

Autoren: Graber Johnny, Müdespacher Andreas  
Thema: Sicherheitstool für USB-Sticks  
Datum: 14. Dezember 2006

geht an: Dubois Jean-Paul  
Fuhrer Claude  
Voirol Pierre-Yves

# Benutzerhandbuch AtaraxiS

1	Installation.....	2
1.1	Systemvoraussetzungen.....	2
1.2	Zusätzliche Software.....	2
1.3	Installation auf USB-Stick.....	2
1.4	Lokale Installation auf Festplatte.....	2
1.5	Installation einer zusätzlichen Java JRE (USB-Stick oder Festplatte).....	2
2	1. Start und Login.....	2
3	Benutzer erstellen.....	3
4	Grundlegende Benutzerführung.....	4
5	Daten verschlüsseln.....	4
6	Daten entschlüsseln.....	5
7	Daten sicher löschen.....	5
8	Passwörter verwalten.....	6
9	Einstellungen vornehmen.....	7
10	Programminformationen.....	7
11	Programm beenden.....	7
12	Autostart konfigurieren.....	8
12.1	Autorun.inf.....	8
12.2	C't USB Agent.....	8
13	Problembehebung.....	9
13.1	Probleme mit „policy“ Dateien.....	9
13.2	Startproblem unter Linux.....	9

# 1 Installation

## 1.1 Systemvoraussetzungen

AtaraxiS läuft auf den Betriebssystemen Windows und Linux (getestet auf Fedora Core 5 & 6).

Auf dem Datenträger wird je nach Installationsart unterschiedlich viel Speicherplatz benötigt:

Nur AtaraxiS, kein zusätzliches Java*:	7 MB
AtaraxiS und 1 JRE (Windows oder Linux):	~85 MB
AtaraxiS und 2 JRE (Windows und Linux):	~180 MB

\* Benötigt auf jedem System, auf dem AtaraxiS ausgeführt wird, eine bereits installierte JRE.

## 1.2 Zusätzliche Software

Folgende zusätzliche Software ist nötig, um AtaraxiS benutzen zu können:

- Java Runtime Enviroment (JRE) Version 5 oder höher

Sollten sie noch keine Java-Version installiert haben, finden sie diese auf der Website von SUN ([http://java.sun.com/javase/downloads/index\\_jdk5.jsp](http://java.sun.com/javase/downloads/index_jdk5.jsp)). Alternativ können sie eine JRE für Windows und Linux auf unserer Projekt Website (<http://projects.hti.bfh.ch/ataraxis/>) herunterladen.

## 1.3 Installation auf USB-Stick

Gehen sie wie folgt vor, um AtaraxiS auf einem USB-Stick unter **Windows** zu installieren:

- Schliessen sie ihren USB-Stick am Computer an
- Entpacken sie die Zip-Datei `AtaraxiS_Generic.zip` direkt in das Laufwerk, dass ihrem USB-Stick zugewiesen wurde. (Ist die Laufwerksbezeichnung ihres USB-Sticks `E:\`, entpacken sie die Zip-Datei nach `E:\`)
- Eine Ebene unterhalb des Laufwerks befindet sich nun ein Ordner mit dem Namen `AtaraxiS` (Beispielsweise `E:\AtaraxiS\`)

Gehen sie wie folgt vor, um AtaraxiS auf einem USB-Stick unter **Linux** zu installieren:

- Schliessen sie ihren USB-Stick am Computer an
- Entpacken sie die Zip-Datei `AtaraxiS_Generic.zip` in das Verzeichnis direkt unter dem Mount-Point des USB-Sticks.
- Eine Ebene tiefer im Verzeichnisbaum befindet sich nun ein Ordner namens `AtaraxiS`

## 1.4 Lokale Installation auf Festplatte

Um AtaraxiS lokal auf der Festplatte zu installieren, entpacken sie die Zip-Datei `AtaraxiS_Generic.zip` in das Verzeichnis ihrer Wahl.

