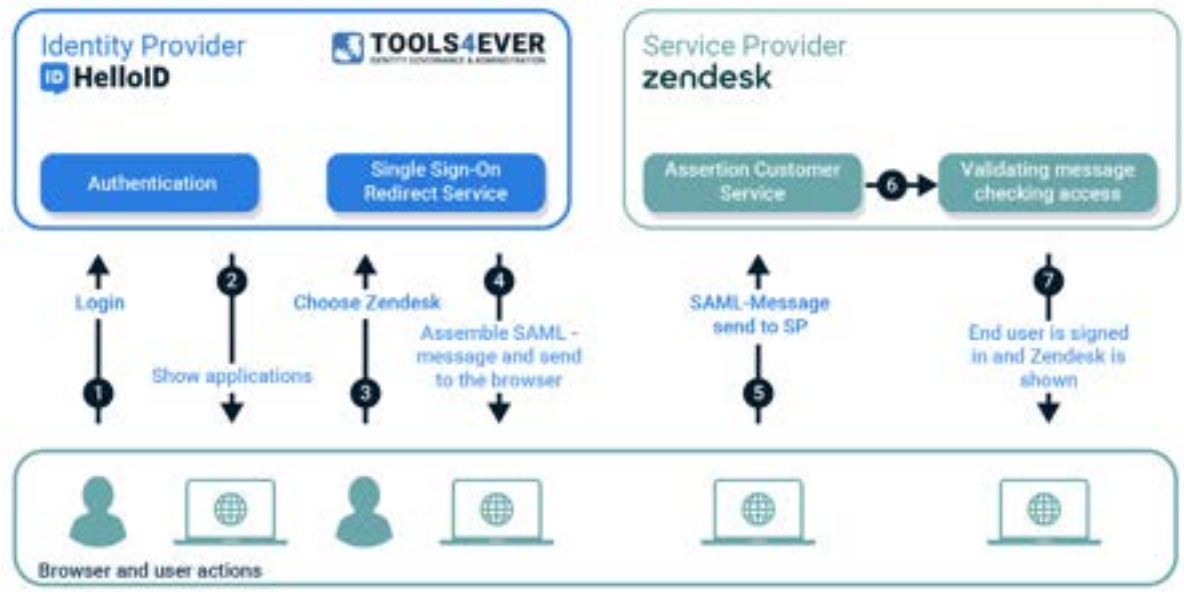
Once the user is authenticated to the HelloID portal, it is possible to automate authentication to other applications via single sign-on (SSO) using the optional Access Management module. In that case, the end-user does not need to log in again to the applications that is linked to HelloID. This means that HelloID becomes the identity provider for the respective applications. To enable SSO, HelloID supports all common SSO protocols such as SAML, WS-Federation and OpenID Connect. For applications that do not support SSO themselves, fallback options include HTTP(S) Post, basic authentication and the HelloID plug-in.

SAML en WS-Federation

SAML is one of the most commonly used standards for exchanging authentication data and enables single sign-on (SSO). The SAML protocol manages authentication and authorisation of a user between an identity provider (IDP) and service provider (SP). *WS-Federation* is a protocol primarily employed by Microsoft and IBM but has a comparable flow. In the usual combination with ADFS, SAML messages are also utilised.

Within HelloID, SAML authentication and authorisation work as follows:

1. A user sends a request to log in, and HelloID validates the request.
2. HelloID displays an overview of applications that the user is allowed to use.
3. The user selects an application.
4. HelloID creates a SAML message to perform authentication with the SP. HelloID signs and encrypts the message using a certificate and sends it to the browser.
5. The SAML message is sent to the corresponding SP.
6. The SP checks the SAML message based on the certificate and validates the access.
7. The user is logged into the SP without the intervention of a login page.



