Gemeinde
Riehen

IT Riehen

Datei-Anhänge verschlüsselt per Mail versenden.

21.05.2014 / T. Frey

Inhalt

1 Umgang mit sensiblen Informationen in Mails

1.1 Wann muss ich Anhänge verschlüsseln?

Die Datenschutzrichtlinien zum Umgang mit Personalinformationen in der Gemeinde Riehen enthält folgenden Absatz:

„Sensible Daten dürfen nicht per Mail versendet werden."

Beispiele für sensible Daten sind:

- Informationen betr. Sozialhilfe- oder EL-Bezügerinnen und –Bezüger
- Informationen betr. Mitarbeitenden
- Informationen betr. Schülerinnen und Schülern
- Informationen betr. Rekurrentinnen und Rekurrenten
- Informationen betr. Steuerpflichtige
- usw.

Besteht dennoch die betriebliche Notwendigkeit, sensible Daten per Mail zu versenden, sind folgende Punkte zu beachten:

- Betreff, Textkörper und die Dateinamen von Anhängen der Mail dürfen keine Rückschlüsse auf Inhalt oder Natur der enthaltenen Daten zulassen.
- Sensible Daten dürfen nur im Anhang enthalten sein.
- **Anhänge mit sensiblen Daten müssen verschlüsselt werden!**

1.2 Wie funktioniert die Verschlüsselung?

Zwar gibt es Möglichkeiten, Mails komplett zu verschlüsseln so dass weder Textkörper noch Anhänge von einem unbefugten eingesehen werden können, doch sind diese aufwändig zu realisieren und setzen nebst technischem Know-how auch ein Grundverständnis für asymmetrische Verschlüsselung auf Seiten des Senders wie auch auf Seiten des Empfängers voraus. Aus diesem Grund beschränkt sich die von der Verwaltung eingesetzte Methodik auf die Verschlüsselung von Dateianhängen. Da das Betriebssystem Windows selbst über keine entsprechende Funktionalität verfügt, ist dafür eine zusätzliche Software nötig.

1.2.1 Software *AES Crypt*

Mit *AES Crypt* steht eine Open Source Anwendung zur Verfügung, welche privat wie auch kommerziell kostenlos eingesetzt werden kann um einzelne Dateien zu verschlüsseln. Ob es sich dabei im Office-, PDF- oder sonstige Dokumente handelt, spielt dabei keine Rolle.

Die Software wird nicht nur zum verschlüsseln der Datei benötigt. Auch auf Seiten des Empfängers muss die Software installiert werden, damit die Datei wieder entschlüsselt werden kann. *AES Crypt* steht für Windows, MacOS, Linux, Android und iOS zur Verfügung.

1.2.2 Grad des Schutzes

AES Crypt verwendet den Verschlüsselungs-Standard AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit und gilt zum jetzigen Zeitpunkt als ausreichend sicher. AES wird u.a. auch zur Verschlüsselung von WLANs und in der IP-Telefonie verwendet.

1.3 Was bedeutet dies für meine Arbeit?

Der Einsatz von verschlüsselten Dateianhängen beim Mailversandt hat primär zwei folgen:

- Dem Empfänger muss das Kennwort zum entschlüsseln mitgeteilt werden.
- Der Empfänger muss ebenfalls über die entsprechende Software (*AES Crypt*) verfügen.

1.3.1 Mitteilung des Kennworts

Das Kennwort muss separat mitgeteilt werden, darf ich also nicht im selben Mail wie der verschlüsselte Anhang sichtbar sein. Grundsätzlich ist auch die Mitteilung des Kennworts in einer separaten Mail als unzureichend anzusehen, da davon ausgegangen werden muss, dass ein Angreifer, der eine Mail abzufangen vermag, auch an die zweite Mail gelangen wird. Kennwörter sollten deshalb über ein anderes Medium (Telefon, Postweg, SMS) mitgeteilt werden.