## 1.5 Installation einer zusätzlichen Java JRE (USB-Stick oder Festplatte)

Um eine zusätzliche JRE lokal auf dem USB-Stick oder am gleichen Ort auf der Festplatte zu installieren, können sie wie folgt vorgehen:

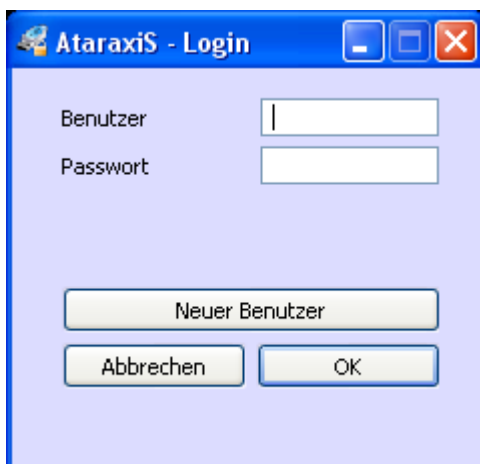
- Laden sie sich von unserer Projektseite die zum Betriebssystem passende JRE-Version herunter
- Entpacken sie die so erhaltene Zip-Datei direkt in den Ordner, in dem sich AtaraxiS befindet.

# 2 1. Start und Login

War die Installation erfolgreich, haben sie einen Ordner namens `AtaraxiS` erstellt. Wechseln sie in diesen Ordner hinein. Sie sollten dort diese Unterordner und Dateien vorfinden:

- \application\_data\: Hier sind Daten von AtaraxiS abgelegt, die für den Betrieb benötigt werden
- \user\_data\: Hier werden ihre Benutzerdaten (Login-Informationen) gespeichert
- \lib\: Dieser Ordner enthält für AtaraxiS notwendige Hilfsprogramme
- AtaraxiS.jar: Die gepackten Programmdateien von AtaraxiS
- autostart.bat: Programm für den automatischen Start. (Siehe Autostart-Konfigurieren)
- startWin.bat: Windows-Start-Programm für Ataraxis mit dem System-JRE
- startWin\_LocalJava.bat: Windows-Start-Programm für Ataraxis mit dem lokalen (USB-Stick) JRE
- startLinux.sh: Linux-Start-Programm für Ataraxis mit dem System-JRE
- startLinux\_LocalJava.sh: Linux-Start-Programm für Ataraxis mit dem lokalen (USB-Stick) JRE
- Backup\_Windows.bat: Backup-Programm für Windows
- Backup\_Linux.sh: Backup-Programm für Linux

Durch das Ausführen des für ihr Betriebssystem passenden Start-Programms können sie AtaraxiS starten. Für Benutzer von Windows ist dies `startWin.bat` oder `startWin_LocalJava.bat`, für Benutzer von Linux `startLinux.sh` oder `startLinux_LocalJava.sh`.



Nach dem Ausführen des Start-Programms öffnet sich dieser Dialog.

sie haben beim 1. Start noch kein Benutzerkonto. Klicken sie daher auf [Neuer Benutzer]

Wenn sie ein Benutzerkonto haben, können sie hier ihren Benutzernamen und ihr Passwort eingeben und auf [OK] klicken.

### 3 Benutzer erstellen



In diesem Dialog können sie einen neuen Benutzer erstellen. Verwenden sie als Benutzernamen bitte nur Kleinbuchstaben und Zahlen. Die minimale Länge eines Benutzernamens beträgt 2 Zeichen.

Ihr Passwort muss mindestens 4 Zeichen lang sein. Wählen sie dies sorgsam, da von der Sicherheit dieses Passworts die Sicherheit ihrer Daten abhängt. Wiederholen sie das Passwort im 2. Passwort-Feld.

Bei Sprache können sie die Sprache der Hauptapplikation ändern. Der Login-Screen wird immer automatisch auf die Systemsprache eingestellt.