OpenID Connect

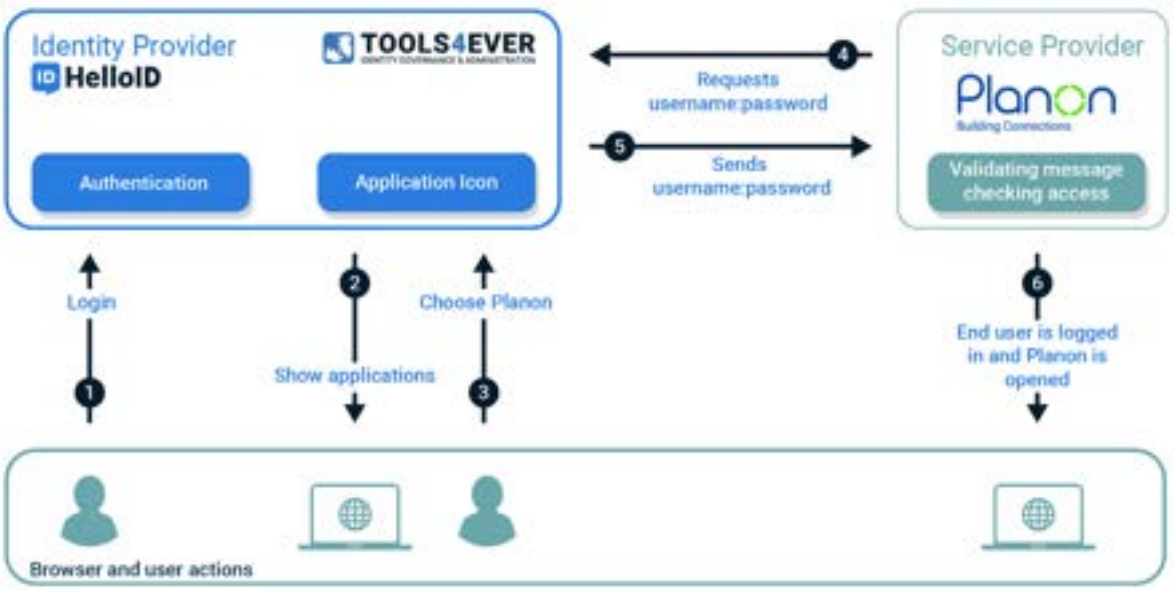
OpenID Connect (OIDC) is an open standard built on the OAuth 2.0 protocol. Authentication works through an ID token, also known as a JSON Web Token (JWT).

Authentication via OpenID Connect works as follows:

1. A user sends a request to log in and HelloID validates the request.
2. HelloID displays an overview of applications that the user is allowed to use.
3. The user selects an application.
4. Generate authorisation code and request token.
5. HelloID validates the user and sends the user back to the application with a token.
6. The application validates the token and creates a session for the user.
7. The user is logged into the application without the intervention of a login page.

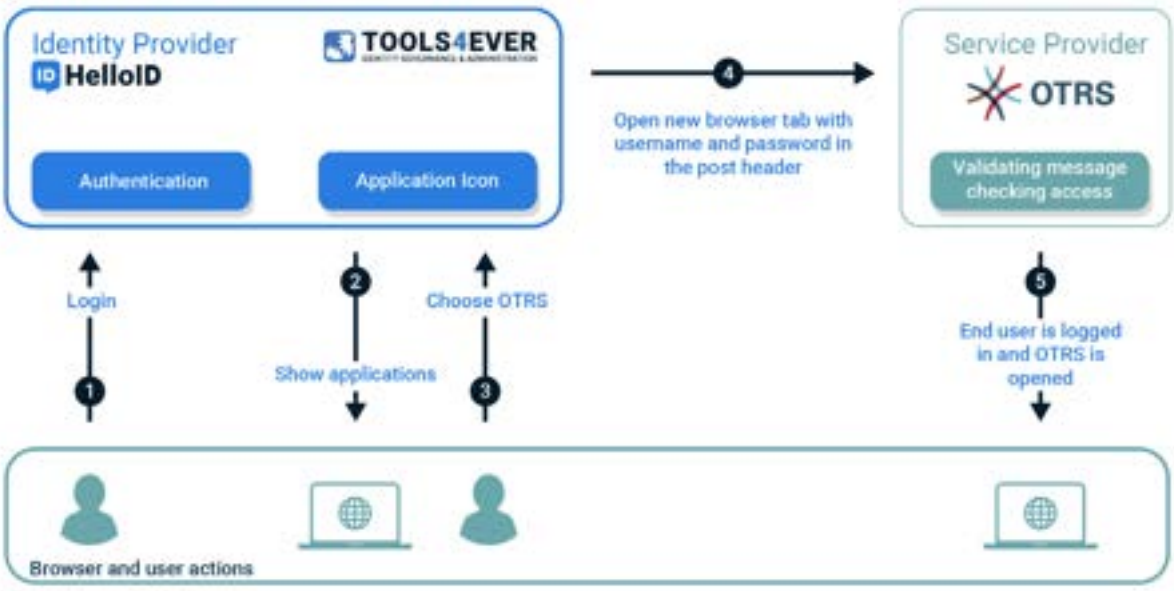
Basic authentication

Basic authentication is a simple authentication scheme built on the HTTP(S) protocol. HelloID sends an HTTP request with an authorisation header containing the word 'Basic' and a base64-encoded string with the username and password. The application receives the authentication request, decodes the authorisation header, splits the username and password, and then uses these to validate the user



