Das Leben nach TrueCrypt - Alternativen

Edgar 'Fast Edi' Hoffmann

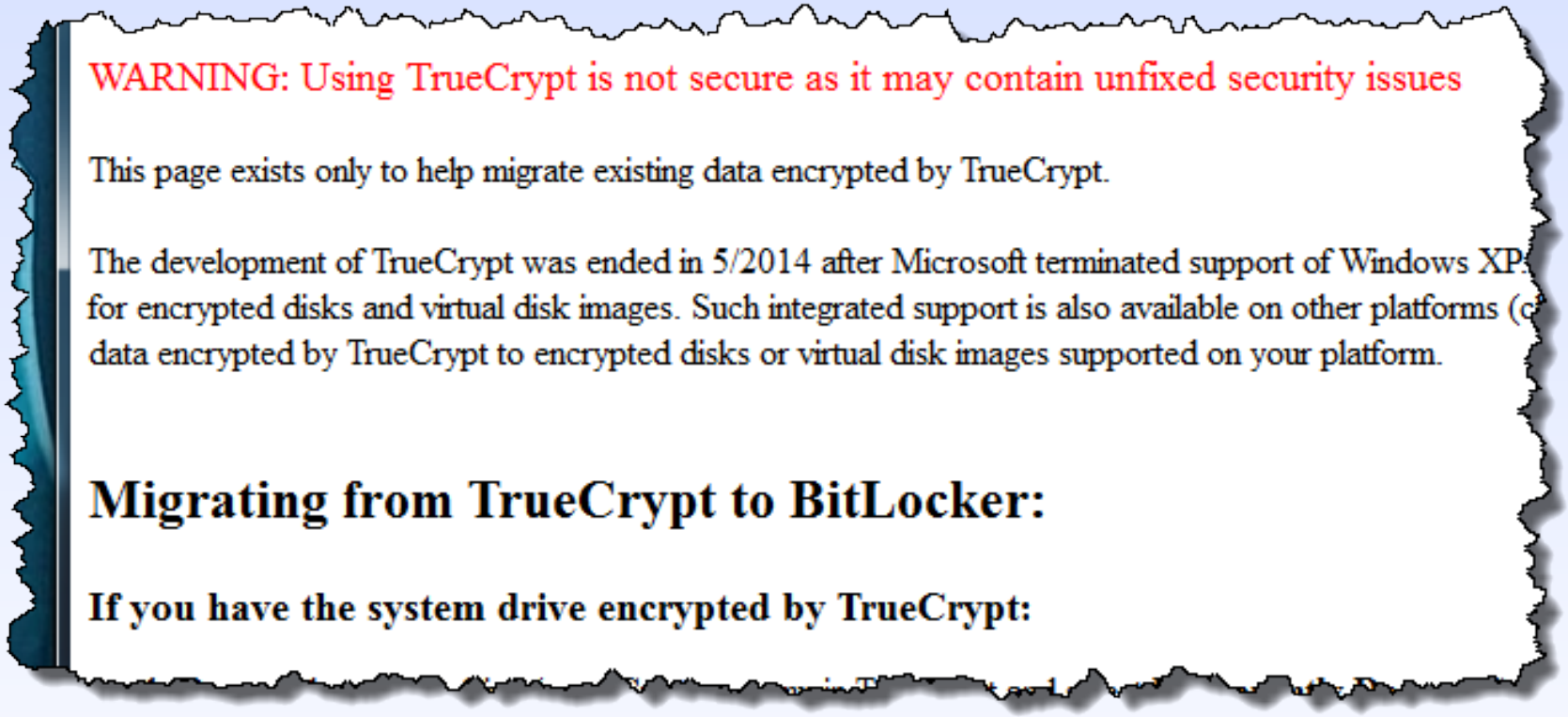
Community FreieSoftwareOG

kontakt@freiesoftwareog.org

1. Oktober 2014

TrueCrypt
Die X-Akte...