## 4 Grundlegende Benutzerführung

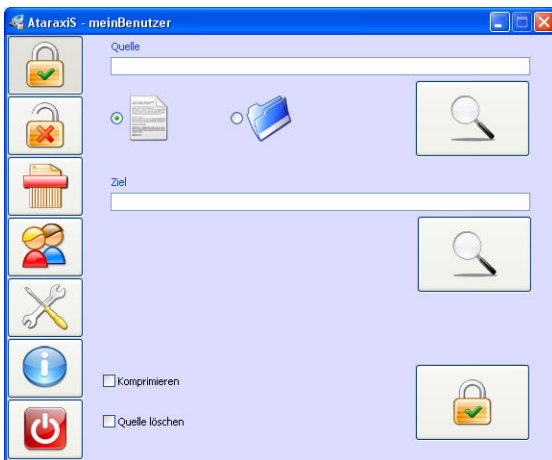


Nach dem erfolgreichen Login öffnet sich die Hauptoberfläche von AtaraxiS und es wird ein System-Tray (Ein kleines Bild mit einem Menü neben der Zeitangabe auf der Taskleiste) erzeugt.

Durch einen klick mit der rechten Maustaste auf das System-Tray erscheint die nebenstehende Liste.

Im der Hauptoberfläche finden sie am linken Rand die gleichen Bilder. Um die einzelnen Funktionen aufzurufen, können sie sowohl in der Hauptoberfläche wie auch im System-Tray auf das jeweilige Bild klicken.

## 5 Daten verschlüsseln



Dieser Dialog hat 2 Bereiche (Quelle und Ziel). Als Quelle können sie die Datei oder das Verzeichnis angeben, das Verschlüsselt werden soll. Als Ziel können sie die Datei angeben, in der AtaraxiS den verschlüsselten Inhalt abspeichern soll.

Über die Radio-Knöpfe können sie auswählen, ob sie eine Datei oder ein Verzeichnis verschlüsseln wollen. Durch einen klick auf den oberen Knopf mit der Lupe erreichen sie einen Dialog fürs auswählen.

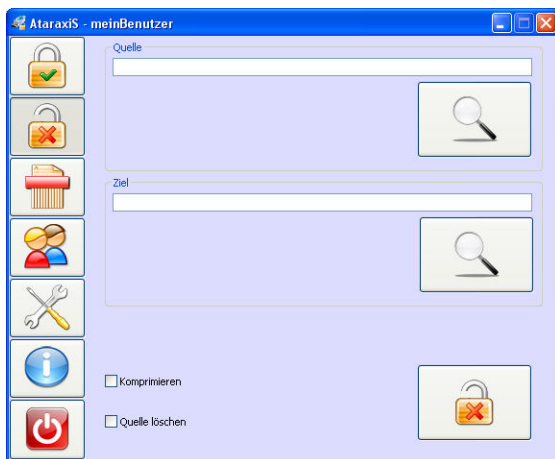
Alternativ können sie die gewünschte Datei per Drag&Drop in den jeweiligen Bereich hinein ziehen.

Als Ziel dient immer eine Datei, deshalb können sie hier nur Dateien auswählen.

Nun können sie noch die Kästchen unten links markieren, falls sie die Daten vor dem Verschlüsseln komprimieren und oder die Quelldatei (Klartext) nach erfolgreicher Verschlüsselung löschen wollen.

Zum Verschlüsseln klicken sie auf den Knopf mit dem Schloss (Rechts unten). Nach einer erfolgreichen Verschlüsselung erhalten sie eine Meldung.

## 6 Daten entschlüsseln



Das Entschlüsseln einer Datei funktioniert gleich einfach wie das Verschlüsseln.

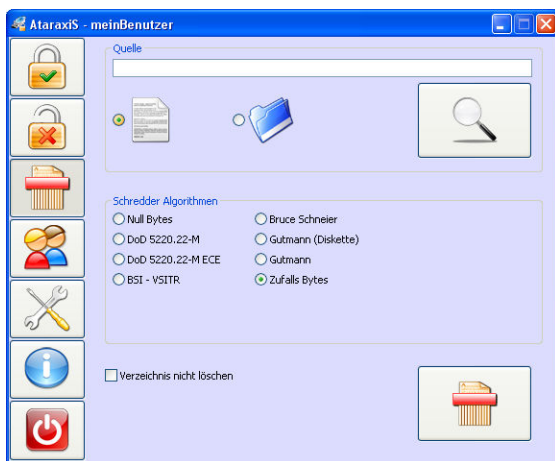
Wählen sie als Quelle die Datei, die den verschlüsselten Inhalt enthält.

