



State of Hesse (Germany)

Profile

- IT service provider for the Hessian state administration.
- 800 employees provide practical solutions.

Users

- 60,000 staff forming part of the Hessian state administration.

Challenges

- Easy and secure access to applications.
- Many different user IDs and passwords.

Benefits

- **Higher security** as each user only needs to remember a single password.
- **More efficient work** through simple interaction between individual applications.
- **Cost savings** through proven reductions of up to 30% in the help desk's workload.

A local government simplifies and secures access.

Facilitating work for the state administration's staff

As IT service provider for the Hessian state administration with locations in Wiesbaden and Hünfeld, HZD operates as a state enterprise under business management. At the core of HZD's activities is a market-oriented IT expertise combined with 40 years of administrative experience and customer-focused solutions ranging from project planning to implementation and operation.

Data processing at the administrative level is meant to serve citizens and businesses, and facilitate the work for the state administration's employees. Especially in these economically difficult times, HZD is committed to make processes more efficient and less costly.

Since 1970, HZD has steadily expanded its competence as an IT service provider for the State of Hesse. In close cooperation with the Hessian state authorities, about 800 dedicated employees develop and implement practical solutions for citizen-oriented administration.

Single sign-on: the way out of a dilemma

Sign-on procedures for a variety of specialized applications complicate Hessian state administration staff' daily tasks at PC workstations. Each such application can have its own user administration system with separate passwords and password rules, making it necessary for users to recall a correspondingly large number of different user IDs and passwords.

The undue burden this places on many people gives rise to high security risks. Many users resort to choosing identical passwords for the various specialized applications, or noting passwords down somewhere. When such measures fail, this often necessitates a reset of forgotten passwords or an unlocking of user accounts, thereby placing a high workload on the help desk.

As a solution to this dilemma, single sign-on (SSO) allows state administration staff, via a sole authentication procedure, to access all computers and specialized applications for which they are authorized.

Linked with Active Directory, this centralized solution optimizes utilization of the Hessian state administration's existing infrastructure and complements it with the security features of SSO.

Integrated, single sign-on

The Hessian state government commissioned HZD to research and implement a single sign-on (SSO) solution. The Evidian Enterprise SSO product offered by T-Systems International was selected after an extensive bidding process and practical tests of leading SSO systems. Evidian Enterprise SSO could be integrated smoothly into Hesse's IT infrastructure and met all requirements for security as well as application support.

The single sign-on mechanism takes over the user identification tasks. First of all, the user must successfully log into Windows to enable a non-recurrent transfer of data relating to the integrated, specialized applications which the user is authorized to access. After that, the system provides a dialog instructing the user to enter their passwords. From then on, the user no longer needs to remember these passwords.

The SSO module performs all password changes automatically in accordance with the guidelines prescribed for the specialized applications. The passwords are stored securely in encrypted form. This is done both locally (for offline operation) and centrally. Regardless of the workstation at which the user signs on via an SSO client, the related passwords are then relayed to this client for the purpose of automatic authentication.

From then on, the SSO client performs the entire password management for the integrated, specialized applications. Changes to any of these applications are processed automatically without the need for any user intervention.

Improved security and comfort

• Minimizing user IDs and passwords

The often tedious management of diverse user IDs and passwords is minimized by SSO to use of a single user ID and password. State administration staff simply need to log into the system at their respective workplace using their personal identification. Any further authentication, for instance, at the employee portal, is automatically performed by single sign-on mechanisms. This eliminates the need for separate sign-on by the user again.

• Increased security during user authorization

The user does not need to remember any further IDs or passwords to access authorized applications following regular sign-on at the workplace. Central password rules compliant with general security standards for each individual, specialized application guarantee protection against misuse. Unnoticeable to the user, password complexity can be increased - exclusively at the system end - to a level at which it becomes practically impossible for third parties to crack passwords.

• Lower burden on users and central services

Reducing diverse collections of user IDs and passwords to realize a single sign-on procedure facilitates work for users, shortens the time required to access specialized applications, and significantly relieves the help desk with regard to unlocking user accounts and resetting passwords.

"Multiple login procedures with different user name / password combinations often complicate the everyday work of state employees.

With the SSO solution, Hessian state administration staff can use a single authentication procedure to access all computers and services for which they are authorized, without having to sign-on again each time. This also increases IT security."

Manfred Pospich,
Head of Planning and Procurement,
HZD.