DTS

DTS
Identity

Identity

Les identités et autorisations numériques jouent un rôle essentiel dans l'informatique. Une gestion des identités et des accès (IAM) attribue ces identités et met en correspondance toutes les autorisations d'accès. Sans cela, vous vous exposez à de graves dangers tels que des accès et des connexions compromis, des rançongiciels, des hameçonnages, des logiciels malveillants, etc. L'IAM est un outil essentiel pour protéger les données et répondre aux exigences de conformité.

En tant que fabricant de logiciels de sécurité informatique, notre objectif est d'empêcher les cybercriminels et les utilisateurs non autorisés d'accéder aux applications et aux données. C'est pourquoi nous avons développé une plateforme qui découple et gère l'identification des utilisateurs. Le résultat est un accès sécurisé et sans ambiguïté pour les utilisateurs, les applications et le cloud ; pour les entreprises et leurs clients.

Notre solution offre les avantages objectifs suivants :

Protection accrue grâce à l'authentification multi-facteurs et à la gestion des accès ; prévention de la prolifération des applications, des droits et des autorisations dans la gestion des accès ; conformité avec la réglementation européenne GDPR en matière de protection des données ; pas d'externalisation des données vers les États- Unis ou en dehors de l'UE ; grande flexibilité dans l'adaptation des fonctionnalités à la croissance dynamique des entreprises.

- Plate-forme centrale pour IAM et CIAM
- Solution „as a Service" utilisable à partir de nos centres de données certifiés et conformes au GDPR
- Multi Factor Authentication, gestion des accès et des profils
- Dashboard central et intuitif pour la gestion et les applications
- Access Gateway pour l'identité - Standard SAML et OIDC
- SSO pour les applications locales ou en cloud
- Libre-service et personnalisation de l'identité d'entreprise
- Focus sur la sécurité informatique

L'Identity suit le principe de l'authentification multifactorielle, dans lequel un utilisateur accède à toutes les applications locales ou en nuage connectées via une authentification unique (SSO). Toutes les applications avec les normes OIDC ou SAML peuvent être associées. Les applications autorisées sont visibles sur le tableau de bord après la première connexion et peuvent être gérées de manière centralisée ici - tout en un seul aperçu. Une base de données dédiée gère toutes les données et les mots de passe des utilisateurs. En outre, les services d'annuaire ou les systèmes d'authentification existants, la gestion des groupes et le stockage des attributs peuvent être utilisés via la connexion AD/LDAP.

Grâce au contrôle d'accès basé sur les rôles (RBAC), différents rôles peuvent être créés. Une fois qu'un utilisateur s'est vu attribuer un rôle, il reçoit les autorisations et les accès prédéfinis dans les applications. Les applications apprennent automatiquement quel est le rôle de l'utilisateur et peuvent afficher ou partager des ressources en conséquence. Cela évite aux administrateurs informatiques de distribuer séparément les autorisations, rend possible une prise en main rapide et limite la génération incontrôlée d'autorisations. Identity permet également l'autorisation d'API Machine-to-Machine (M2M). Dans ce cas, une application s'authentifie via Identity, qui valide ces informations et renvoie un jeton d'accès. L'application peut ensuite utiliser le jeton d'accès pour demander des ressources à cette API - de manière entièrement automatique.

DTS Identity offre une expérience utilisateur intuitive. Chaque utilisateur, en fonction des autorisations qui lui sont attribuées, peut modifier de manière autonome les données et les paramètres de la plateforme en libre-service, tels que la gestion des accès, la langue, les options de vérification ou la personnalisation de l'identité du client. Dans le tableau de bord, les administrateurs peuvent visualiser toutes les activités de la plateforme, telles que le nombre de connexions, le nombre d'utilisateurs, les organisations connectées, les applications et les API associées. Dans la section Gestion, il est possible de créer de nouvelles organisations, d'inviter des utilisateurs, d'attribuer des autorisations et des rôles, d'associer des applications et des API et de consulter les journaux.

Nous nous concentrons sur la sécurité informatique moderne. C'est pourquoi les mots de passe des systèmes externes sont déjà cryptés dans les navigateurs et ne sont jamais affichés par Identity. La protection contre les attaques de type Brute-Force est également garantie. Identity compare les mots de passe les plus courants avec ceux choisis par l'utilisateur et, si nécessaire, en demande un autre à utiliser. Si des données de connexion compromises sont utilisées, une détection de violation de mot de passe en avertit l'utilisateur et l'invite à modifier son mot de passe. En plus du mot de passe, un facteur supplémentaire peut être configuré, par exemple un message par SMS ou par e-mail. L'enregistrement des journaux, c'est-à-dire le suivi de toutes les activités, complète le niveau de sécurité déjà élevé.

Le nombre d'entreprises qui ne gèrent pas uniformément l'administration d'AD et la gestion des droits est élevé. Dans le même temps, on utilise souvent des applications ou des microservices accessibles à différents groupes de personnes. DTS offre une plateforme centrale „as a Service". Cela signifie que nous fournissons l'Identity, y compris le support, à partir de notre DTS Cloud, afin qu'il puisse être utilisé dans un environnement dédié et automatisé.

Cas d'utilisation d'un intérêt particulier :

- **Utilisation dynamique en tant que IAM et CIAM,** sia per B2E, B2B che B2C
- **Respect des exigences de conformité** par exemple, en rapport avec le règlement européen GDPR qui exige la minimisation des droits d'accès, ainsi que la démonstration de la conformité et de la gestion du consentement pour le traitement des données des clients
- **Mise en œuvre des politiques,** par exemple en ce qui concerne les directives internes du "Home Office"
- **Onboarding & Offboarding efficaces** également pour les entreprises multisites, avec des structures d'autorisation ciblées et automatisées
- **Politique et gestion normalisées des mots de passe**
- **Intégration sécurisée des clients et des partenaires,** par exemple, lorsqu'il est nécessaire d'accorder l'accès au réseau de l'entreprise à des utilisateurs externes de manière ciblée et contrôlée
- **Profil client unifié.** „One face to the customer", y compris son Corporate Identity
- **Visualisation des activités des clients** attravers un dashboard intuitif
- **Soutenir le développement interne de solutions logicielles** dans l'authentification et l'autorisation des utilisateurs : plus de sécurité sans devoir déposer des données en dehors de l'Union européenne

ISL DTS Identity 27022023 FR

ISL Member of the DTS Group

ISL
+49 234 976672-0
www.isl.de
info@isl.de

Soufian Rhazi
+49 234 976672-37
france@isl.de

DTS
+49 5221 1013-000
www.dts.de
info@dts.de