

Datensicherheit & Verschlüsselung

Journalistischer Kompetenzblock

Robert Bienert

Nordhessen Media e.V.

18. Juni 2009

- URL: <http://hnawatchblog.de/vortrag/datensicherheit>
- Es ist gestattet, das Werk vervielfältigen, verbreiten und öffentlich zugänglich machen, zu folgenden Bedingungen: 
-  Namensnennung
-  Nicht-Kommerziell
-  Keine Bearbeitung und abgeleitete Werke
- ( Creative Commons by-nc-nd)

- 1 Einleitung
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation
- 5 Ausblick
- 6 Referenzen und Links

- 1 Einleitung
 - Datensicherheit: Worum es (heute) nicht geht
 - Datensicherheit: Wofür?
 - Datensicherheit: Wie?
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation
- 5 Ausblick
- 6 Referenzen und Links



Abbildung: Diverse Medien zur Datenspeicherung/Backups.



Abbildung: Diverse Medien zur Datenspeicherung/Backups.

- unbefugten Zugriff verhindern
 - vor Sicherheits- und Geheimdienste
 - auf externe Datenträgern
 - ...

- unbefugten Zugriff verhindern
 - vor Sicherheits- und Geheimdienste
 - auf externe Datenträgern
 - ...
- eigene und Privatsphäre anderer schützen

- unbefugten Zugriff verhindern
 - vor Sicherheits- und Geheimdienste
 - auf externe Datenträgern
 - ...
- eigene und Privatsphäre anderer schützen
- Kommunikation in nicht vertrauenswürdigen Umgebungen

Dieses Seminar geht auf folgende Aspekte und Werkzeuge genauer ein:

Dieses Seminar geht auf folgende Aspekte und Werkzeuge genauer ein:

- GnuPG^a und GPA^b zur Email- und Datenverschlüsselung sowie -signierung
- TrueCrypt zur Daten- und Datenträgerverschlüsselung
- SSH^c für den sicheren Datentransport

^aGNU Privacy Guard

^bGNU Privacy Assistant

^cSecure Shell

- 1 Einleitung
- 2 Daten sicher Speichern**
 - GnuPG (GPA)/PGP
 - TrueCrypt
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation
- 5 Ausblick
- 6 Referenzen und Links

Funktionsprinzip

- wahlweise
 - symmetrische Verschlüsselung (ein Schlüssel)
 - *asymmetrische Verschlüsselung (einer fürs Ver-, einer fürs Entschlüsseln)*

Funktionsprinzip

- wahlweise
 - symmetrische Verschlüsselung (ein Schlüssel)
 - *asymmetrische Verschlüsselung (einer fürs Ver-, einer fürs Entschlüsseln)*
- asymmetrisch:
 - Public-Key: Verschlüsseln, Signatur Prüfen
 - Secret-Key: Entschlüsseln, Signieren