1.3.2 Software Installation

Es ist davon auszugehen, dass die wenigsten Empfänger bereits die benötigte Software installiert haben. Es ist deshalb sinnvoll, Mails mit verschlüsselten Anhängen mit einem entsprechenden Hinweistext, z.B. in der Signatur, zu ergänzen. Ein möglicher Wortlaut wäre:

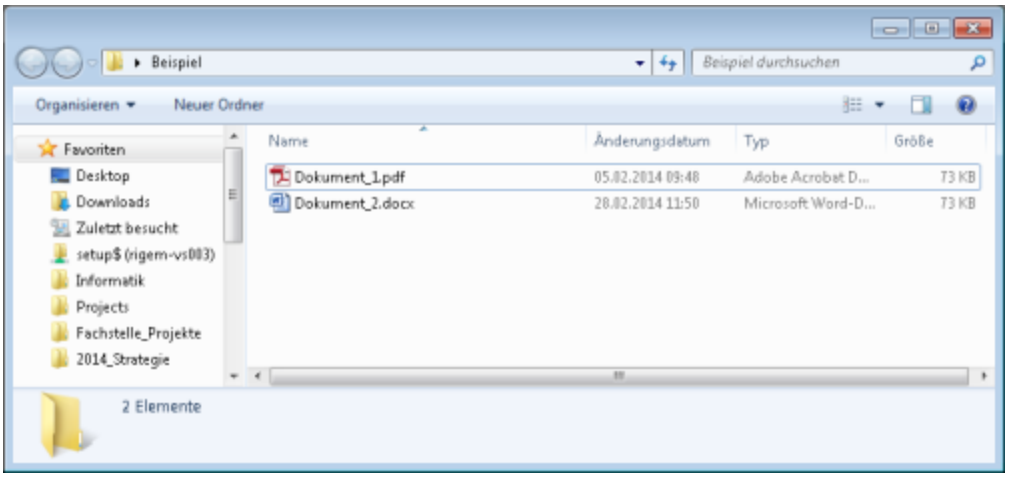
> „HINWEIS: Der Anhang dieser Mail ist zum Schutz ihrer persönlichen Daten mit einem Kennwort geschützt. Zum öffnen der Datei benötigen Sie die Software AES Crypt. Sollte Ihnen das Kennwort noch nicht mitgeteilt worden sein, kontaktieren Sie bitte den Absender telefonisch.“

1.4 Was, wenn ich meinen Gegenüber damit überfordere?

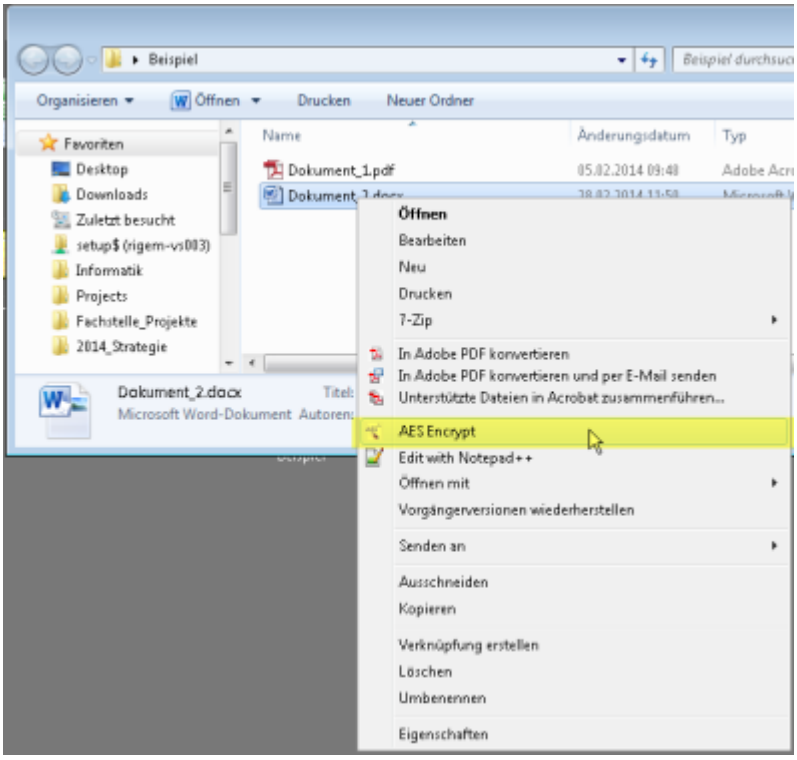
Hat der Empfänger keine Möglichkeit, die benötigte Software zu installieren, lehnt dies grundsätzlich ab oder scheitert bei der Verwendung der Software, ist auf den Versandt sensibler Daten per Mail zu verzichten und es müssen alternative Kanäle (Telefon, Postweg) verwendet werden.

