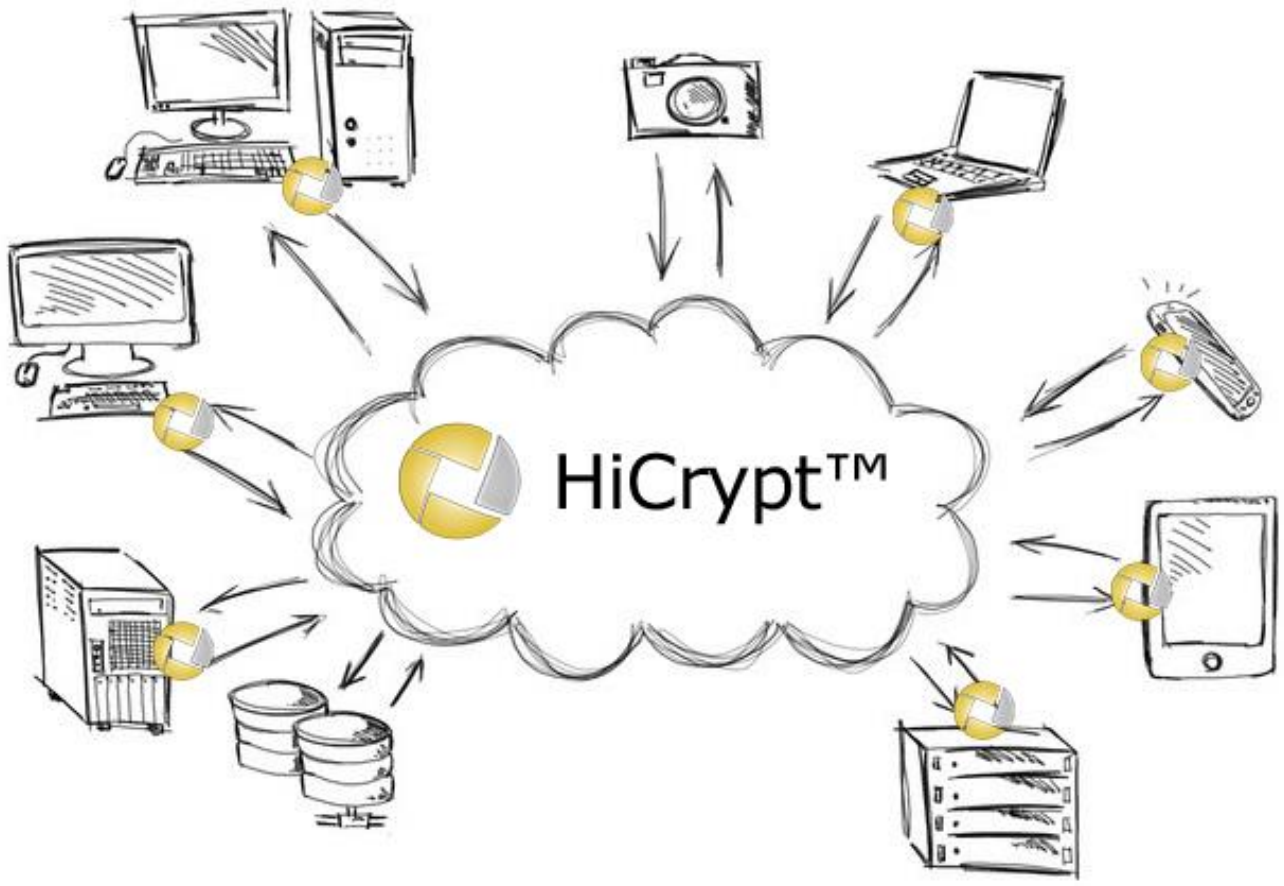
**Verschlüsselung von Netzlaufwerken**

digitronic®.net

# HiCrypt™ Professional




- ☑ *transparent: ohne Ausbau der Infrastruktur*
- ☑ *individuell: separate Schlüssel für jedes Laufwerk*
- ☑ *einfach: zu integrieren – 1 bis 1000e Arbeitsplätze*
- ☑ *komfortabel: intuitiv zu bedienen und zentral zu verwalten*
- ☑ *sicher: Technologie state of the art*
- ☑ *wasserdicht: optional mit 2-Faktor-Authentifizierung*

***www.digitronic.net*** ***vetrieb@digitronic.net***

### *Herausforderung*

Der Zugriff auf vertrauliche Daten wird oft allein über bestehende Berechtigungskonzepte geregelt. Damit können jedoch auch externe Dienstleister, die Verwalter der Berechtigungskonzepte und Angreifer, die in die Rolle dieser Verwalter schlüpfen, Zugang zu hochsensiblen Daten erlangen, mitunter selbst dann, wenn die Daten verschlüsselt wurden.

### *Lösung*

Die Lösung bietet eine Verschlüsselung vertraulicher Daten in Verbindung mit einer vom bestehenden Berechtigungskonzept unabhängigen Benutzerverwaltung, mit deren Hilfe der Zugriff auf die verschlüsselten Daten geregelt wird. Diese Trennung ermöglicht es, z. B. Administratoren von dem Verdacht zu befreien, unwissentlich oder wissentlich auf vertrauliche Daten zuzugreifen. Berechtigte Nutzer können dagegen mit den verschlüsselten Daten in gewohnter Weise arbeiten, um die erforderliche hohe Akzeptanz der Lösung auch bei den Nutzern zu erreichen.

