ins Multi-Factor-ID

Authentication through comparison of "knowledge" and "possession".

Simple and secure.

Via app or token.

Static passwords alone do not provide sufficient security to protect your IT infrastructure from unwanted access. Whereas the two-factor authentication with INS's multi-factor ID is the simple and safe solution. In the course of the login to your systems you will utilize not only a static password, but also a combination of a PIN ("knowledge", 1st factor) and a constantly changing code ("possession", 2nd factor), which is displayed on a separate device (app or token).

ins Multi-Factor-ID offers you i.a.:

- Supports all common 2FA apps (IOS, Android)
- Connection e.g. via **Windows Credential Provider**, Radius and Netscaler
- Extremely low downtimes thanks to **high availability (99.8%)** and load balancing
- Hosting in a German Tier 3+ data centre
- Utilization as a **self-service** or **Managed Service**
- **Pay per use**: monthly. license price per user
- Availability of **inexpensive hardware tokens**
- Secure transmission via HTTPS

The German Federal Office for Information Security (BSI) strongly recommends a two-factor authentication, particularly for security-critical areas of application, but also for web-based services.

We would be happy to present ins Multi-Factor-ID to you in detail, which represents a cost-effective and secure alternative to solutions such as RSA.

How it works:

When accessing a protected resource, such as a web user interface or the Windows login, the user is prompted for the passcode. The passcode is based on two components: the PIN, which was generated by the multi-factor ID system during the setup, and the code, which is generated by the user's authentication app or token. The token generator generates a new security token in the form of a six-digit number every 30 seconds. The corresponding host, whose access is secured with this token, generates a matching number according to the same algorithm. Our MFID system calculates which number the token should display at the current time, compares it with the information provided by the user, and decides whether to allow or deny access to the system.

Make an appointment for a free and noncommittal initial consultation, during which we will discuss your specific requirements and show you the various options.

Certified security that you can rely on:
INS is certified according to **ISO 9001:2015** and **ISO/IEC 27001:2013**.