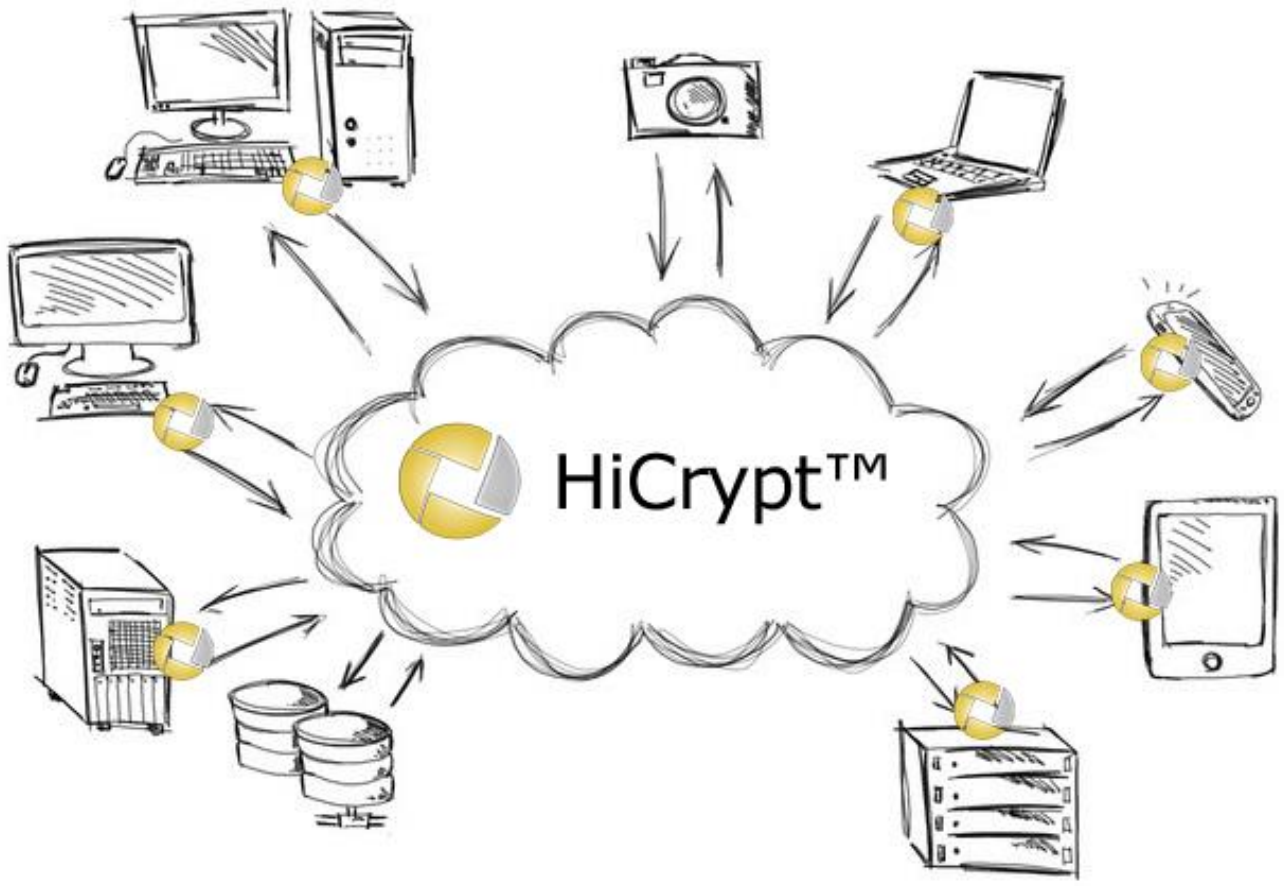
Network encryption –
Secure your sensitive data!

digitronic®
.net

HiCrypt™ Professional



- ☑ *transparent:* *without expansion of infrastructure*
- ☑ *individual:* *separate keys for every drive*
- ☑ *easy:* *to integrate – on just one or on up to thousands of workspaces*
- ☑ *comfortable:* *intuitive use and central administration*
- ☑ *secure:* *state-of-the-art technology*
- ☑ *impermeable:* *optionally with two-factor authentication*

Test now: https://www.digitronic.net/en/download-hicrypt

Challenge

The access to sensitive data is often only handled via existing authorisation concepts. However, external service providers, the administrators of said authorisation concepts and attackers who impersonate those administrators can get access to this sensitive data as well, even if the data was encrypted.

