DTS

DTS
Identity as a Service (IDaaS)

Identity as a Service (IDaaS)

Digital identities and authorizations play an important role in IT. Identity & access management (IAM) should assign these identities and map all access authorizations. Without IAM, gateways are open for compromised logins and accesses, ransomware, phishing, malware and much more. The goal: secure data and meet compliance guidelines.

As a cyber security software vendor, we want to prevent cyber criminals and unauthorized users from accessing apps and data. That's why we developed a platform that decouples and manages user identification. The result is a single, secure gateway for users, apps and the cloud - for entire enterprises, their customers and connections. Second, we provide you with the answer to these questions:

Do you want to better protect yourself with multi factor authentication & access management?

Do you want to avoid uncontrolled growth in applications, rights & approvals and access management?

You want to comply with the EU-DSGVO & prove this?

You don't want to outsource data to the USA & foreign countries?

You want to grow dynamically & the features should grow with it?

Our answer: "Cyber Security made by DTS" with DTS Identity as a Service (IDaaS). We enable centralized, midmarket-friendly IAM to the highest standards. The self-developed, intuitive platform ensures secure authentication, access control and profile management - automatically, scalable and securely provided from the German, certified DTS Cloud!

- IAM & CIAM on a central platform
- SaaS delivered from own certified & EU-DSGVO compliant data centers
- Multi factor authentication, access management & profile management
- Centralized, intuitive dashboard for all management & applications
- Access gateway for identity standards SAML & OIDC
- SSO for local or cloud apps
- Self-Service, incl. CI customizing
- Cyber security focus

The IDaaS follows the principle of multi-factor authentication, in which a user logs on once to all connected, local or cloud apps via single sign-on (SSO). All applications with OIDC or SAML standards can be bundled. After the single sign-on, the approved apps are visible on a dashboard and can be controlled centrally from there - everything at a glance. A separate database manages all user data and passwords. In addition, existing directory services or systems can be used via AD/LDAP connection for authentication, administration of groups and storage of attributes.

Different roles can be created using Role-based Access Control (RBAC). Once a user is assigned a role, he or she is given the predefined permissions and access in the applications. An app automatically learns which role the user has and can display or release resources accordingly. This way, your IT is spared the separate distribution of permissions, fast onboarding is possible and it limits possible proliferation of permissions. IDaaS also provides machine-to-machine (M2M) API authorization. An application authenticates itself with the IDaaS, which validates this information and returns an access token. The application can then use the Access Token to request resources from this API - fully automatically.

The management of the DTS IDaaS is focused on an intuitive user experience. Each user can independently edit data and settings on the self-service interface, depending on the rights assigned. In addition to access management, this also applies to language, verification options and CI customizing. In the dashboard, admins can see all activities within the platform, including the number of logins, the number of users, connected organizations, connected apps and APIs. In management, new organizations can be created, users invited, permissions and roles assigned, apps and APIs connected, and logs viewed.

Our focus is on modern cyber security. For this reason, passwords for external systems are already encrypted in the browser and never viewed by the IDaaS. Protection against brute force attacks is also guaranteed. The IDaaS compares the most common passwords with the user‘s selection and asks to use a different one if necessary. Should login data be used that is compromised, the Breached Password Detection indicates this with a request to change the password. In addition to the password, another factor can be configured, e.g. messages via SMS or e-mail. Log reporting, i.e. the tracking of all activities, completes the high security level.

There is a wide range of companies where AD administration and authorization management are not standardized. At the same time, there are usually a wide variety of apps or micro services that can be accessed by several groups of people. „As a Service“ means that we provide the IDaaS from our DTS Cloud, including support, so that you can use it in a dedicated, automated environment. In this way, we enable a central platform for all companies.

Use cases from which you will particularly benefit:

- **Dynamic deployability as IAM & CIAM,** whether for B2E, B2B or B2C.
- **Fulfillment of compliance requirements,** e.g. with regard to the EU-DSGVO, which requires minimization of access rights as well as proof of compliance and consent management for customer data
- **Transparency & control through visibility to all included apps and connected users**
- **Enforcement of policies,** e.g. for internal guidelines on home office use
- **Efficient, cross-site onboarding & offboarding** for targeted, automated authorization structures• Standardisierte Passwort-Politik & -Verwaltung
- **Standardized password policy & management**
- **Secure integration of customers & partners,** e.g. if external users need to be granted access to the company network in a targeted and controlled manner
- **Uniform customer profile** for „one face to the customer“, incl. own CI
- **Overview of customer activities** on the clear dashboard
- **Support of in-house developments** regarding authentication and authorization of users to avoid insecure products and without moving data abroad