



Land de Hesse (Allemagne)

Profil

- HZD : prestataire de services informatiques du Land de Hesse.
- 800 salariés proposent des solutions axées sur la pratique.

Utilisateurs

- 60 000 agents du Land de Hesse.

Défis

- Accès simplifié et plus sûr aux applications.
- Nombreux identifiants et mots de passe différents.

Résultats-clés

- **Gain de temps** avec l'authentification unique.
- **Sécurité renforcée** : un seul mot de passe à retenir pour les agents.
- **Efficacité accrue** grâce à la collaboration simplifiée entre les applications.
- **Réduction des coûts** : la charge du help desk baisse de près de 30 %.

Une grande collectivité territoriale sécurise ses postes de travail.

Faciliter la tâche des agents du gouvernement du Land

Implantée à Wiesbaden et Hünfeld, la société HZD fournit des services informatiques au gouvernement du Land de Hesse. Elle travaille en tant qu'entreprise régionale gérée par le Land. HZD, qui allie une compétence informatique orientée marché à 40 années d'expérience dans le secteur de l'administration, propose des solutions personnalisées globales, de la phase de planification d'un projet jusqu'à sa mise en œuvre et son exploitation.

L'informatisation de l'administration a un double objet : servir les citoyens et les entreprises et faciliter le travail des fonctionnaires du Land. En période de difficultés économiques, il est important de rationaliser les processus et de réduire les coûts.

Prestataire du Land de Hesse depuis 1970, HZD n'a eu de cesse de consolider ses compétences en la matière. Travaillant en étroite collaboration avec les agents du Land, les quelque 800 salariés de l'entreprise s'impliquent dans le développement et l'exploitation de solutions pratiques au service d'une administration proche des citoyens.

Le single sign-on, pour concilier sécurité et facilité d'utilisation

Les procédures d'identification des nombreuses applications métier alourdissent au quotidien le travail des utilisateurs de PC, et notamment les fonctionnaires de la Hesse. En effet, chaque application peut disposer de sa propre gestion des utilisateurs, avec des mots de passe spécifiques régis par des règles particulières. La conséquence pour l'utilisateur est qu'il doit se souvenir d'une multitude d'identifiants et de mots de passe distincts.

Cette surcharge, excessive pour de nombreux salariés, entraîne des risques importants pour la sécurité. Il arrive fréquemment que les utilisateurs définissent des mots de passe identiques pour des applications différentes, ou bien qu'ils notent une série de mots de passe par écrit. Il est donc souvent nécessaire de réinitialiser des mots de passe oubliés ou de débloquer des comptes d'utilisateur, ce qui implique une forte sollicitation de l'assistance technique.

Le single sign-on (SSO) est la clé de ce dilemme. Cette solution permet aux salariés du Land de s'authentifier une seule fois afin d'accéder à tous les ordinateurs et applications pour lesquels ils disposent d'une autorisation.

Cette solution centralisée connectée à l'annuaire Active Directory exploite au maximum l'infrastructure informatique existante de l'administration de la Hesse et lui fait en outre bénéficier des caractéristiques de sécurité du SSO.

Solution de single sign-on (SSO) intégrée

HZD a mis en œuvre une solution de single sign-on dans le cadre d'une mission confiée par le gouvernement de la Hesse. Suite à un appel d'offres de grande envergure et à des tests pratiques des principales solutions du marché, le choix s'est porté sur Evidian Enterprise SSO, une solution distribuée par T-Systems, filiale de Deutsche Telekom. Evidian Enterprise SSO s'intègre directement dans la structure informatique du Land de la Hesse et remplit toutes les exigences en matière de sécurité et de prise en charge des applications.

Le mécanisme de SSO se charge d'identifier l'utilisateur. Quand l'utilisateur se connecte aux applications pour lesquelles il dispose d'autorisations, le système ouvre une boîte de dialogue l'invitant à entrer son identifiant et son mot de passe. Une fois ces données fournies, l'utilisateur n'a plus à les mémoriser – le SSO les entrera désormais à sa place.

Le SSO répercute automatiquement toute modification du mot de passe de chaque application. Les mots de passe stockés sont sécurisés, tant au niveau local (pour le fonctionnement hors ligne) que central. Dès lors, l'utilisateur peut se connecter via n'importe quel poste de travail équipé du client de SSO. Les identifiants sont transmis au client de SSO et l'identification est automatique. Le SSO assure intégralement la gestion des mots de passe pour l'ensemble des applications intégrées dans la solution. Toute modification est traitée automatiquement, sans aucune intervention de l'utilisateur.

Amélioration de la sécurité et de la convivialité

• Identifiants et mots de passe réduits au strict minimum

L'accumulation souvent fastidieuse de multiples identifiants et mots de passe qui était la règle jusqu'alors se limite désormais à un identifiant et un mot de passe uniques dans le cadre du SSO. Le salarié se connecte une fois pour toutes via son poste de travail à l'aide des données qui lui ont été attribuées. Chaque connexion ultérieure, effectuée par exemple via le portail des RH, est automatiquement prise en charge par les mécanismes de single sign-on. Les procédures distinctes d'identification ne sont ainsi plus nécessaires.

• Meilleure protection lors des procédures d'autorisation des utilisateurs

Pour travailler sur les applications auxquelles il a accès, l'utilisateur n'a pas d'autres données de connexion à mémoriser que celles de son PC habituel. Les règles centralisées de gestion des mots de passe, qui font cadrer individuellement chaque application avec les mesures générales de sécurité, garantissent une protection contre toute utilisation non autorisée. Ainsi, sans que cela ne soit visible de l'utilisateur, il est possible de définir des mots de passe d'un tel niveau de complexité que leur décryptage par des tiers est pratiquement impossible.

• Diminution de la charge de travail des utilisateurs et des services centraux

Le fait de passer de plusieurs identifiants et mots de passe à une authentification unique simplifie le travail des utilisateurs. Les temps d'accès aux applications sont réduits et la charge de travail de l'assistance technique liée à la réinitialisation des mots de passe et au déblocage des comptes utilisateur diminue considérablement.

« De multiples procédures d'identification avec diverses combinaisons de mots de passe et d'identifiants constituent souvent un poids dans le travail quotidien des fonctionnaires de la Hesse.

Grâce à la solution de SSO d'Evidian, il leur suffit désormais de s'authentifier une seule fois pour accéder à l'ensemble des ordinateurs et services qu'ils sont autorisés à utiliser, sans avoir à s'identifier à chaque fois. En outre, cela implique une amélioration de la sécurité informatique. »

Manfred Pospich,
Responsable du service Planung und
Beschaffung (planification
et approvisionnement),
HZD.