Schlüssel erzeugen

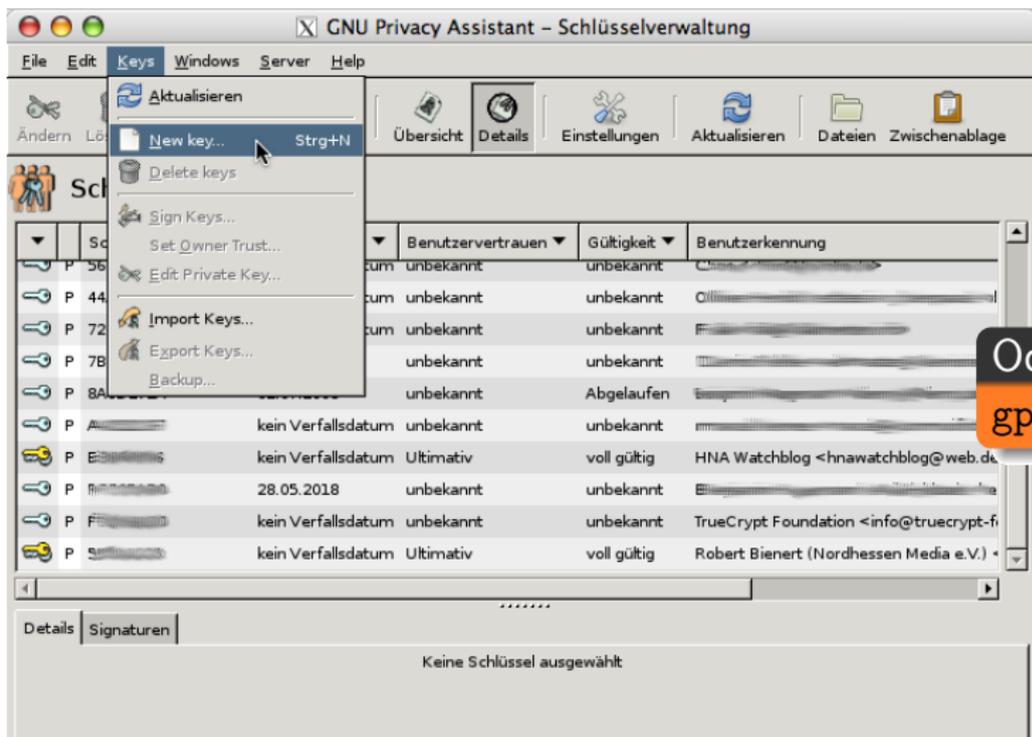
The screenshot shows the GNU Privacy Assistant - Schlüsselverwaltung window. The 'Keys' menu is open, and 'New key...' is highlighted. The main window displays a table of keys with columns for 'Benutzervertrauen', 'Gültigkeit', and 'Benutzerkennung'.

	Benutzervertrauen	Gültigkeit	Benutzerkennung
um	unbekannt	unbekannt	
um	unbekannt	unbekannt	
um	unbekannt	unbekannt	
	unbekannt	unbekannt	
	unbekannt	Abgelaufen	
kein Verfallsdatum	unbekannt	unbekannt	
kein Verfallsdatum	Ultimativ	voll gültig	HNA Watchblog <hnowatchblog@web.de>
28.05.2018	unbekannt	unbekannt	
kein Verfallsdatum	unbekannt	unbekannt	TrueCrypt Foundation <info@truencrypt-fi>
kein Verfallsdatum	Ultimativ	voll gültig	Robert Bienert (Nordhessen Media e.V.)

Details | Signaturen

Keine Schlüssel ausgewählt

Schlüssel erzeugen



Schlüssel erzeugen

Wichtig:

- sichere Passphrase
- langer Schlüssel
- guter Algorithmus
- Secret-Key gut und *sicher* aufbewahren

Schlüssel erzeugen

Wichtig:

- sichere Passphrase
- langer Schlüssel
- guter Algorithmus
- Secret-Key gut und *sicher* aufbewahren
- Public-Key veröffentlichen

Schlüssel verwalten

GNU Privacy Assistant – Schlüsselverwaltung

File Edit Keys Windows Server Help

Ändern Löschen Signieren Import Export Übersicht Details Einstellungen Aktualisieren Dateien Zwischenablage

Schlüsselverwaltung

	Schlüsselkennung	Verfallsdatum	Benutzervertrauen	Gültigkeit	Benutzerkennung
	kein Verfallsdatum	unbekannt	unbekannt	unbekannt	unbekannt
P	kein Verfallsdatum	unbekannt	unbekannt	unbekannt	unbekannt
P	kein Verfallsdatum	unbekannt	unbekannt	unbekannt	unbekannt
P	26.03.2012	unbekannt	unbekannt	unbekannt	unbekannt
P	01.07.2008	unbekannt	unbekannt	Abgelaufen	unbekannt
P	kein Verfallsdatum	unbekannt	unbekannt	unbekannt	unbekannt
P	EB669546	kein Verfallsdatum	Ultimativ	voll gültig	HNA Watchblog <hnawatchblog@web.de>
P	F	28.05.2018	unbekannt	unbekannt	unbekannt
P	F0D6B1E0	kein Verfallsdatum	unbekannt	unbekannt	TrueCrypt Foundation <info@truecrypt-fi>
P	551A1225	kein Verfallsdatum	Ultimativ	voll gültig	Robert Bienert (Nordhessen Media e.V.)