TrueCrypt
Die X-Akte...



WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues

This page exists only to help migrate existing data encrypted by TrueCrypt.

The development of TrueCrypt was ended in 5/2014 after Microsoft terminated support of Windows XP. for encrypted disks and virtual disk images. Such integrated support is also available on other platforms (e data encrypted by TrueCrypt to encrypted disks or virtual disk images supported on your platform.

Migrating from TrueCrypt to BitLocker:

If you have the system drive encrypted by TrueCrypt:

FreieSoftwareOG.org

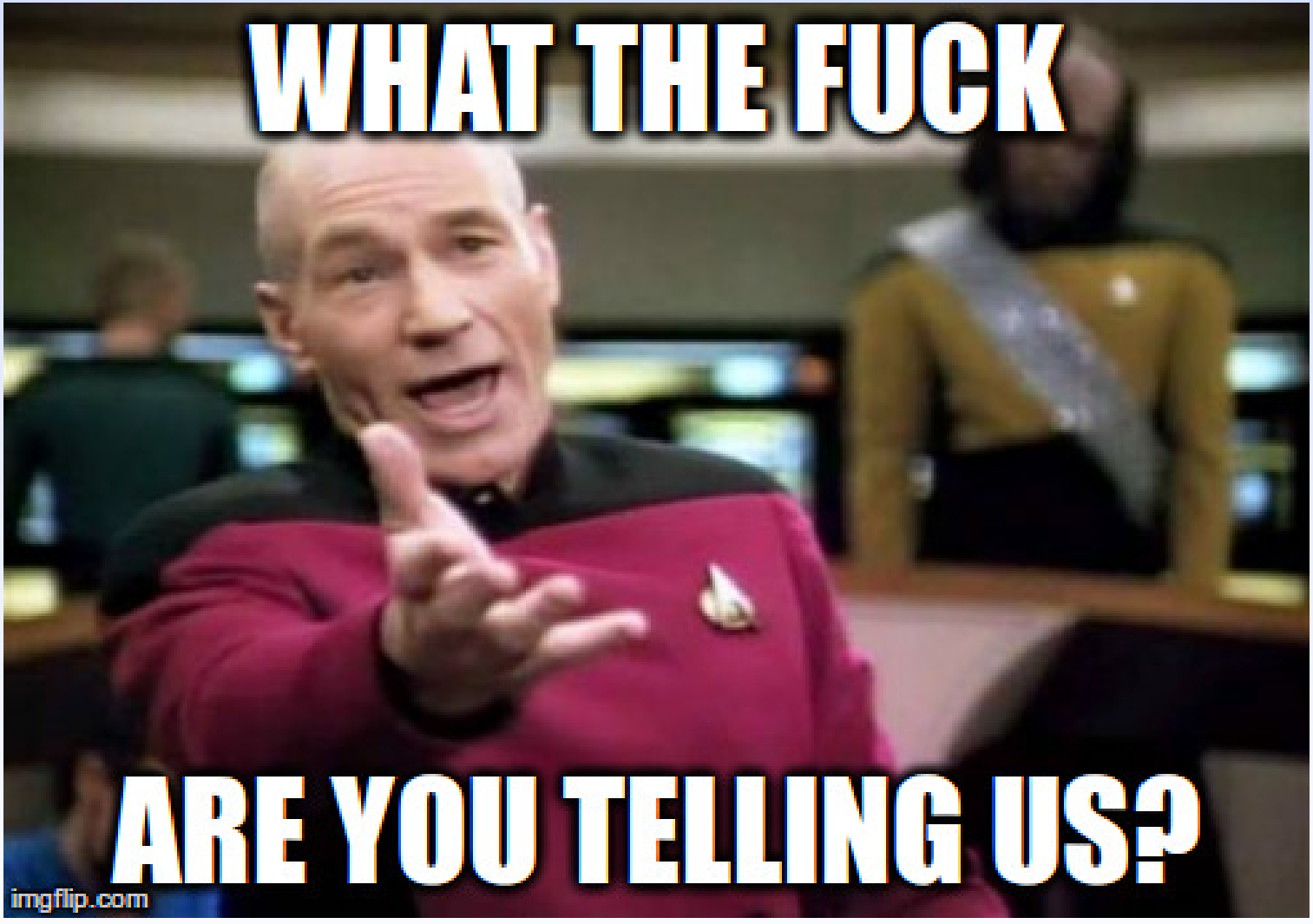
TrueCrypt
Die X-Akte...