Form post

The *'form post'* mechanism places the username and password in the HTTP(S) POST header that is sent to the web application. This mechanism is also used when a user gains access to the application via the usual login page of the website. The login page places the user data in the header (client-side), and the application (server-side) reads this data, verifies it and authenticates the user. For applications that do not support SSO protocols, HelloID can use this mechanism to log in automatically. HelloID supports both HTTP and HTTPS. Tools4ever strongly recommends HTTPS due to the significant increase in security through



Plug-in authentication

For applications that do not support any of the aforementioned methods, you can use the HelloID browser plug-in. Within HelloID, it is determined which applications and which URLs the plug-in should handle. The plug-in uses a secure SSL connection with the HelloID platform to obtain authentication data such as a username and password. The login credentials are not stored by the plug-in but are used directly for SSO. The plug-in recognises the input fields of the web application's login form based on, among other things, unique identifiers. Then the plug-in automatically fills in the fields with the user's login details. Depending on how the login form works, HelloID can send the login details automatically, or the user may need to briefly press the login button themselves.

Storage of personal data

Tools4ever processes the personal data of clients to be able to deliver its services. A distinction is made between the personal data that are minimally required for the functioning of the acquired HelloID modules and the personal data that you as a client wish to process. By default, HelloID does not process data that is marked as 'special categories of personal data'.

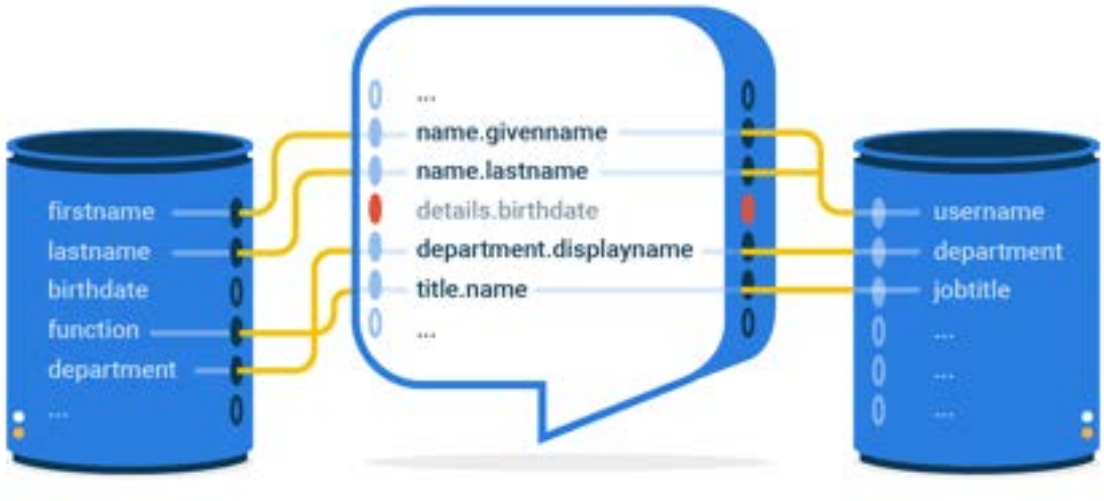
Below you will learn which data are minimally required for each module:

- **Provisioning** - requires at least the name (initials, first name, insertion, surname, preferred name) and contract details (employee number, job title, department, organisation, date of joining and leaving) to manage users and authorisations.
- **Service Automation** - requires at least the login name and display name to authenticate on the portal.
- **Access Management** - like Service Automation, requires at least the login name and display name to be able to log in to the portal.

As a client, you can decide if Tools4ever may process additional data. Through the HelloID 'attribute mapper', Tools4ever's administrators and consultants and partners can configure which data from linked systems will and will not be processed and/or stored in the HelloID database. This configurable mapping ensures that the HelloID database remains fully compliant with your organisation's privacy and security policies at all times.