2 Schritt-für-Schritt Anleitung

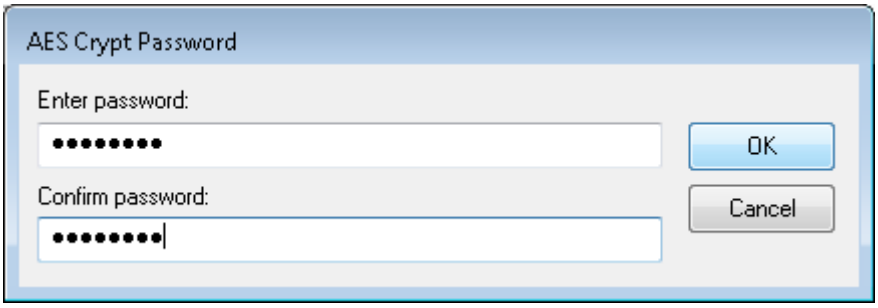
2.1 Verschlüsseln einer Datei



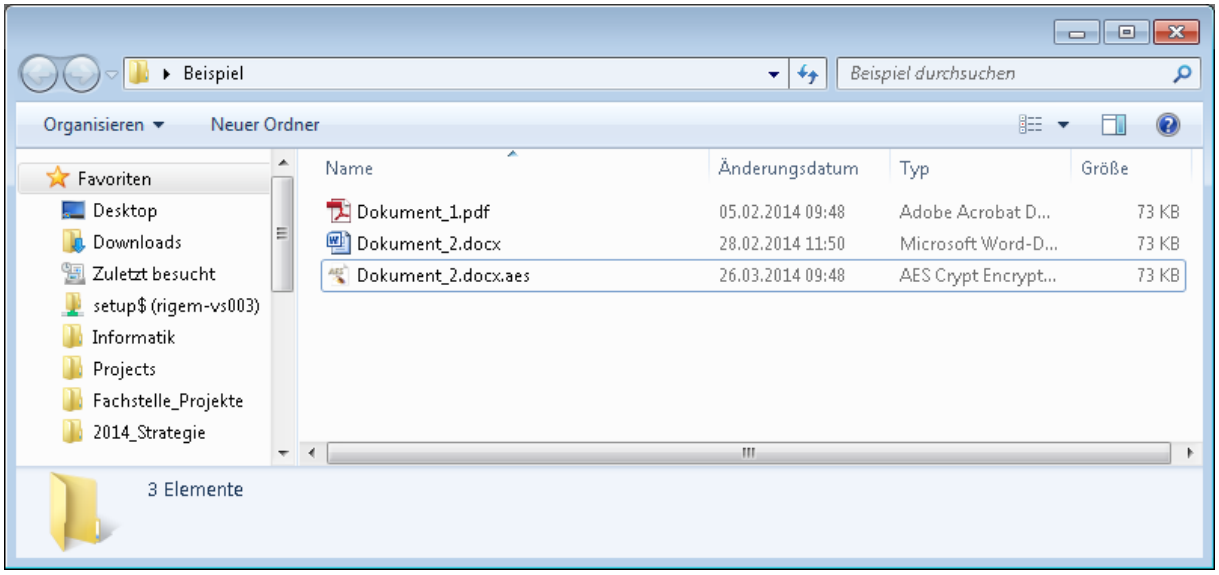
Markieren sie die zu verschlüsselnde Datei. Es können auch mehrere Dateien gleichzeitig ausgewählt werden.



Rufen Sie mit der rechten Maustaste das Kontextmenü der markierten Datei auf und wählen Sie den Menüpunkt *AES Encrypt*.