TrueCrypt
Die X-Akte...

Als Ende Mai die (anonymen) Entwickler des populären Verschlüsselungsprogrammes TrueCrypt bekannt gaben, es sei nicht mehr sicher, das Tool zu verwenden, war die Community gleichsam Überrascht als auch vor den Kopf gestossen...

TrueCrypt
Die X-Akte...

TrueCrypt
Die X-Akte...



FreieSoftwareOG.org

TrueCrypt
Stand der Dinge

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von
„Sie hatten wohl einfach keine Lust mehr“

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von
„Sie hatten wohl einfach keine Lust mehr“
über

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von
„Sie hatten wohl einfach keine Lust mehr“
über
„Das Projekt ist tatsächlich unsicher“

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von
„Sie hatten wohl einfach keine Lust mehr“
über
„Das Projekt ist tatsächlich unsicher“
bis hin zu

TrueCrypt
Stand der Dinge

Naturgemäß gab es (zum Teil sehr wilde) Spekulationen über die Beweggründe der TrueCrypt-Entwickler.
Diese reichten von
„Sie hatten wohl einfach keine Lust mehr“
über
„Das Projekt ist tatsächlich unsicher“
bis hin zu
„Die NSA zwang sie dazu“

TrueCrypt
Stand der Dinge

TrueCrypt
Stand der Dinge

Fakt ist: Momentan weiss es niemand.

TrueCrypt
Stand der Dinge

Fakt ist: Momentan weiss es niemand.
Es gibt allerdings Hoffnung!

TCnext
TrueCrypt lebt!

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt.

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt.
Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt. Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder
Unter dem Namen TCnext wird emsig daran gearbeitet, den Nutzern bald wieder eine sichere und verlässliche Möglichkeit der Verschlüsselung zu geben.

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt. Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder
Unter dem Namen TCnext wird emsig daran gearbeitet, den Nutzern bald wieder eine sichere und verlässliche Möglichkeit der Verschlüsselung zu geben.

- Hosting in der Schweiz

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt. Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder
Unter dem Namen TCnext wird emsig daran gearbeitet, den Nutzern bald wieder eine sichere und verlässliche Möglichkeit der Verschlüsselung zu geben.

- Hosting in der Schweiz
- Keine anonymen Entwickler für ein sicherheitsrelevantes Projekt

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt. Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder
Unter dem Namen TCnext wird emsig daran gearbeitet, den Nutzern bald wieder eine sichere und verlässliche Möglichkeit der Verschlüsselung zu geben.

- Hosting in der Schweiz
- Keine anonymen Entwickler für ein sicherheitsrelevantes Projekt
- TrueCrypt-Sourcecode liegt auf GitHub (`https://github.com/FreeApophis/TrueCrypt`)

FreieSoftwareOG.org

TCnext
TrueCrypt lebt!

Zur Zeit gibt es eine schweizer Initiative, welche das Projekt weiterverfolgt. Massgeblich beteiligt sind hier: Thomas Bruderer und Jos Doekbrijder
Unter dem Namen TCnext wird emsig daran gearbeitet, den Nutzern bald wieder eine sichere und verlässliche Möglichkeit der Verschlüsselung zu geben.