Details Signaturen

Schlüsselkennung	Gültigkeit der Beglaubigung	Benutzerkennung
EB669546	unbekannt	HNA Watchblog <hnawatchblog@web.de>
551A1225	unbekannt	Robert Bienert (Nordhessen Media e.V.) <robert.bienert@nordhessen-media.de>

Standard-Schlüssel: 18BD7A3C Robert Bienert (Schlüssel fuer private Kommunikation) <robertbienert@web.de>

Schlüssel verwalten

GNU Privacy Assistant – Schlüsselverwaltung

File Edit Keys Windows Server Help

Ändern Löschen Signieren Import Export Übersicht Details Einstellungen Aktualisieren Dateien Zwischenablage

Schlüsselverwaltung

	Schlüsselkennung	Verfallsdatum	Benutzervertrauen	Gültigkeit	Benutzerkennung
P		kein Verfallsdatum	unbekannt	unbekannt	
P		kein Verfallsdatum	unbekannt	unbekannt	
P		26.03.2012	unbekannt	unbekannt	
P		01.07.2008	unbekannt	Abgelaufen	
P		kein Verfallsdatum	unbekannt	unbekannt	
P	EB669546	kein Verfallsdatum	Ultimativ	voll gültig	HNA Watchblog <hnawatchblog@web.de>
P	F	28.05.2018	unbekannt	unbekannt	
P	F0D6B1E0	kein Verfallsdatum	unbekannt	unbekannt	TrueCrypt Foundation <info@truencrypt-f>
P	551A1225	kein Verfallsdatum	Ultimativ	voll gültig	Robert Bienert (Nordhessen Media e.V.)

Details Signaturen

Schlüsselkennung	Gültigkeit der Beglaubigung	Benutzerkennung
EB669546	unbekannt	HNA Watchblog <hnawatchblog@web.de>
551A1225	unbekannt	Robert Bienert (Nordhessen Media e.V.) <robert.bienert@nordhessen-media.de>

Standard-Schlüssel: 18BD7A3C Robert Bienert (Schlüssel fuer private Kommunikation) <robertbienert@web.de>

- Schlüsseling
- `gpg --list-keys`
- `gpg --edit-key`
- `gpg --sign-key`
- ...

Schlüssel verwalten

GNU Privacy Assistant – Schlüsselverwaltung

File Edit Keys Windows Server Help

Ändern Löschen Signieren Import Export Übersicht Details Einstellungen Aktualisieren Dateien Zwischenablage

Schlüsselverwaltung

	Schlüsselkennung	Verfallsdatum	Benutzervertrauen	Gültigkeit	Benutzerkennung
P		kein Verfallsdatum	unbekannt	unbekannt	
P		kein Verfallsdatum	unbekannt	unbekannt	
P		26.03.2012	unbekannt	unbekannt	
P		01.07.2008	unbekannt	Abgelaufen	
P		kein Verfallsdatum	unbekannt	unbekannt	
P	EB669546	kein Verfallsdatum	Ultimativ	voll gültig	HNA Watchblog <hnawatchblog@web.de>
P	F	28.05.2018	unbekannt	unbekannt	
P	F0D6B1E0	kein Verfallsdatum	unbekannt	unbekannt	TrueCrypt Foundation <info@truencrypt-f
P	551A1225	kein Verfallsdatum	Ultimativ	voll gültig	Robert Bienert (Nordhessen Media e.V.)

