Das Open-Source-Tool Cryptonit

Plattformübergreifend sicher ver- und entschlüsseln

Dateien mit sensiblem Inhalt sollten nie unverschlüsselt per E-Mail verschickt oder auf einem USB-Stick gespeichert werden. Deshalb ist ein einfach zu bedienendes – und wenn möglich sogar plattformübergreifendes – Programm gefragt. Eine gute Wahl ist das Programm Cryptonit, das sowohl für GNU-Linux als auch für Windows verfügbar ist. Der Hersteller hat auch eine Macintosh-Version angekündigt. Wir zeigen Ihnen, wie Sie dieses Tool richtig einsetzen.

Die französische Firma OpenTrust S.A. (früher IDEALX) ist Anbieter des Tools Cryptonit. Die Produkte und Dienstleistungen der Firma sind alle im Umfeld PKI, Zertifikate, Verschlüsselung und Smartcards angesiedelt.

Es ist keine Installation erforderlich

Sie müssen Cryptonit nicht installieren. Es ist ausreichend, die ausführbare Datei – unter Windows zur Zeit Cryptonit-0.9.7.exe – an geeigneter Stelle zu speichern und im Startmenü oder auf dem Desktop eine Verknüpfung anzulegen.

Die übersichtliche Oberfläche des Programms Cryptonit von OpenTrust.

Das Tool Cryptonit wird mit Quellcode veröffentlicht

OpenTrust veröffentlicht Cryptonit mit dem kompletten Quelltext. Es steht unter der GPL v2. Sie können es überall frei einsetzen (*http://www.cryptonit.org*).

Für einen kommerziellen Einsatz des enthaltenen IDEA-Algorithmus ist in einigen Ländern, so beispielsweise in Deutschland, unter Umständen eine IDEA-Lizenz erforderlich.

Cryptonit gibt es auch auf Deutsch

Die Software ist in sieben Sprachen, darunter Deutsch, Englisch und Französisch, verfügbar.

Beim ersten Start legt das Tool im User-Verzeichnis – unter Windows XP in C:\Dokumente und Einstellungen\<<username>> – ein Verzeichnis mit dem Namen „Cryptonit“ an.

Hier speichert das Programm seine Konfigurationsdateien sowie alle Schlüssel und Zertifikate.

Auf andere Rechner lässt sich das Tool ganz leicht kopieren

Durch das schlichte Kopieren dieses Verzeichnisses können Sie die komplette Umgebung und Konfiguration der Software auf einen anderen Rechner transferieren.

Ein Assistent führt leicht verständlich durch den Verschlüsselungsprozess

Mit Cryptonit können Sie RSA-Schlüsselpaare erzeugen. Darüber hinaus lassen sich vorhandene öffentliche Schlüssel bzw. X.509-Zertifikate und -Schlüsselpaare importieren.

Zugang zu diesen Funktionalitäten erhalten Sie über den Button „Einstellungen“. Wählen Sie dann im linken Menü den Punkt „Benutzerkennungen“ aus.

Ein Schlüsselpaar erstellen Sie über den untersten Button „Zertifikatantrag“. Ein Assistent führt Sie durch den Prozess.

Schlüsselverwaltung per Mausklick

Die Verwaltung der öffentlichen Schlüssel der Kommunikationspartner geschieht über den Button „Kontakte“ in der Hauptleiste.

Sobald das X.509-Zertifikat eines Partners importiert ist, können Dateien für diesen Partner verschlüsselt werden.

Reihenfolge einhalten!

Die Menü-Buttons „Verschlüsseln“, „Entschlüsseln“, „Signieren“ und „Überprüfen“ lösen die entsprechenden Funktionen aus.

Zum Signieren und Verschlüsseln müssen Sie die beiden Operationen genau

Wird eine selbstentschlüsselnde Datei erzeugt, fragt diese beim Start nach dem Passwort.

Selbstentschlüsselnde Dateien

Über den Menü-Button „Selbst“ können Sie selbstentschlüsselnde Dateien sowohl für das Zielsystem Windows als auch für GNU-Linux erzeugen.

Hierbei wird beim Verschlüsseln und beim Entschlüsseln ein – hoffentlich gutes – Passwort verwendet. Beachten Sie aber, dass manche Mailserver ausführbare Dateien als Anhang verbieten.

in dieser Reihenfolge ausführen. Eine Automatik für gleichzeitiges Signieren und Verschlüsseln gibt es nicht.

Standardkonforme PKCS7-Dateien

Das Tool erzeugt standardkonforme PKCS7-Dateien. Diese können auch viele andere Programme verarbeiten.

Nach geeigneter Konfiguration kann das Programm auch auf einen LDAP-Server im Unternehmen zugreifen und Kontaktdaten sowie X.509-Zertifikate von dort beziehen, d.h. importieren.

Die Einbindung kryptografischer Hardware

Ihre kryptografische Hardware, beispielsweise eine Chipkarte oder ein USB-Dongle, können Sie über die Standard-Schnittstelle PKCS11 nutzen.

Hier wird insbesondere der belgische Personalausweis mit seinem eingebauten Kryptochip unterstützt.

Eine Anleitung zur Einbindung kryptografischer Hardware finden Sie im Downloadbereich der Cryptonit-Programm-Homepage.

Einfach, sicher und kostenlos

Cryptonit ist ein mächtiges, aber dank der grafischen Oberfläche trotzdem einfach zu bedienendes Verschlüsselungswerkzeug. Jeder kann diese Open-Source-Verschlüsselungssoftware kostenlos benutzen.

Zudem bietet es den großen Vorteil, dass es den plattformübergreifenden Austausch verschlüsselter Dateien ermöglichst. Dies ist in heterogenen Umgebungen extrem wichtig.

Dr. Rainer W. Gerling

Rainer W. Gerling ist Datenschutz- und IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München.

GPL – GNU General Public License

GNU ist ein Projekt der Free Software Foundation (FSF) zur Entwicklung eines freien Betriebssystems. Der Name ist ein rekursives Akronym von „GNU's Not UNIX“. Am bekanntesten ist die von der FSF herausgegebene Lizenz für freie Software. Die GPL gewährt die folgenden vier Freiheiten:

- Das Programm darf ohne Einschränkung für jeden Zweck, kommerzielle eingeschlossen, genutzt werden.
- Kopien des Programms dürfen kostenlos oder gegen Entgelt verteilt werden, wobei der Quellcode mitverteilt oder dem Empfänger des Programms auf Anfrage zum Selbstkostenpreis zur Verfügung gestellt werden muss. Dem Empfänger müssen dieselben Freiheiten gewährt werden.
- Die Arbeitsweise eines Programms darf studiert und individuell angepasst werden.
- Es dürfen auch die gemäß Freiheit 3 veränderten Versionen des Programms unter den Regeln von Freiheit 2 vertrieben werden, wobei dem Empfänger des Programms der Quellcode der veränderten Version verfügbar gemacht werden muss. Veränderte Versionen müssen nicht veröffentlicht werden.