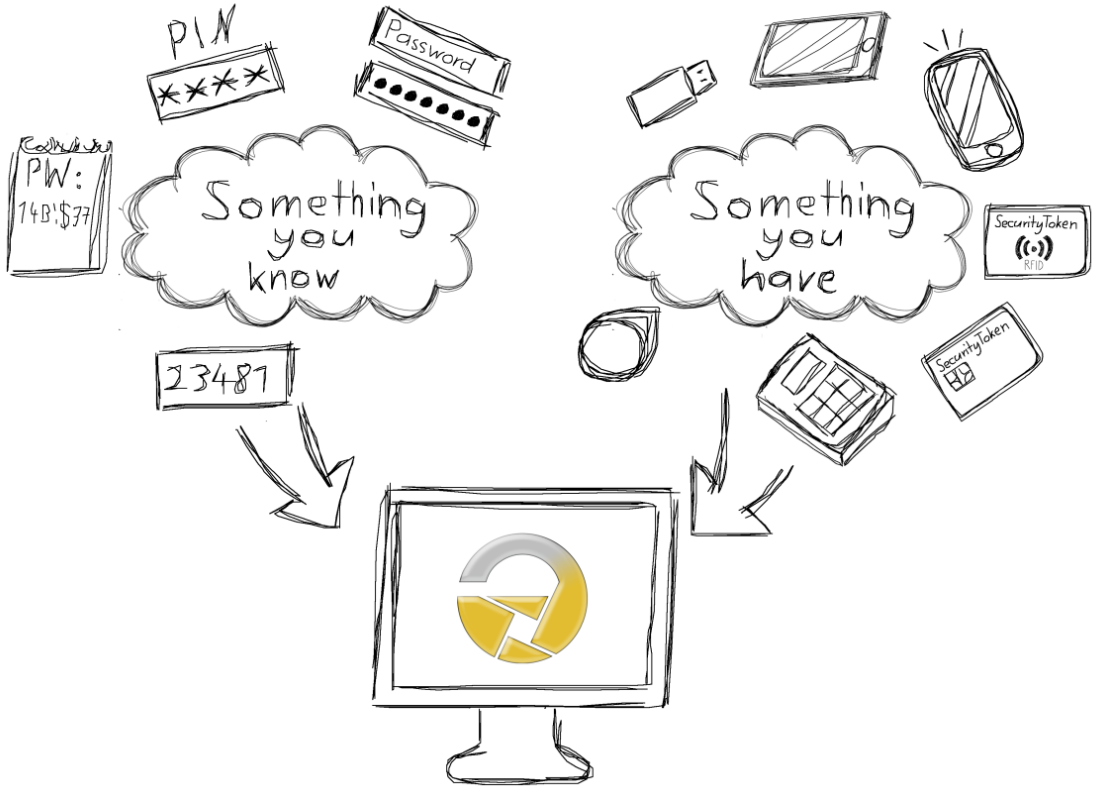
2-Factor-Authentication

Our contribution to protecting your sensitive data

digitronic®.net

SmartLogon™



- ☑ *modern: 2-factor-authentication, with or without PKI*
- ☑ *secure: knowledge (PIN) and possession (certified Token) required*
- ☑ *simple: quick implementation, also in large environments*
- ☑ *convenient: can be managed centrally (via ADMX-file)*
- ☑ *flexible: integration of the Tokens also possible in other systems*
- ☑ *innovative: log-on with Smartphone**

www.digitronic.net ***vertrieb@digitronic.net***

The challenge

Logging onto an IT-system by using a password suffers from its own divergent requirements: on the one hand a high-level of complexity for the password (secret) is necessary so that it can't be found out through simple spying techniques; on the other hand, that level of complexity cannot be so high that the user is unable to remember his or her own password. Since security is most often given the highest priority, complex password policies lead to the infamous scribbled note hidden under the keyboard or to extremely time-consuming support efforts on the part of the administrators, due to the work involved in re-setting forgotten passwords or those that were incorrectly typed in several times over.