Details Signaturen

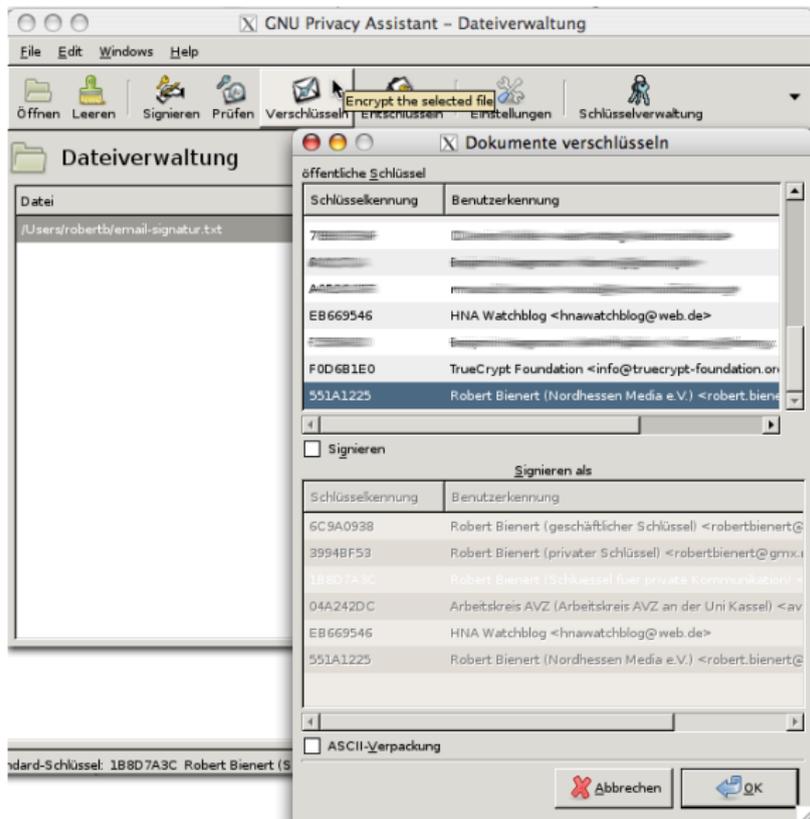
Schlüsselkennung	Gültigkeit der Beglaubigung	Benutzerkennung
EB669546	unbekannt	HNA Watchblog <hnawatchblog@web.de>
551A1225	unbekannt	Robert Bienert (Nordhessen Media e.V.) <robert.bienert@nordhessen-media.de>

Standard-Schlüssel: 18BD7A3C Robert Bienert (Schlüssel fuer private Kommunikation) <robertbienert@web.de>

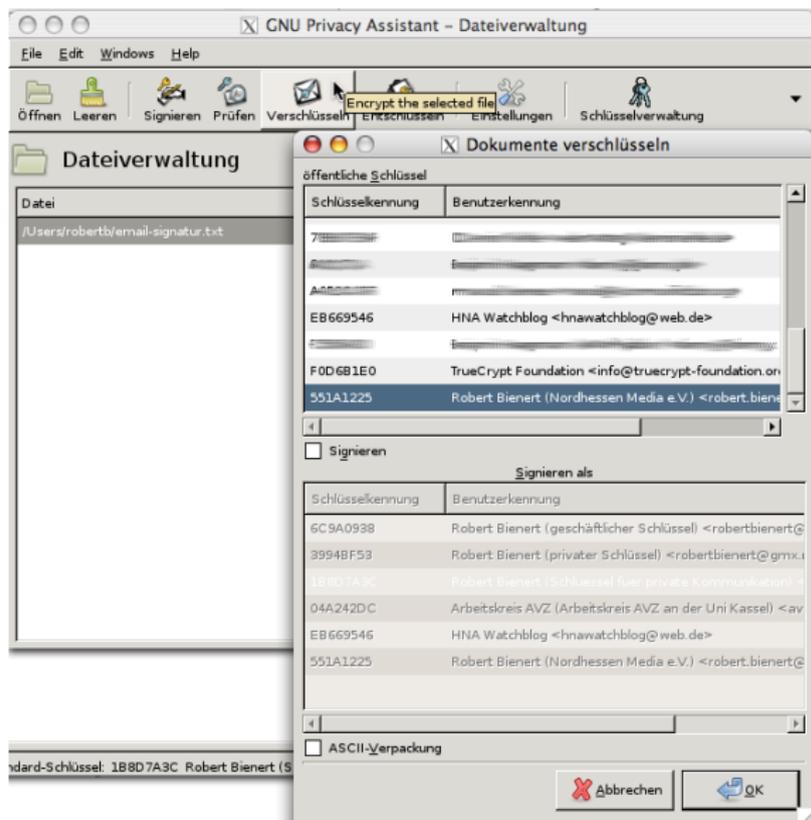
- Schlüsseling
- `gpg --list-keys`
- `gpg --edit-key`
- `gpg --sign-key`
- ...