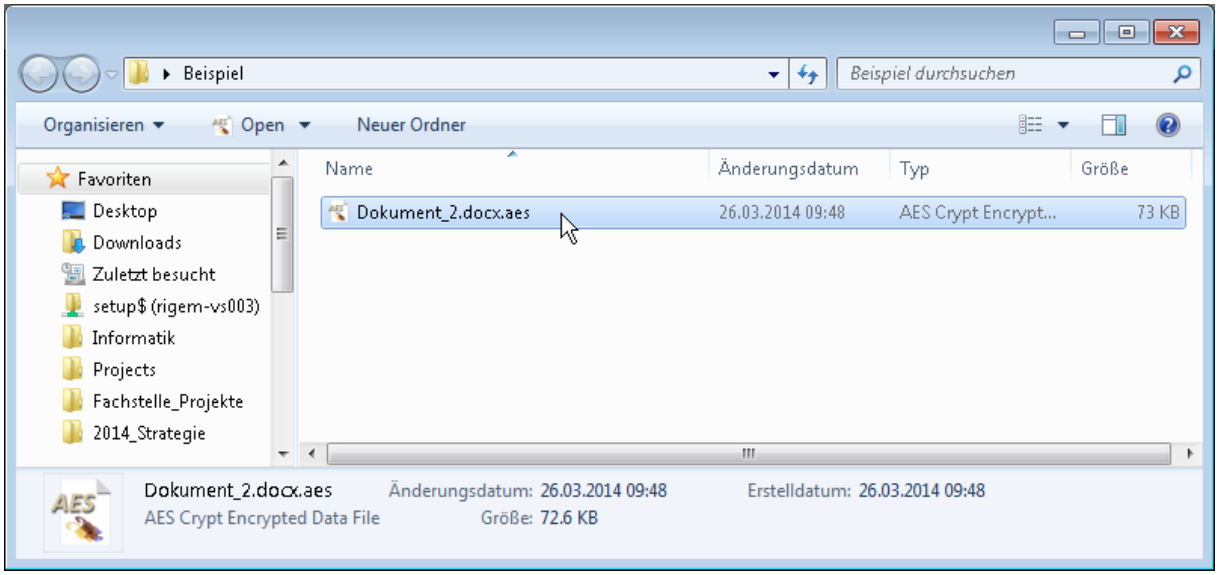
Es erscheint ein Dialogfenster in welchem Sie das Kennwort für die Datei festlegen (muss zweimal eingegeben werden). Grundsätzlich sollte das Kennwort mindestens 8 Zeichen umfassen und aus Ziffern, Klein- sowie Grossbuchstaben bestehen. Denke Sie daran, sich das Kennwort zu notieren, da Sie es dem Empfänger mitteilen müssen.



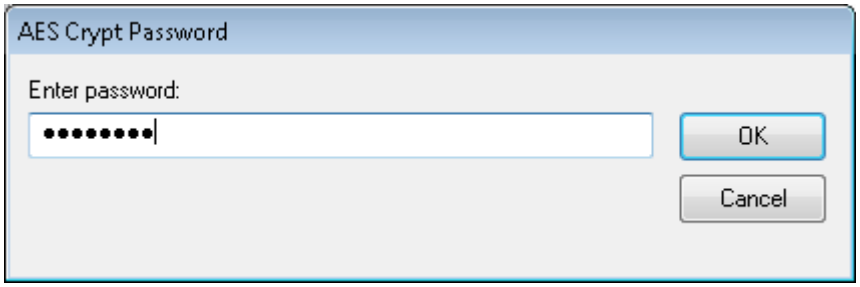
Die verschlüsselte Datei wird unter demselben Dateinamen wie die Ursprungsdatei erstellt, jedoch mit der zusätzlichen Dateiendung .aes versehen. Die Ursprungsdatei bleibt in unverschlüsselter Form erhalten.

Die verschlüsselte Datei (Dateiendung .aes) können Sie nun per Mail versenden. Denken Sie bitte daran, dem Empfänger vorgängig das zur Entschlüsselung benötigte Kennwort mitzuteilen.

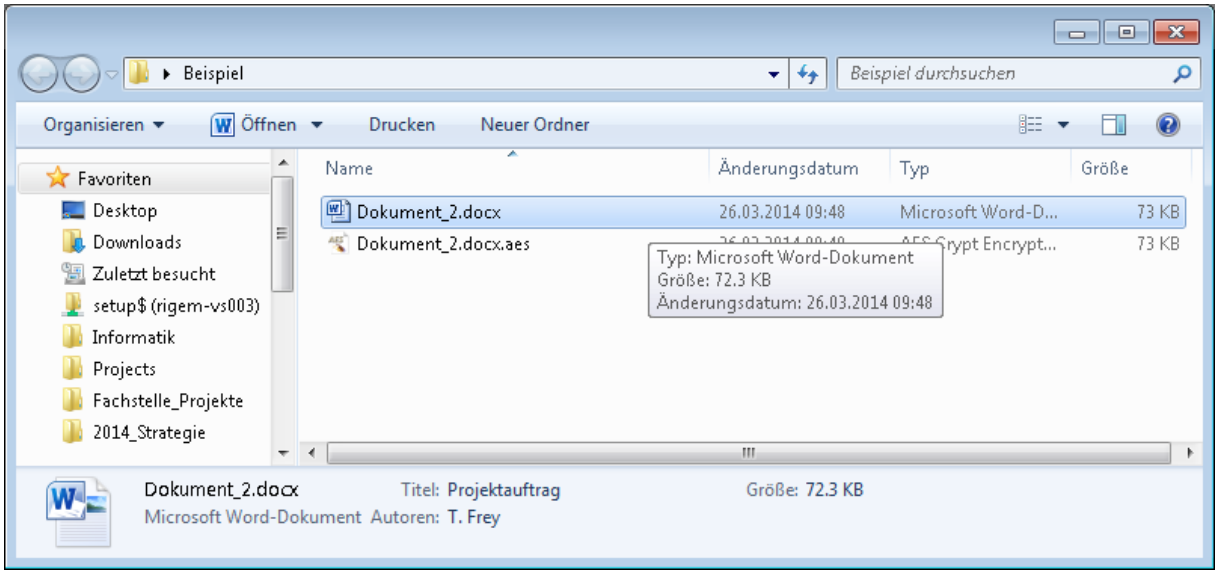
2.2 Entschlüsseln einer bereits verschlüsselten Datei



