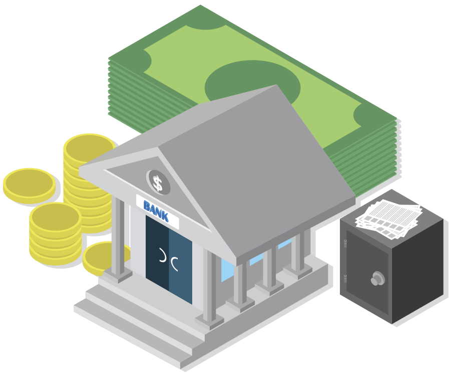
PASSWORD SAFE

IT-Security in the financial sector

In recent years, the risk of cybe -attacks on the economy and thus also on the financial sector has increased significantly. The reasons for this are obvious. On the one hand, the digitalisation of our economy and the increasing networking of companies, which creates new gateways for hackers. On the other hand, attackers are finding ever new, more professional ways to attack companies. It is therefore not surprising that cyber attacks are currently considered the greatest operational risk for the financial sector.



In order to optimise IT security in critical infrastructures in particular, BaFin (Federal Financial Supervisory Authority) laid down the minimum requirements for risk management (MaRisk) for banks in a circular as early as 2006. Banks and other financial institutions must therefore comply with standards such as BaFin according to AT 4.3.1 Tz.2, AT 7.2 Tz, ISO 27001, MaRisk according to BTO Tz. 9, SOX, PCI Standard, BAIT and FINMA. Institutions should ensure a minimum level of security and thus be protected from cyberattacks and the resulting negative consequences. Password Safe helps your company to fulfil security-relevant requirements and at the same time to noticeably increase the security of the access data.

> **Optimise IT security in your company now. Company-wide secure passwords are one of the best ways to prevent cyber attacks. Work with the market leader in password management - we have the expertise to secure your institution against cyber attacks!**

Large financial service providers are also required by law to store sensitive data in a secure environment. Password Safe is self-hosted exclusively on the company's own servers. Compared to SaaS solutions and storing data in a public cloud, local hosting in the company has the advantage that all information is stored in a legally secure manner at the company's location, for example in Germany, and the servers are less likely to be the target of hacker attacks compared to large cloud providers.

Play it safe

Especially in the financial sector, with an estimated three times more cyber attacks than in other economic sectors, high password protection is enormously important. In large companies, the problem of securing all accesses, passwords and apps arises simply because of the large number of employees. If employees protect their login with „Neumann1964!“, hackers have an easy time cracking passwords.

To protect banks, BaFin regularly publishes a catalogue of IT requirements. Password Safe offers numerous features to increase information security and meet the requirements of BaFin.

BaFin: „Measures such as the guidelines for choosing secure passwords should prevent the circumvention of the specifications of the authorisation concepts.“

With Password Safe, „Neumann1964!“ is a thing of the past: employees can log in automatically in seconds – without even knowing the password, as all passwords are securely managed in the software. A password generator is available for creating secure passwords: with just one click, complex passwords can be generated that hackers can‘t get their teeth into. In addition, IT can create individual password policies that offer protection against passwords that are too easy. With the Password Reset function, passwords can be automatically replaced by IT based on events or time.

Intelligent and secure solutions for financial institutions

Password Safe supports you with a password management solution individually tailored to your company, no matter for one branch or multiple locations. Regardless of whether you are dealing with branched authorisation structures at banks or central password management at other financial institutions: Trust our many years of experience in the IT security industry!

Securing processes through multiple eyes

The multiple-eyes principle is the order of the day in the financial industry. Activities or processes are approved by at least two people, which safeguards against manipulation and misuse. Why not apply this principle to the handling of passwords?

BaFin: „Changes [...] of authorisations [...] must be documented in a comprehensible and evaluable manner.“

The seal function integrated in Password Safe ensures that access to a password must first be approved by one or more roles. Only after approval has been granted can people access passwords and accounts. If passwords are combined with additional privacy protection, employees can only use the passwords in encrypted form to log in, but cannot see them in plain text. This way, passwords remain secure even in the event of espionage and social engineering attacks. Moreover, when employees leave the company, passwords of shared accounts do not have to be exchanged.

All actions and approvals in Password Safe are also documented, stored in the logbook in an audit-proof manner and can be exported in the form of reports. This ensures a high level of password protection and traceability for audits.

Securely guarantee access to passwords from everywhere

In banks, customer service representatives work at different terminals, often have to change their location and log into the system again each time. In addition, they often work at various locations at home and abroad. Since financial institutions in particular are closely networked digitally, security cannot be thought of locally from branch to branch.

The scalable architecture of Password Safe enables secure and fast access to access data in Password Safe from any location. By connecting multiple servers, performance remains consistently good. In the event of a failure, data remains secure through SQL clustering and cluster replication.

Log in quickly and securely

For more security when logging in to Password Safe, a second factor can be added. In this way, each individual login is doubly secured and the identity can be ensured beyond doubt by means of a smart card or the query of biometric features. At the same time, Password Safe as an identity provider also enables passwordless login to applications. The login to Password Safe itself can thus take place without a password by combining a master password with a FIDO-2-compliant token or a smartcard.

Trust is good – security is better

A frequent gateway for cyber criminals is the employee himself, who either maliciously or in ignorance endangers the security of the entire company. In order to keep the risk as low as possible, employees should only have access to data that they absolutely need for their work, in accordance with the least-knowledge principle.

BaFin: „The authorisation concept should work according to the economy concept.“

Password Safe is based on this security approach: employees only have access to the data, accounts and passwords that are absolutely necessary for efficient work. Rights are granted to specific groups of employees on a role-based basis (RBAC) and can be withdrawn just as easily.

A holistic approach to security

An insecure password or a password written on a Post-it is enough to give hackers access to company secrets. Especially in the financial sector, it is extremely important that employees can use and manage secure passwords across all devices and applications.

With Password Safe, the management and secure handling of access data can be ensured regardless of the size of the financial institution and the associated number of licences. Password Safe reduces the risk of cyberattacks through complex passwords and secured access. Invest in comprehensive password protection today and secure tomorrow‘s customers.

Feel free to contact us and have us advise you why Password Safe is your right solution!

Why Password Safe?

Experience

MATESO has focused on professional enterprise password management since **2006**. Over **21 of the top 40 DAX companies** and more than **10,000 users** already rely on Password Safe for password protection.

Comprehensive protection

With the influence of over **20 years of market experience**, the solution is holistically tailored to the individual security requirements and needs of companies. All passwords are protected holistically throughout the **password lifecycle** - from creation to archiving.

Made in Germany

As a member of the TeleTrust initiative **„IT-Security Made in Germany“**, MATESO stands for trustworthy IT security solutions that meet the requirements of German data protection law, can be used in **compliance with the DSGVO** and do not contain any hidden accesses.

MATESO GmbH
Daimlerstraße 15, D-86356 Neusäß
Web: www.passwordsafe.com
E-mail: sales@passwordsafe.de
Tel: +49 821 74 77 87-0

MATESO
PASSWORD SAFE