Solution

The solution to this problem is the encryption of sensitive data in combination with a user administration that is separate from the existing authorisation concept, which helps to regulate the access to the sensitive data. With this separation, administrators are freed from the suspicion of willingly or unwillingly accessing sensitive data. Authorised users, on the other hand, are able to work with the encrypted data as they are used to. This way, the necessary acceptance of the solution by the user can be achieved.

Product

With HiCrypt™ Professional, the access key to sensitive data is back in the hands of the people who are responsible for its confidentiality. IT administrators provide the infrastructure, yet they do not give out the keys.

HiCrypt™ Professional combines this guarantee of owning the only key with a comfortable use, ingenious simplicity and a flexible adaptation to your protection needs.

To increase security, HiCrypt™ Professional supports the authentication of authorised users on the encrypted network drive with the help of a two-factor authentication (2FA). The modular structure of the used digitronic® Token Engine supports the access to different types of tokens.

HiCrypt™ Professional is available as a standard license, for terminal servers (desktop-as-a-service, software-as-a-service) as well as in the form of a floating license.

Scope of Services

With HiCrypt™ Professional, you can encrypt several network drives and thus set up confidentiality limits between the data of different departments (such as research and personnel) or between different projects.

You can define individual password directives for the 2FA, to enforce frequently requested security guidelines for passwords and PINs with HiCrypt™ Professional. Various criteria of a password, such as its length, complexity and period of validity can be adjusted in a flexible manner.

HiCrypt™ Professional is a client software, but integral functions are supported nevertheless. The software is of course compatible with software distribution systems. Administrators can initialise encrypted network drives, and the people who are responsible for the data then must simply create the authorised users, which they can choose from existing active directory groups. Overviews of encrypted network drives and authorised users always inform you about the status quo.

Integration/ Adjustment

One token, several functions: The SecurityTokens that are used for the 2FA are most often compatible with other systems like time tracking or access control.

As the producer, we will gladly work with you on adjustments that implement your specific requirements.

Guarantee

Software and support "Made in Germany" guarantees: No access to your sensitive data through loopholes and very short reaction times if you need assistance.

Take advantage of our know-how!

TECHNICAL DETAILS

HiCrypt™ Professional

Operating systems:	as of Windows 7/Server2008 R2
Filesharing protocols:	CIFS/SMB
Requirement:	Microsoft .net Framework 4.6
Encryption algortihms:	AES, Blowfish, IDEA
Download:	www.hicrypt.com/download
Free test period:	30 Tage

SecurityToken

SmartCard:	active (JCOP, CardOS, etc.), passive, native (DESFire, Legic, et al)
Standards:	PKCS#11
Smart Chip certifications:	min. EAL 4+, EMV, ISO 7816
Electronic certification:	FCC, CE, RWTÜV

As a replacement compatible with:

Crypted Group Share (cgs)
SecurStar ShareCypt Version 3

CITRIX® Ready

Short profile and additional offers

Since 1991, Chemnitz-based digitronic® computersysteme gmbh has implemented IT solutions in the fields of communication, IT security and digital confidentiality. With a clear focus on reliability, customer-friendly service and functionality, we are constantly working on innovative solutions to strengthen the confidentiality of sensitive data.

Our **All-In-One security packages**, including the two solutions of encrypting sensitive data on network drives and the secure and comfortable login (SmartLogon™), meet the requirements of assessments and audits in regard to their information security according to VDA ISA (TISAX), ISO 27001 as well as the criteria for critical infrastructures. Additionally, you can choose the services with which we can best support you during the implementation of your projects from a wide range of offers in these packages.

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

digitronic® .net