Bitte beachten Sie, dass die entschlüsselte Datei im selben Verzeichnis wie die verschlüsselte Datei erstellt wird. Haben Sie die Datei per Mail erhalten, sollte diese vorgängig auf dem Desktop oder in einem Verzeichnis abgelegt werden. Um eine verschlüsselte Datei (Dateiendung .aes) zu entschlüsseln reicht ein Doppelklick zum Öffnen der Datei.



Im erscheinenden Dialog muss das Kennwort, welches Ihnen von der Person, welche die Datei verschlüsselt hat, mitgeteilt werden muss, eingegeben werden.



Die entschlüsselte Datei wird nun erstellt. Die verschlüsselte Datei bleibt dabei erhalten und muss, sofern sie nicht mehr benötigt wird, von Hand gelöscht werden.

2.3 Installation der Software auf einem privaten Computer

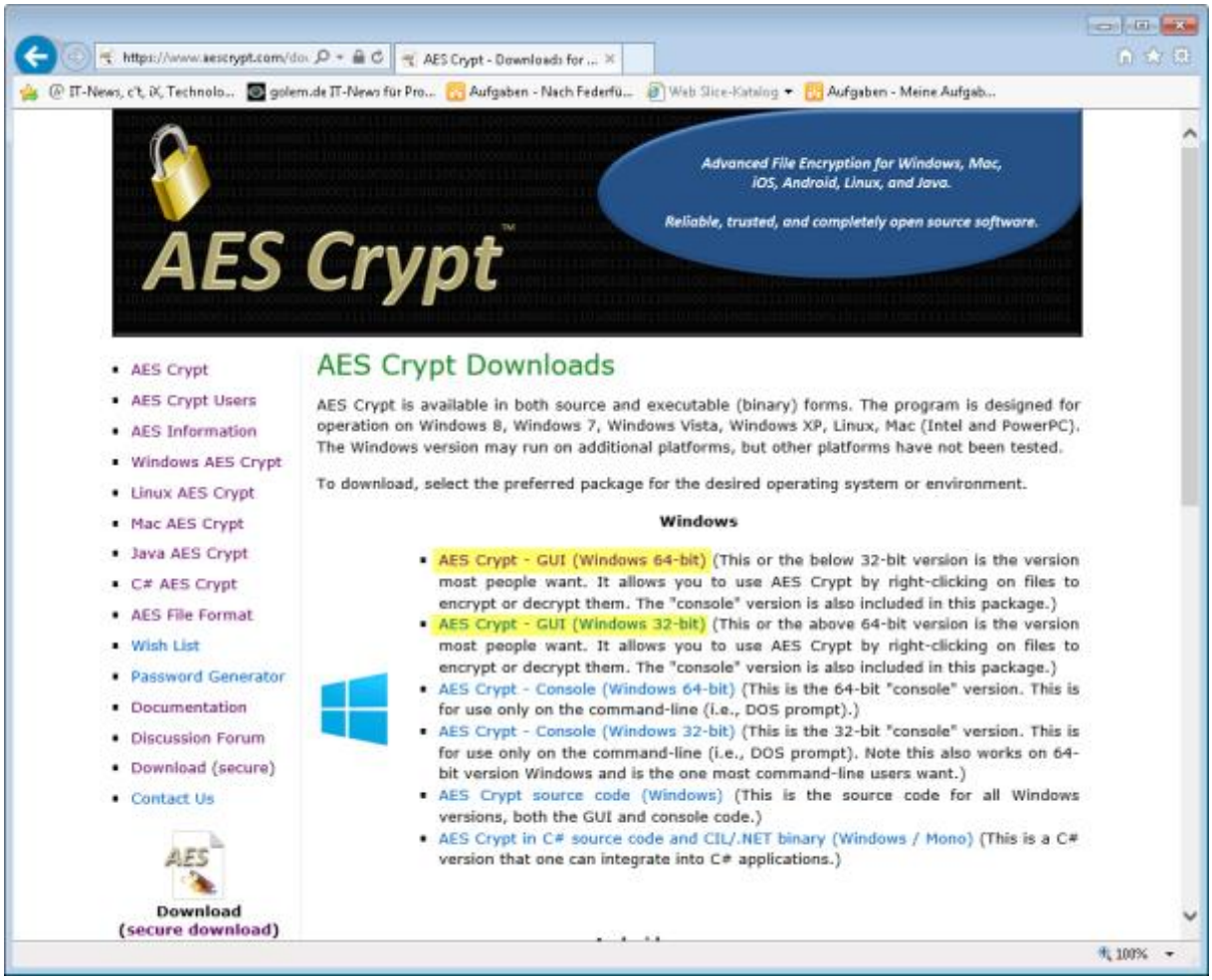
Die benötigte Software *AES Crypt* ist in der Gemeindeverwaltung bereits installiert!