- Hosting in der Schweiz
- Keine anonymen Entwickler für ein sicherheitsrelevantes Projekt
- TrueCrypt-Sourcecode liegt auf GitHub (`https://github.com/FreeApophis/TrueCrypt`)
- Download von TrueCrypt 7.1a wird bereitgestellt

FreieSoftwareOG.org

TrueCrypt Alternativen

TrueCrypt Alternativen

- TCnext ("Coming soon")

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG
- luksus / tcplay

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG
- luksus / tcplay
- realcrypt

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG
- luksus / tcplay
- realcrypt
- ecryptfs

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG
- luksus / tcplay
- realcrypt
- ecryptfs
- dm-crypt + LUKS

TrueCrypt Alternativen

- TCnext ("Coming soon")
- VeraCrypt
- DiskCryptor
- TruPax
- EncFS
- GnuPG
- luksus / tcplay
- realcrypt
- ecryptfs
- dm-crypt + LUKS
- Containerdatei im „Eigenbau“

VeraCrypt

VeraCrypt

VeraCrypt ist eine Verschlüsselungssoftware, basierend auf TrueCrypt.

VeraCrypt

VeraCrypt ist eine Verschlüsselungssoftware, basierend auf TrueCrypt. Durch diverse Anpassungen (z.B. erweiterte Verschlüsselungsalgorhytmen) ist es jedoch zum TrueCrypt-Format inkomaptibel!

VeraCrypt Features

VeraCrypt Features

- Verfügbar für Windows, Linux, MacOS

VeraCrypt Features

- Verfügbar für Windows, Linux, MacOS
- Unterstützte Verschlüsselung: AES-256

VeraCrypt
Features

- Verfügbar für Windows, Linux, MacOS
- Unterstützte Verschlüsselung: AES-256
- Verschlüsselungsschicht: Volumes/Container

VeraCrypt
Features

- Verfügbar für Windows, Linux, MacOS
- Unterstützte Verschlüsselung: AES-256
- Verschlüsselungsschicht: Volumes/Container
- Lizenz: Ms-PL

DiskCryptor

DiskCryptor

DiskCryptor ist eine offene Verschlüsselungslösung, mit der alle Festplattenpartitionen (inkl. der Systempartition) verschlüsselt werden können.

DiskCryptor

DiskCryptor ist eine offene Verschlüsselungslösung, mit der alle Festplattenpartitionen (inkl. der Systempartition) verschlüsselt werden können.
DiskCryptor war von Version 0.1 bis 0.4 kompatibel mit TrueCrypt, wurde aber danach auf ein eigenes Partitionsformat umgestellt, da das TrueCrypt Format ursprünglich zur Erzeugung von leeren Volumes ausgelegt war.

DiskCryptor

DiskCryptor ist eine offene Verschlüsselungslösung, mit der alle Festplattenpartitionen (inkl. der Systempartition) verschlüsselt werden können.
DiskCryptor war von Version 0.1 bis 0.4 kompatibel mit TrueCrypt, wurde aber danach auf ein eigenes Partitionsformat umgestellt, da das TrueCrypt Format ursprünglich zur Erzeugung von leeren Volumes ausgelegt war. Dies führte zu einer verbesserten Stabilität.

DiskCryptor
Features

DiskCryptor Features

- Verfügbar für Windows

DiskCryptor
Features

- Verfügbar für Windows
- Unterstützte Verschlüsselung: AES, Twofisch, Serpent

DiskCryptor
Features

- Verfügbar für Windows
- Unterstützte Verschlüsselung: AES, Twofisch, Serpent
- Verschlüsselungsschicht: Volumes

DiskCryptor
Features

- Verfügbar für Windows
- Unterstützte Verschlüsselung: AES, Twofisch, Serpent
- Verschlüsselungsschicht: Volumes
- Lizenz: GPL3

TruPax

TruPax

TruPax ist ein Java-basiertes Verschlüsselungstool.

TruPax

TruPax ist ein Java-basiertes Verschlüsselungstool.
Es kann TrueCrypt-Container erstellen und verwenden, jedoch nicht mounten.