Reporting and logging

Reporting and logging are fundamental components of any security policy and are required by both laws and regulations as well as information security guidelines. HelloID logs all significant events. Logging sets up an 'audit trail' that provides insights into the use of the HelloID environment. It can identify potential security risks. All actions performed within and by HelloID are stored in Elastic reporting, which offers extensive options for reporting.



Below you will find various examples of the data that are logged, per module:

- **Provisioning**
  All actions performed per system and person are logged concerning the creation, enabling, updating, moving, disabling and deletion of accounts, and the granting and revoking of permissions.
  Service Automation

- **Service Automation**
  For self-service products, information is stored about the request, workflow and approval. With delegated forms, all data is stored about requests, form data and audit information for configuration changes.

- **Access Management**
  Recorded events include successful and unsuccessful logins, the geographic location of the user, devices used, initiated password resets, application access attempts and failed access attempts as a result of the access policy.

Accessing logging data

The data from Elastic can be displayed via the built-in reporting features or used in combination with your own business intelligence (BI) tooling such as PowerBI. All logging data within Elastic is available in near real time and can be read via REST APIs. By using authentication with a HelloID API key, you can be assured that only authorised persons can view the logging data.

Duration of data retention

Within HelloID, data retention periods are distinguished between data stored by the client on the platform and the (audit) logging. User and configuration data are retained for the entire contract duration. Upon termination of the HelloID contract, the data are kept for a maximum of 3 months and thereafter automatically deleted.

HelloID stores internal audit logging for 30 days. After the expiry of this retention period, the logs - including the backup - are deleted. The audit logging accessed via the Elastic reporting platform is retained for one year. After that, these data - including the backups - are erased. If it is desired or required by law and regulation to retain data for a longer period, you can export them to your own reporting/archive/auditing tool via the available APIs. In this way, your organisation has full control over the retention period of the (audit) logging.

Data breach protocol

In the event of a data breach, the data breach protocol is activated to ensure that clients are aware of incidents. Upon discovering a security incident or data breach, Tools4ever notifies its clients within 24 hours as prescribed by the protocol. Tools4ever sends this notification via email to the contact person within your organisation. Tools4ever does not itself make a direct notification to the Data Protection Authority or individuals involved.

Physical security and authorisation policy of Tools4ever

The office of Tools4ever is secured in various ways. Surveillance cameras are used both inside and around the building, and access to the premises is restricted with RFID tokens that are linked to individual persons. Additional forms of access security are also applied, particularly for server, storage and electricity rooms.

When handling client data, Tools4ever adheres to a strict policy. Confidentiality agreements are in place with employees, and they only have access to data that is strictly necessary for their roles. Two-factor authentication is used for accessing systems and applications. Tools4ever promotes awareness, education and training regarding privacy and information security. Trained security managers for information policy and IT security oversee the adherence to the policy and regularly update security measures.

Standards and certifications

The HelloID platform is hosted on the Infrastructure-as-a-Service (IaaS) solutions of Microsoft and Google. Both providers are internationally recognised for the very high security standards which they meet, and the security of our platform is guaranteed based on the service level agreement with both parties. Additionally, HelloID as an IDaaS solution helps you, the client, comply with various (sector-specific) information security standards and certifications. Tools4ever also finds it important to meet standards set by the software industry and ensures there is systematic scrutiny by other parties of our systems, processes and procedures.

OWASP

The 'security by design' principles as defined by OWASP form the basis of our approach.

Microsoft Gold Partner

Tools4ever is ISO 27001 certified, meaning that Tools4ever has a well-organised management system for information security. Specifically, this means that we develop software in a secure and controlled manner, but also that we act adequately in the face of potential risks or security incidents. In 2022, we will add SOC 2 certification.

ISO 27001

Deloitte Risk Services conducts penetration tests twice a year. The report of findings provided by Deloitte is addressed with high priority by our development department for implementation, and/or Tools4ever provides a substantive response.

Deloitte.

Tools4ever has a long-standing Microsoft Gold Partnership and possesses specific security expertise in working with the Microsoft product suite.

TOOLS4EVER

Address	102-103 Church Street, GL20 5AB, Tewkesbury, UK
General	+44 (0)1684 274 845
Support	+44 (0)1684 270 822
Information	uksales@tools4ever.com
Sales	uksales@tools4ever.com
Support	uksupport@tools4ever.com