The solution

The solution to this is a 2-factor-authentication (2FA), in which a highly complex secret is stored on a secure Token and unblocked by typing in a simpler PIN. The high level of security is a result of the fact that now 2 factors are necessary for successful authentication: the secure Token with the secret (possession) and the PIN (knowledge) required for unblocking.

The product

SmartLogon™ enables access to local and network resources in the Windows environment by way of a Security Token and a PIN.

For the client-based software neither a central server component nor a complex Public-Key-Infrastructure is necessary. The software contains a Credential Provider that is integrated seamlessly into the Windows operating system, making the 2FA possible.

Specially developed for the SmartLogon™, the digitronic® Token Engine, with its modular construction, is built on an extremely flexible architecture and, by way of an EPI for example, enables access to different types of Tokens.

Service features

Several identities can be stored on the Security Token and transferred onto a target system.

Despite the decentralized and independent solution, existing security policies are maintained. With SmartLogon™ aging passwords and/or PINs as well as the policies regarding their complexity are supported in full - this includes passive RFID Tokens.

This solution also raises the level of security and convenience: by removing the Security Token either the PC can be blocked or, via an adjustable countdown, the user can be deregistered. Unlocking your KeePass database is also very easy ("KeePass ready").

SmartLogon™ can be centrally rolled out via software distribution (msi-Pakete) and can be administrated using group guidelines (via ADMX-file).

Integration into other systems/ adjustments

A particular strength of SmartLogon™ lies in the high level of integrability into other systems, such as time recording or access controls. Our Security Tokens are compatible with these systems in most cases.

Moreover, our solution is suitable for a personalized start of certain programs, for example. We would be happy to make modifications to implement your needs.

Put our expertise to work for you!

TECHNICAL DETAILS

Operating systems

Windows 7, 8, 8.1, 10

Security Token

☑ digitronic® USB SecurityToken with Java Card OS (EAL5+-certified)
☑ Mifare DESFire EV1 (EAL4+), MIFARE DESFire EV2 (EAL5+)
☑ further Security Tokens such as IBM/NXP, Giesecke & Devrient, Gemalto, Oberthur or with operating systems such as STARCOS, Multos, TCOS and CardOS upon request and/or without support
☑ Android Smartphone*

Standards PKCS #11, RFID native

Card readers

☑ RFID-based (in accordance with ISO/IEC 14443) and contact-based card readers, such as ReinerSCT cyberJack RFID basis, ReinerSCT cyberJack RFID Komfort, Cherry TC 1200 und Identity CLOUD 3700F

PIN-complexity

☑ Alphanumerical PIN and PUK
☑ Up to 4 criteria (upper-/lowercase letters, numbers, etc.)
☑ Complexity check against a dictionary
☑ Determining the minimum and maximum PIN length
☑ Delta check to existing PIN and PUK

*available as a prototype

Short portrait and further services

The digitronic® computersysteme gmbh, with headquarters in Chemnitz, has been creating IT solutions in the fields of communication, IT-security and digital confidentiality since 1991. With a clear focus on reliability, customer-friendly service and functionality we create, among other things, innovative solutions for strengthening the confidentiality of sensitive data.

Our **All-In-One-Security Packages** with their enclosed 2FA solutions as well as the encryption of sensitive data on network drives HiCrypt™ Professional fulfill the corresponding requirements in tests and audits of information security in accordance with VDA ISA (TISAX), ISO 27001 and the criteria for critical infrastructures. Additionally, you can select those services offered in the packages that best support you in implementing your projects.

Your point of contact

digitronic® computersysteme gmbh
Oberfrohnaer Str. 62
09117 Chemnitz

Tel.: +49 371 81539 0
Fax: +49 371 81539900
E-Mail: vertrieb@digitronic.net
Web: www.digitronic.net