Dieser Absatz behandelt die Installation der Software auf einem privaten Computer um beispielsweise den sicheren Dateiaustausch zu gewährleisten, wenn Sie sensible Daten zuhause weiterbearbeiten müssen.

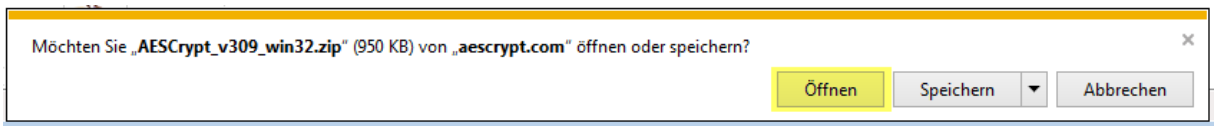
Wenn Sie regelmässig sensible Daten von Zuhause aus bearbeiten müssen, wird stattdessen der Einsatz von *RemoteBS* empfohlen. Für weitere diesbezügliche Auskünfte kontaktieren Sie bitte das IT Service Desk der Gemeindeverwaltung.

Die Software kann kostenlos von der Webseite http://www.aescrypt.com/ heruntergeladen werden.

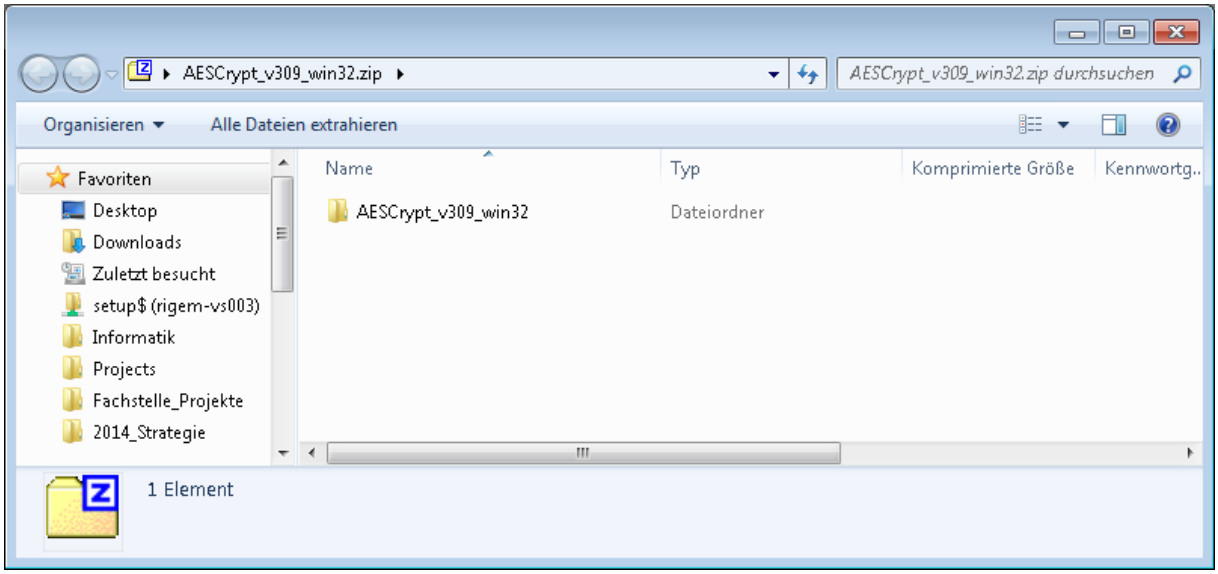
Klicken Sie auf der Website auf den Link „*secure download*“ unterhalb des Menüs.