TruPax
Features

TruPax
Features

- Verfügbar für Windows, Linux, MacOS

TruPax
Features

- Verfügbar für Windows, Linux, MacOS
- Unterstütze Verschlüsselung: AES-256

TruPax
Features

- Verfügbar für Windows, Linux, MacOS
- Unterstütze Verschlüsselung: AES-256
- Verschlüsselungsschicht: Volumes/Container

TruPax
Features

- Verfügbar für Windows, Linux, MacOS
- Unterstütze Verschlüsselung: AES-256
- Verschlüsselungsschicht: Volumes/Container
- Lizenz: LGPL3

EncFS

EncFS

EncFS ist ein verschlüsseltes Dateisystem (im user-space), welches die FUSE-Bibliothek und Linux Kernel-Module nutzt.

EncFS
Features

EncFS
Features

- Verfügbar für Windows, Linux (nativ), MacOS, Android, iOS

EncFS
Features

- Verfügbar für Windows, Linux (nativ), MacOS, Android, iOS
- Unterstützte Verschlüsselung: AES, Blowfish, weitere (vom BS abhängig)

EncFS
Features

- Verfügbar für Windows, Linux (nativ), MacOS, Android, iOS
- Unterstützte Verschlüsselung: AES, Blowfish, weitere (vom BS abhängig)
- Verschlüsselungsschicht: Dateibasiert

EncFS
Features

- Verfügbar für Windows, Linux (nativ), MacOS, Android, iOS
- Unterstützte Verschlüsselung: AES, Blowfish, weitere (vom BS abhängig)
- Verschlüsselungsschicht: Dateibasiert
- Lizenz: GPL

GnuPG

GnuPG

GnuPG findet nicht nur Verwendung bei der Verschlüsselung von Emails, sondern kann auch Dateien verschlüsseln.

GnuPG
Features

GnuPG
Features

- Verfügbar für Windows, Linux, MacOS, Android, iOS

GnuPG
Features

- Verfügbar für Windows, Linux, MacOS, Android, iOS
- Unterstützte Verschlüsselung: IDEA, 3DES, CAST5, Blowfish, AES-128/192/256, Twofish, Camelia-128/192/256

GnuPG
Features

- Verfügbar für Windows, Linux, MacOS, Android, iOS
- Unterstützte Verschlüsselung: IDEA, 3DES, CAST5, Blowfish, AES-128/192/256, Twofish, Camelia-128/192/256
- Verschlüsselungsschicht: Dateibasiert, Text

GnuPG
Features

- Verfügbar für Windows, Linux, MacOS, Android, iOS
- Unterstützte Verschlüsselung: IDEA, 3DES, CAST5, Blowfish, AES-128/192/256, Twofish, Camelia-128/192/256
- Verschlüsselungsschicht: Dateibasiert, Text
- Lizenz: GPL

luksus / tcplay

luksus / tcplay

luksus ist ein wrapper für tcplay, cryptsetup und weitere Verschlüsselungs-Tools.

luksus / tcplay

luksus ist ein wrapper für tcplay, cryptsetup und weitere Verschlüsselungs-Tools.
Bietet eine Menübasierte Oberfläche auf der Konsole und kann TrueCrypt-Volumes verarbeiten.

luksus / tcplay
Features

luksus / tcplay
Features

- Verfügbar für Linux

luksus / tcplay
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES

luksus / tcplay
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES
- Verschlüsselungsschicht: Datei-/Volumebasiert

luksus / tcplay
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES
- Verschlüsselungsschicht: Datei-/Volumebasiert
- Lizenz: GPL

realcrypt

realcrypt

realcrypt ist ein Linux-Remake von TrueCrypt (TrueCrypt Sourcecode mit neuem Anstrich).

realcrypt

realcrypt ist ein Linux-Remake von TrueCrypt (TrueCrypt Sourcecode mit neuem Anstrich).
Kann alles, was TrueCrypt kann, liegt aber leider nur als rpm vor.