- *Web of Trust*

Dateien verschlüsseln



Dateien verschlüsseln



analog:

- Entschlüsseln
- Signieren

Funktionsprinzip

Verschlüsselung von

- Partitionen
- externen Datenträgern
- Teilen von Partitionen, Dateicontainer

Funktionsprinzip

Verschlüsselung von

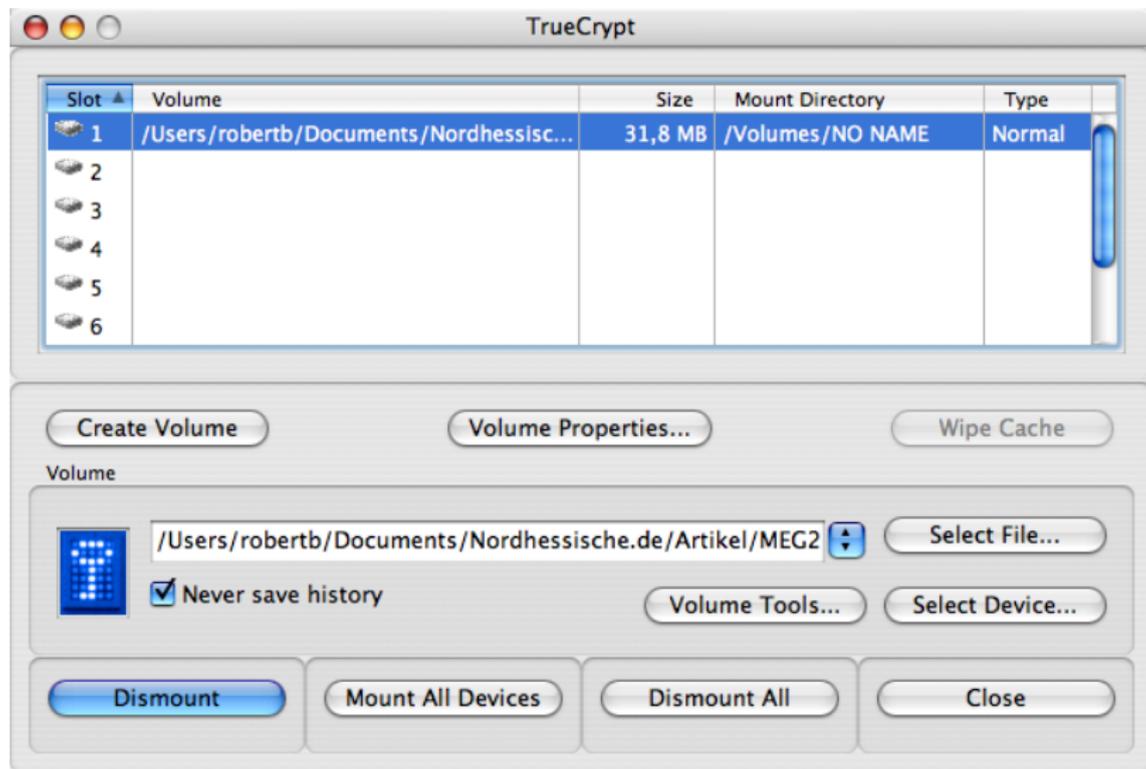
- Partitionen
 - externen Datenträgern
 - Teilen von Partitionen, Dateicontainer
-
- mehrere Verschlüsselungsverfahren hintereinander
 - Keyfiles
 - transparent (beim Arbeiten)
 - *Konzept der glaubhaften Abstreitbarkeit:*