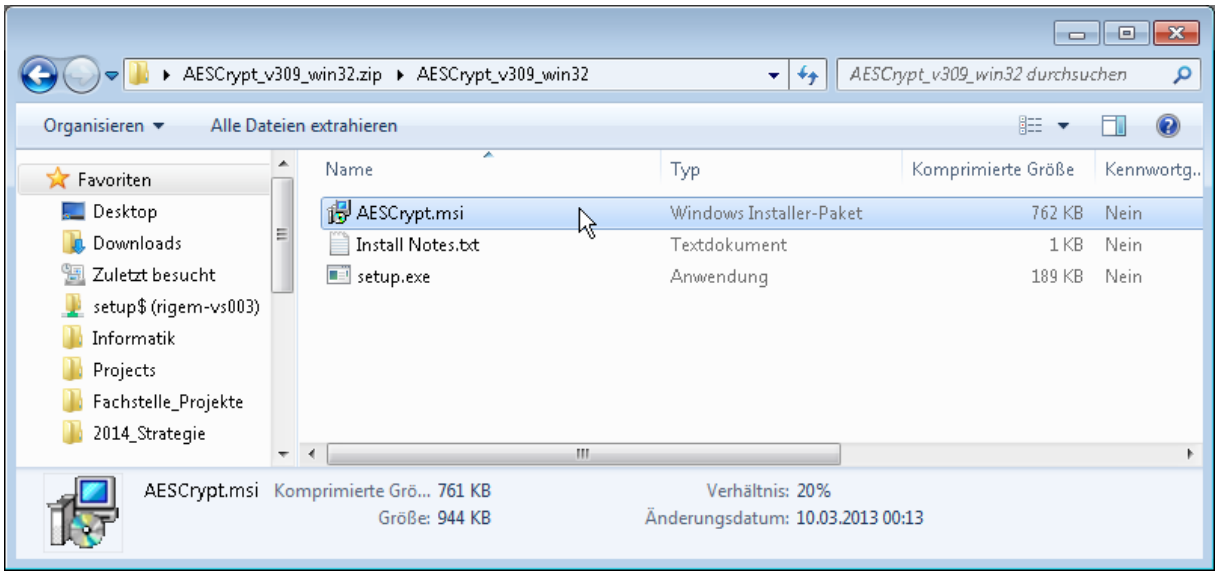
Die Software steht für diverse Betriebssysteme zur Verfügung. Verwenden Sie zuhause Windows muss *AES Crypt – GUI* heruntergeladen werden. Sind Sie nicht sich, ob Sie zuhause ein 64-Bit oder ein 32-Bit Windows einsetzen, wählen Sie den Download *AES Crypt – GUI (Windows 32-bit)*.



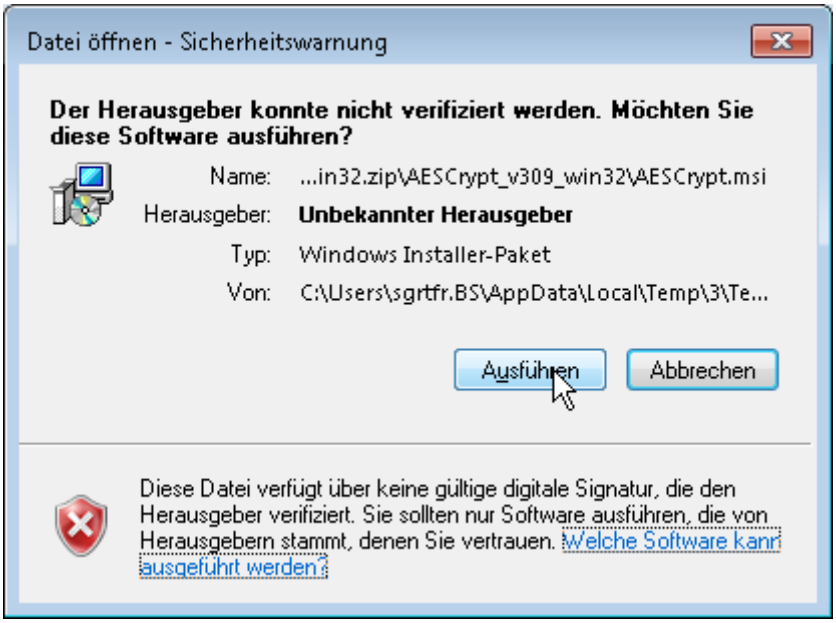
Je nach verwendetem Browser (oberes Bild stammt vom Internet Explorer 11) erscheint die Download-Aufforderung. Die Installationsdatei kann direkt geöffnet/ausgeführt oder auch zuerst lokal abgespeichert und dann geöffnet werden.