### *Produkt*

Mit HiCrypt™ Professional halten wieder diejenigen den Schlüssel für den Zugang zu sensiblen Daten in der Hand, die für deren Vertraulichkeit tatsächlich verantwortlich sind. IT-Administratoren stellen die Infrastruktur bereit, vergeben jedoch nicht die Schlüssel. Die Lösung verbindet diese „Schlüssel-Alleinbesitzgarantie" mit komfortabler Nutzbarkeit, genialer Einfachheit und flexibler Anpassung an Ihren Schutzbedarf.

Zur Steigerung der Sicherheit unterstützt HiCrypt™ Professional eine Authentifizierung berechtigter Nutzer am verschlüsselten Netzlaufwerk mit Hilfe einer 2-Faktor-Authentifizierung (2FA). Der modulare Aufbau der dafür verwendeten digitronic® Token Engine unterstützt den Zugriff auf unterschiedliche Arten von Token.

HiCrypt™ Professional ist sowohl als Standardlizensierung, für Terminalserver (Desktop-as-a-Service, Software-as-a-Service), als auch als Floating Licence erhältlich.

### *Leistungsumfang*

Mit HiCrypt™ Professional können Sie mehrere Netzlaufwerke verschlüsseln und so Vertraulichkeitsgrenzen z. B. zwischen den Daten verschiedener Abteilungen (wie Forschung und Personal) oder zwischen unterschiedlichen Projekten ziehen.

Für die 2FA sind individuelle Kennwortrichtlinien definierbar, um häufig geforderte Sicherheitsrichtlinien für Kennworte und PINs auch mit HiCrypt™ Professional durchzusetzen. Diverse Kriterien eines Kennworts, wie Länge, Komplexität und Gültigkeitsdauer, können flexibel eingestellt werden.

HiCrypt™ Professional ist eine Client-Software, zentrale Funktionen werden trotzdem unterstützt. Die Software ist selbstverständlich kompatibel zu Softwareverteilungssystemen. Administratoren können verschlüsselte Netzlaufwerke initialisieren, die für die Daten Verantwortlichen müssen dann nur noch die berechtigten Nutzer anlegen und können diese aus bestehenden Active-Directory-Gruppen auswählen. Übersichten über verschlüsselte Netzlaufwerke und berechtigte Benutzer informieren jederzeit über den Status quo.

### *Integration/ Anpassung*

Ein Token, mehrere Funktionen: Die für die 2FA verwendeten SecurityToken sind in den meisten Fällen zu anderen Systemen, wie Zeiterfassung oder Zugangskontrolle, kompatibel.

Als Hersteller entwickeln wir gern gemeinsam mit Ihnen Anpassungen, die Ihre spezifischen Anforderungen umsetzen.

### *Garantie*

Software und Support „Made in Germany" garantieren Ihnen: Kein Zugriff auf Ihre vertraulichen Daten durch eine Hintertür und kürzeste Reaktionszeiten, wenn Sie unsere Unterstützung benötigen.

# *TECHNISCHE DETAILS*

### *HiCrypt™ Professional*

| | |
|---|---|
| Betriebssysteme: | ab Windows 7/Server2008 R2 |
| Filesharing Protokolle: | CIFS/SMB |
| Voraussetzung: | Microsoft .net Framework 4.6 |
| Verschlüsselungsalgorithmen: | AES, Blowfish, IDEA |
| Download: | www.hicrypt.com/download |
| Kostenfreier Testzeitraum: | 30 Tage |

### *SecurityToken*

| | |
|---|---|
| SmartCard: | aktiv (JCOP, CardOS, etc.), passiv, nativ (DESFire, Legic, u.a.) |
| Standards: | PKCS#11 |
| Smart Chip Zertifizierungen: | min. EAL 4+, EMV, ISO 7816 |
| Elektrische Zertifizierung: | FCC, CE, RWTÜV |

### *Als Ablösung kompatibel zu:*

Crypted Group Share (cgs)
SecurStar ShareCypt Version 3

CITRIX® Ready

## *Kurzportrait und weitergehende Angebote*

Die digitronic® computersysteme gmbh mit Sitz in Chemnitz realisiert seit 1991 IT-Lösungen auf den Gebieten Kommunikation, IT-Sicherheit und digitale Vertraulichkeit. Mit einem klaren Fokus auf Zuverlässigkeit, Kundenfreundlichkeit und Funktionalität erarbeiten wir u.a. innovative Lösungen zur Stärkung der Vertraulichkeit schützenswerter Daten.

Unsere **All-In-One-Sicherheitspakete** erfüllen mit den beiden beinhalteten Lösungen Verschlüsselung sensibler Daten auf Netzlaufwerken und sichere und komfortable Anmeldung (Secure Logon™ 2.0) die Anforderungen von Prüfungen und Audits der Informationssicherheit nach VDA ISA (TISAX), ISO 27001 sowie Kriterien für kritische Infrastrukturen. Zudem können Sie in diesen Paketen aus verschiedenen Dienstleistungsangeboten diejenigen auswählen, mit denen wir Sie bei der Umsetzung Ihrer Projekte am besten unterstützen.

## *Kontakt*

**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