PRODUCT FLYER

HELLOID SECURITY

What happens to your data?

The HelloID database contains global configuration settings and customer information. Your customer database will contain all of your organization's specific configurations and user data. All data, sensitive or otherwise, is encrypted using an RSA 1024-bit encryption key. Each customer has their own separate database and encryption key.

The customer can configure exactly which user data is available for retrieval from other source systems and stored in the HelloID database. Administrators use the HelloID attribute mapper to configure which attributes from the source system—Active Directory (AD) in this example—will be used in the HelloID database. Thus, if the first name of a user is stored in AD, the customer may choose whether this attribute will be made available in HelloID. This configurable mapping ensures that the HelloID database always remains fully compliant with your organization's privacy and security policy. All tenants with a HelloID instance are completely insulated from each other. This way, only the relevant data is synchronized instead of 100% of the available fields.

Internet communications

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.

Take complete control of your security.

- ✓ Hosted on Microsoft Azure Cloud
- ✓ Backed by biannual Deloitte security testing
- ✓ Active compliance and certification policy
- ✓ RSA 1024-bit encryption on data

PRODUCT FLYER

Active compliance

Tools4ever has an active compliance and certification policy. A recent example of this is our HelloID OpenID certification. The HelloID OpenID certification confirms the high quality of the OpenID Connect implementation as part of our HelloID Identity-as-a-Service (IDaaS) solution, further reinforcing our customers' confidence in the quality of our services.

Our cloud IDaaS provider, Microsoft Azure, maintains the largest compliance portfolio in the industry both in terms of breadth (total number of offerings), as well as depth (number of customer-facing services). Compliance covers major, globally applicable standards and certifications.

See HelloID Security Whitepaper for more information on Microsoft Azure Cloud.

Deloitte security testing

In addition to in-house testing done by our team of security experts, HelloID is externally tested twice a year by the top-class ethical hackers of Deloitte. Deloitte is an independent, highly-qualified market leader in information security and was ranked first in global Security Consulting Services for six consecutive years by Gartner. By proactively and frequently testing our security solutions, we are able to meet and exceed security requirements while complying with relevant industry standards.

We implement security standards to ensure internal and external security

Amongst various technical security standards like HTTPS, SSL certificates, RSA and AES encryption, we also follow the NCSC ICT-B v2 guidelines. HelloID is penetration tested by Deloitte according to NCSC ICT-B v2 guidelines and with the use of e.g. OWASP Top 10 Application Security Risks

We provide backups for peace of mind

Your HelloID data is backed up, encrypted, and stored in multiple data centers for maximum redundancy. In the event of a disaster, your information can be recovered and restored to any point in time. This recovery can be done as needed, or upon customer request.

We create backups within very short periods of time (e.g. SQL DB backups). These can be used to restore your instance to the specific could environment from any point in time. Backups are stored and encrypted in multiple data centers in the Azure cloud for protection/resiliency. Restoring a customer's instance can be performed anytime on request.

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

New York
300 Merrick Road, Suite 310
Lynbrook, NY 11563
(866) 482-4414
nainfo@tools4ever.com

Washington
11515 Canyon Road E
Puyallup, WA 98373
(888) 770-4242
nwsales@tools4ever.com