Als Ziel können sie den Ort wählen, an den die Datei entschlüsselt werden soll.

Auch hier können sie durch markieren der Kästchen die Quelldatei nach dem Entschlüsseln automatisch löschen lassen und oder entpacken lassen. Es können jedoch nur komprimierte Daten (.acz-Endung) entpackt werden!

Zum Entschlüsseln klicken sie auf den Knopf mit dem Schloss (Rechts unten). Nach erfolgreichem entschlüsseln erhalten sie eine Meldung.

## 7 Daten sicher löschen



Um Daten sicher zu löschen, können sie diese wie von der Verschlüsselung bekannt auswählen.

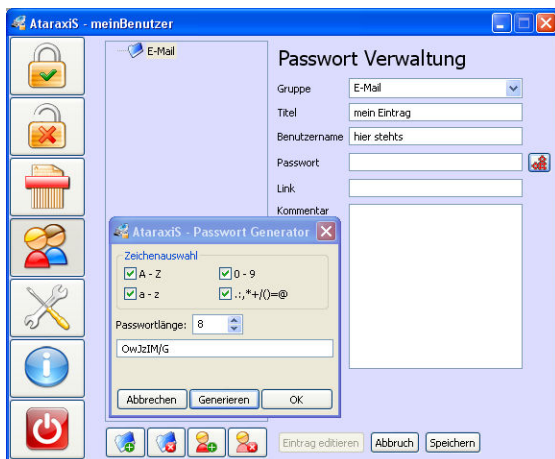
Bei Schredder-Algorithmen können sie auswählen, wie ihre Datei oder Verzeichnis überschrieben werden soll, bevor die Datei gelöscht wird.

Durch das mehrmalige überschreiben vor dem Löschen wird es so gut wie unmöglich, die Daten wieder herzustellen. Achten sie daher genau darauf, welche Dateien sie löschen!

### Implementierte Schredder Algorithmen

Null Bytes:	Überschreiben der Datei mit 0x00 (Byte)	1 Durchgang
DoD 5220.22-M (E):	Alter DoD Standard	3 Durchgänge
DoD 5220.22-M (ECE):	Erweiterter DoD Standard	7 Durchgänge
VSITR:	Deutscher Standard	7 Durchgänge
Bruce Schneier:	Implementierung der Empfehlung	7 Durchgänge
Peter Gutmann:	Implementierung des Algorithmus	35 Durchgänge (langsam)
Peter Gutmann für Disketten:	Für 3.5" Disketten optimierte Variante	18 Durchgänge
Zufallsdaten:	Zufallsmuster	10 Durchgänge

## 8 Passwörter verwalten



Wenn sie die Passwort Verwaltung zum ersten Mal benutzen, ist diese bis auf eine Gruppe E-Mail leer. Sie können beliebig viele Gruppen erstellen, die wiederum beliebig viele Einträge enthalten können.

Um Gruppen und Einträge zu erstellen und zu löschen finden sie am unteren Ende der Oberfläche vier Knöpfe. Die Knöpfe mit dem grünen + dienen zum Erstellen des jeweiligen Typs (Gruppe oder Eintrag), die mit dem roten x dienen zum löschen der Einträge oder Gruppen.

Um einen Eintrag zu erstellen, klicken sie auf die Figur mit dem grünen +. Als Gruppe können sie angeben, wo ihr Eintrag abgelegt werden soll. Der Titel sollte möglichst aussagekräftig gewählt werden, da dieser im Auswahlbaum angezeigt wird.

Achtung: Mit Version 1 von AtaraxiS dürfen Gruppen und Einträge nicht die gleichen Namen haben.

Mit dem Knopf rechts vom Passwort-Feld können sie den Passwort-Generator aufrufen. Dieser schlägt ihnen ein Passwort vor, das sie mit [OK] übernehmen können.