Funktionsprinzip

Verschlüsselung von

- Partitionen
 - externen Datenträgern
 - Teilen von Partitionen, Dateicontainer
-
- mehrere Verschlüsselungsverfahren hintereinander
 - Keyfiles
 - transparent (beim Arbeiten)
 - *Konzept der glaubhaften Abstreitbarkeit:*
 - Dateien oder Partitionen nicht identifizierbar
 - versteckte Container

Datenträger-Verwaltung



- 1 Einleitung
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren**
- 4 Sichere Kommunikation
- 5 Ausblick
- 6 Referenzen und Links

SSH nur kurz

- **Secure Shell**
- sichere und authentifizierte Remote-Verbindung
- Public-Key-Authentifizierung möglich
- Absichern beliebiger Anwendungen
- SSHFS für „entfernte Ordner“
- sicheres Kopieren von Dateien (`scp`, `WinSCP`, ...)

- 1 Einleitung
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation**
 - Emails
- 5 Ausblick
- 6 Referenzen und Links

GPG als Plug-In

Eigenschaften

- Ver- und Entschlüsseln sowie Signieren per Mausklick (Mail und Anhänge)
- Zugriff auf eigenen Schlüsselring
- automatisches Prüfen von Signaturen

GPG als Plug-In

Eigenschaften

- Ver- und Entschlüsseln sowie Signieren per Mausklick (Mail und Anhänge)
- Zugriff auf eigenen Schlüsselring
- automatisches Prüfen von Signaturen

Plug-Ins

Enigmail: Thunderbird

GPGMail: Apple Mail.app

GPG als Plug-In: GPGMail (Apple Mail.app)

An: test@example.org

Kopie:

Blindkopie:

Antwort an:

Betreff: GPGMail-signiert

Account: "Robert Bienert (Vorstand Nordhessen Media e..." Signatur: Keine

PGP: Signieren Robert Bienert <robert.bienert...> Verschlüsseln Schlüssel

Hallo,

Abbildung: Signieren von Emails

Nordhessische.de – Nachr...	Re: Fragen Piraten	11.06.2009	15:12	🔗	1 Objekt
Jonas Dörge	Logo(s) Nordhessen Media e.V.	11.06.2009	20:31	🔗	1 Objekt
Nordhessische.de – Nachr...	Re: HNA Watchblog	11.06.2009	21:27	🔗	2 Objekte

 Signiert von Robert Bienert (Nordhessen Media e.V.) <robert.bienert@nordhessen-media.de>

Signiert am Donnerstag, 11. Juni 2009 20:31 Uhr Europe/Berlin Gültigkeit: voll

Fingerabdruck: 49D1 E8B0 9788 0128 CC10 ADC1 C539 70CA 551A 1225 Benutzer IDs ▾

Betreff: **Logo(s) Nordhessen Media e.V.**

Abbildung: Überprüfen und Anzeigen einer signierten Email

- 1 Einleitung
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation
- 5 Ausblick**
- 6 Referenzen und Links

- anonyme Kommunikation (z. B. TOR, Proxies, ...)
- „tote Briefkästen“
- gemeinsames Schlüssel-Generieren und -Unterschreiben
- ...

- anonyme Kommunikation (z. B. TOR, Proxies, ...)
- „tote Briefkästen“
- gemeinsames Schlüssel-Generieren und -Unterschreiben
- ...

- *dein Wunsch hier*

- 1 Einleitung
- 2 Daten sicher Speichern
- 3 Daten sicher Transferieren
- 4 Sichere Kommunikation
- 5 Ausblick
- 6 Referenzen und Links**

Referenzen

 KAI RAVEN: *Deutsche GnuPG-Anleitung*.

Online: <http://hp.kairaven.de/pgp/gpg/index.html>, 2001.

 TRUECRYPT FOUNDATION: *TrueCrypt Documentation*.

Online: <http://www.truecrypt.org/docs/>

Links

GNU Privacy Guard: <http://gnupg.org/>

Enigmail: <http://enigmail.mozdev.org/>

GPGMail: <http://www.sente.ch/software/GPGMail/>