



ID LA SÉCURITÉ HELLOID

Qu'advient-il de vos données ?

La base de données HelloID contient des paramètres de configuration globale et des informations client. Votre base de données clients contiendra toutes les configurations et données utilisateur spécifiques de votre organisation. Toutes les données, sensibles ou non, sont cryptées à l'aide d'une clé de cryptage RSA 1024 bits. Chaque client a sa propre base de données et sa clé de chiffrement distincte.

Le client peut configurer exactement quelles données des utilisateurs sont disponibles pour être récupérées à partir d'autres systèmes sources et stockées dans la base de données HelloID. Les administrateurs utilisent le mappeur d'attributs HelloID pour configurer les attributs du système source qui seront utilisés dans la base de données HelloID. Ainsi, si par exemple le prénom d'un utilisateur est stocké dans AD, le client peut choisir si cet attribut sera rendu disponible dans HelloID. Ce mappage configurable, garantit que la base de données HelloID reste toujours entièrement conforme à la politique de confidentialité et de sécurité de votre organisation. De cette façon, seules les données pertinentes sont synchronisées au lieu de 100% des champs disponibles. Toutes les instances HelloID sont complètement isolées les unes des autres.

Prenez le contrôle total de votre sécurité.

- ✓ Hébergé aux Pays Bas
- ✓ Soutenu par les tests de sécurité semestriels de Deloitte
- ✓ Politique de conformité et de certification active
- ✓ Cryptage des données en RSA 1024 bits

Communications Internet

Le serveur Web HelloID communique avec les composants sur Internet en HTTPS. Le niveau de cryptage est le TLS 1.2, AES avec cryptage 256 bits.

Conformité active

Tools4ever a une politique de conformité et de certification active. Un exemple récent de cela est nos certifications HelloID OpenID, ISO27001 et NEN 7510. La certification HelloID OpenID confirme la haute qualité de la mise en œuvre d'OpenID Connect dans le cadre de notre solution HelloID Identity-as-a-Service (IDaaS), renforçant encore la confiance de nos clients dans la qualité de nos services. La certification ISO27001 confirme que les solutions Tools4ever sont en règle en matière de sécurité de l'information. La certification NEN 7510 est une extension de la norme ISO207001 dédiée au secteur hospitalier dans le cadre de la numérisation des données des patients.

Notre fournisseur de cloud IDaaS, Microsoft Azure, maintient le plus grand portefeuille de conformité du secteur, tant en termes d'étendue (nombre total d'offres) que de profondeur (nombre de services destinés aux clients). Cette conformité couvre les principales normes et certifications applicables à l'échelle mondiale.

Consultez **Le Livre blanc de la Sécurité HelloID** pour plus d'informations sur Microsoft Azure Cloud.

Tests de sécurité Deloitte

En plus des tests internes effectués par notre équipe d'experts en sécurité, HelloID est testé en externe deux fois par an par les meilleurs hackers éthiques de Deloitte. Deloitte est un leader indépendant et hautement qualifié du marché de la sécurité de l'information et a été classé premier dans les services mondiaux de conseil en sécurité pendant six années consécutives par Gartner. En testant de manière proactive et fréquente nos solutions

de sécurité, nous sommes en mesure de répondre aux exigences de sécurité et de les dépasser tout en nous conformant aux normes pertinentes de l'industrie.

Nous mettons en œuvre des normes de sécurité pour assurer la sécurité interne et externe

Parmi les différentes normes de sécurité technique comme HTTPS, les certificats SSL, le chiffrement RSA et AES, nous suivons également les directives NCSC ICT-B v2. HelloID est testé contre la pénétration par Deloitte selon les directives NCSC ICT-B v2 et avec l'utilisation par exemple OWASP : Top 10 des risques de sécurité des applications.

Nous réalisons des sauvegardes pour votre tranquillité d'esprit

Vos données HelloID sont sauvegardées, chiffrées et stockées dans plusieurs centres de données pour une redondance maximale. En cas de sinistre, vos informations peuvent être récupérées et restaurées à tout moment. Cette récupération peut être effectuée selon les besoins ou à la demande du client.

Nous créons des sauvegardes dans des délais très courts. Ceux-ci peuvent être utilisés pour restaurer votre instance dans l'environnement spécifique à tout moment. Les sauvegardes sont stockées et chiffrées dans plusieurs centres de données dans le cloud Azure pour leur protection/résilience. La restauration de l'instance d'un client peut être effectuée à tout moment sur demande.