Am Ende der Erstellung müssen sie mit [Speichern] die Eintragserfassung beenden



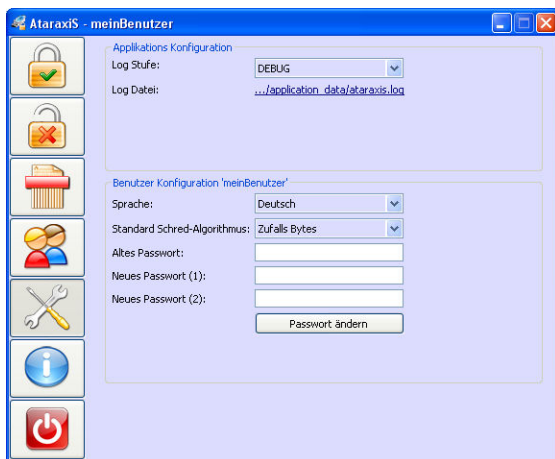
Nachdem sie einen Eintrag hinzugefügt haben, können sie diesen im linken Gruppierungsbaum auswählen.

Neben dem Benutzernamen und dem Passwort gibt es einen Knopf zum kopieren des jeweiligen Feldes in die Zwischenablage.

Neben dem Link gibt es einen Knopf, der den angegebenen Link in ihrem Webbrowser öffnet.

Sie können den Eintrag über den Knopf [Eintrag editieren] anpassen und wieder speichern.

## 9 Einstellungen vornehmen



Unter Einstellungen können sie die Vorgaben für die Log-Stufe, die Sprache und den Standard Schredder-Algorithmus ändern und ihr Passwort wechseln.

Die Log-Stufe beeinflusst die Eintragsanzahl in der Log-Datei. Falls Probleme auftauchen sollten sie diese auf DEBUG stellen. Ansonsten reicht WARN oder FATAL aus. Diese Einstellung ist für alle Benutzer gleich, sie gilt also applikationsweit.

Wenn sie das Passwort wechseln wollen, müssen sie ihr aktuelles Passwort eingeben und das Neue 2-mal angeben. Die Änderung wird erst wirksam, wenn sie auf [Passwort ändern] klicken.

Abgesehen vom Passwort werden alle Änderungen der Einstellungen sofort gesichert.

Das wechseln der Sprache und der Log Stufe werden erst mit dem nächsten Start wirksam.

## 10 Programminformationen



Hier finden sie neben Informationen zur Applikation auch einige Angaben zu ihrem System und der verwendeten Java-Version.

## 11 Programm beenden



Sie können jederzeit AtaraxiS über diesen Knopf beenden.

Es erscheint jeweils noch eine Meldung, ob sie wirklich beenden wollen. Falls ja, klicken sie auf [Ja], andernfalls auf [Nein]



## 12 Autostart konfigurieren

Es gibt derzeit keine überall funktionierende Möglichkeit für den automatischen Start von Programmen auf USB-Sticks. Damit AtaraxiS auf den Windows-PCs in ihrer täglichen Umgebung aber dennoch automatisch gestartet werden kann, empfohlen wird die Verwendung eines der beiden folgenden Ansätze.

### 12.1 Autorun.inf



Wenn sie nach unserer Installationsanleitung für den Einsatz von AtaraxiS auf einem USB-Stick vorgegangen sind, haben sie auf der gleichen Verzeichnisebene einen Ordner AtaraxiS und eine Datei autorun.inf.

Wenn dem so ist, genügt es den USB-Stick mit dem PC zu verbinden und es sollte sich ein Dialog öffnen, der wie der nebenstehende aussieht. Um AtaraxiS zu starten genügt ein klick auf den Knopf [OK].

Sollten sie eine andere Installationsart gewählt haben, finden sie in der Zip-Datei die entsprechende autorun.inf. Kopieren sie diese in die oberste Verzeichnisebene ihres USB-Sticks. (Ist ihr USB-Stick unter E:\ eingebunden, sollte der Dateipfad E:\autorun.inf sein)

### 12.2 C't USB Agent

Das Magazin C't hat in der Ausgabe 26/2002 einen Überwachungsdienst vorgestellt, der unter Windows 2000 und Windows XP das einstecken und abmelden von USB-Sticks überwacht und ein Event auslösen kann.