realcrypt Features

realcrypt Features

- Verfügbar für Linux

realcrypt Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES, Twofish

realcrypt Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES, Twofish
- Verschlüsselungsschicht: Datei-/Volumenbasiert

realcrypt
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES, Twofish
- Verschlüsselungsschicht: Datei-/Volumenbasiert
- Lizenz: GPL

ecryptfs

ecryptfs

ecryptfs ist ein Stacked Dateisystem auf Kernel-Ebene.

ecryptfs

ecryptfs ist ein Stacked Dateisystem auf Kernel-Ebene.
Es erlaubt die Auswahl zu verschlüsselnder Ordner.

ecryptfs

ecryptfs ist ein Stacked Dateisystem auf Kernel-Ebene.
Es erlaubt die Auswahl zu verschlüsselnder Ordner.
Standard bei Ubuntu (home-Verzeichnis)

ecryptfs
Features

ecryptfs
Features

- Verfügbar für Linux

ecryptfs
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung:

ecryptfs
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung:
- Verschlüsselungsschicht: Dateisystem, Dateien und Verzeichnisse

ecryptfs
Features

- Verfügbar für Linux
- Unterstützte Verschlüsselung:
- Verschlüsselungsschicht: Dateisystem, Dateien und Verzeichnisse
- Lizenz: GPL

dm-crypt + LUKS

dm-crypt + LUKS

dm-crypt + LUKS ist die native Linux Disk-Verschlüsselung vieler Distributionen.

dm-crypt + LUKS

dm-crypt + LUKS ist die native Linux Disk-Verschlüsselung vieler Distributionen.
Ausserdem bedeutet es: **L**inux **U**nified **K**ey **S**etup

dm-crypt + LUKS
Features

dm-crypt + LUKS
Features

- Verfügbar für Windows, Linux (nativ), Android (nur BS)

dm-crypt + LUKS
Features

- Verfügbar für Windows, Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden

dm-crypt + LUKS
Features

- Verfügbar für Windows, Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden
- Verschlüsselungsschicht: Block-Level, kann verschiedene Dateisysteme enthalten

dm-crypt + LUKS
Features

- Verfügbar für Windows, Linux (nativ), Android (nur BS)
- Unterstützte Verschlüsselung: AES-256, weitere können hineinkompiliert werden
- Verschlüsselungsschicht: Block-Level, kann verschiedene Dateisysteme enthalten
- Lizenz: GPL

Containerdatei im „Eigenbau“
Beispiel Ubuntu

Containerdatei im „Eigenbau“ Beispiel Ubuntu

Siehe Beispiel im Handout...

Links zur Präsentation

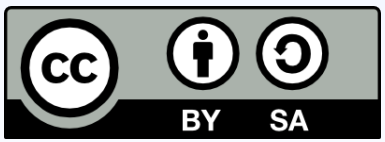
http://www.truecrypt.ch/
http://veracrypt.codeplex.com/
https://diskcryptor.net/wiki/Main_Page
http://www.coderslagoon.com/ (TruPax)
https://en.wikipedia.org/wiki/EncFS
https://www.gnupg.org
https://github.com/thomasfrivold/luksus
http://rpmfusion.org/Package/realcrypt
http://ecryptfs.org/
http://arstechnica.com/civis/viewtopic.php?f=21&t=1245367
http://wiki.ubuntuusers.de/LUKS
http://wiki.ubuntuusers.de/LUKS/Containerdatei

FreieSoftwareOG.org

Weitere Informationen bekommen Sie hier:

http://www.FreieSoftwareOG.org
und
Kontakt@FreieSoftwareOG.org

oder kommen Sie doch einfach zu unserem regelmäßigen Treffen,
jeden 1. Mittwoch im Monat ab 20:00 Uhr.
(Treffpunkt und Thema laut Webseite)



FreieSoftwareOG.org