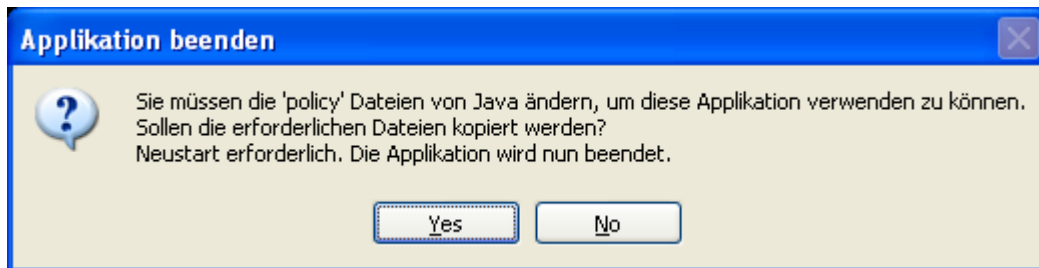
Laden sie von der Heise Website (<ftp://ftp.heise.de/pub/ct/listings/0226-206.zip>) den USB-Agenten herunter, entpacken sie die Zip-Datei und starten sie den Agenten. Am gleichen Ort wo die autorun.inf-Datei auf dem USB-Stick liegt, sollten sie auch eine Datei usbagent.inf vorfinden.

Die Installation des USB Agenten müssen sie auf jedem PC wiederholen, auf dem AtaraxiS automatisch gestartet werden soll.



## 13 Problembehebung

### 13.1 Probleme mit „policy“ Dateien



Falls diese Meldung erscheint, ist die von ihnen verwendete Java-Version bezüglich den Verschlüsselungsfunktionen eingeschränkt. Bestätigen sie mit [Yes] oder [Ja]. Ataraxis versucht nun, die Beschränkung durch kopieren entsprechender Policy-Dateien zu beheben. Um diese neuen Dateien zu nutzen, muss Ataraxis neu gestartet werden.

Meldet Ataraxis nach dem Neustart den gleichen Fehler, konnten die Dateien nicht kopiert werden.

#### Manuelles kopieren der Policy Dateien (Java 1.5)

Falls sie die Java-Version 1.5 (Java 5) verwenden, finden sie die notwendigen Policy-Dateien unter `Ataraxis\application_data\jce_policy\`. Kopieren sie diese beiden Dateien nach `\lib\security\` unterhalb des Pfades der verwendeten JRE.

Falls sie nicht wissen, wo sich ihr JRE befindet, schreibt Ataraxis den JRE-Pfad ins Logfile. Das Logfile selbst finden sie unter `Ataraxis\application_data\ataraxis.log`. Der Entsprechende Hinweis mit „JRE path“ wird nach der Policy-Meldung und beim bestätigen mit [Yes] oder [Ja] ins Logfile geschrieben und sollte in etwa so aussehen:

```
..misc.CopyPolicyFiles - JRE path:      C:\Program Files\Java\jdk1.5.0_09\jre\lib\security/  
..misc.CopyPolicyFiles - JRE version: 1.5.0_09  
..gui.AtaraxisLoginGUI - ##### Application close down at: Thu Dec 14 11:23:40 CET 2006 ###
```

#### Manuelles kopieren der Policy Dateien (alle anderen Java-Versionen)

Sollten sie eine andere Version von Java verwenden, müssen sie auf der Webseite von SUN die Dateien selber herunterladen. Suchen sie auf der Übersichtsseite zum Download ihrer Java-Version nach „Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files“.

Kopieren sie die Dateien wie für Java 1.5 beschrieben in das entsprechende Verzeichnis. Falls ihnen die Berechtigungen fehlen, um die Daten zu kopieren, müssen sie sich an ihren Systemadministrator wenden.

#### Verwendung des JRE von Ataraxis

Wie im Kapitel Installation beschrieben, können sie Java auch auf dem USB-Stick selbst installieren. Dazu folgen sie bitte unserer Anleitung und nehmen nach der Installation die `*_Local-Start`-Dateien um Ataraxis zu starten. Die Policy Dateien sind dort schon installiert.

### 13.2 Startproblem unter Linux

Unter Linux kann es zu Problemen beim automatischen mounten des USB-Sticks kommen. Falls sie Ataraxis nicht starten können, unmounten sie den USB-Stick, mounten ihn manuell und starten Ataraxis mit `./startLinux.sh`.