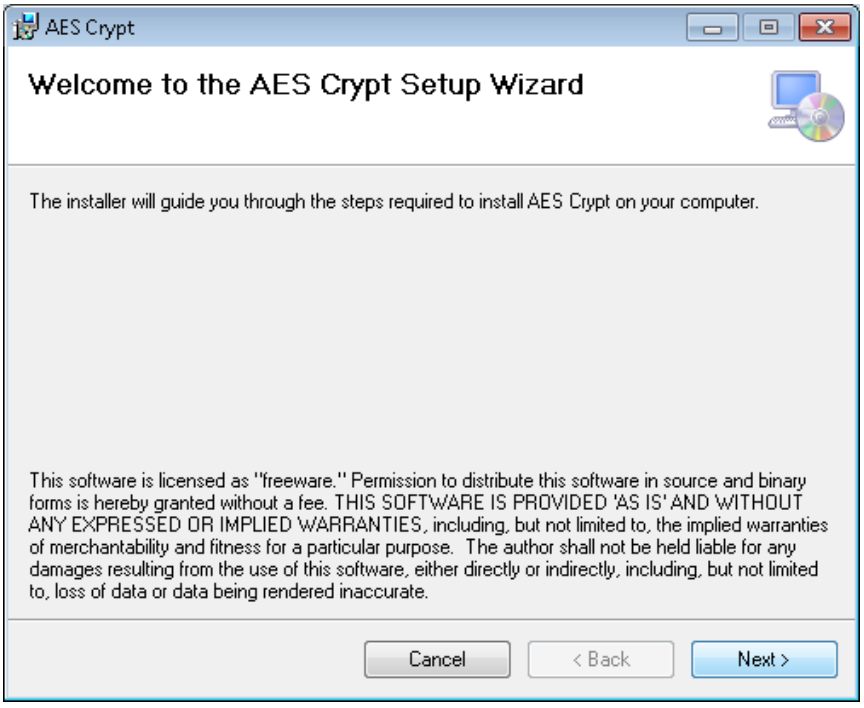
Die Installationsdatei ist ein Zip-Archiv und enthält mehrere Dateien. Öffnen Sie das Verzeichnis *AESCrypt_v309_win32*.



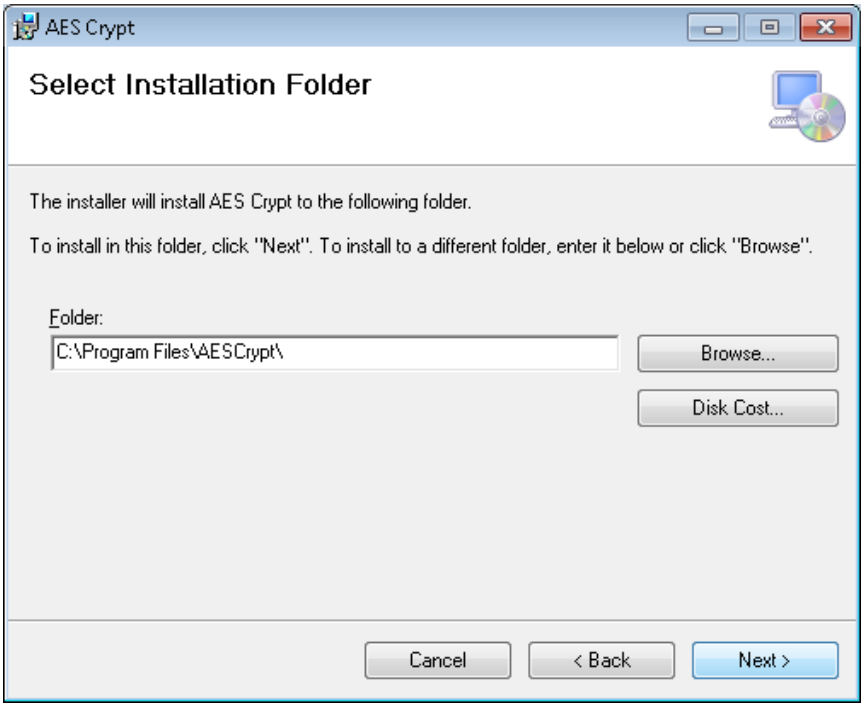
Öffnen Sie nun die Datei *AESCrypt.msi* um mit der Installation zu beginnen.



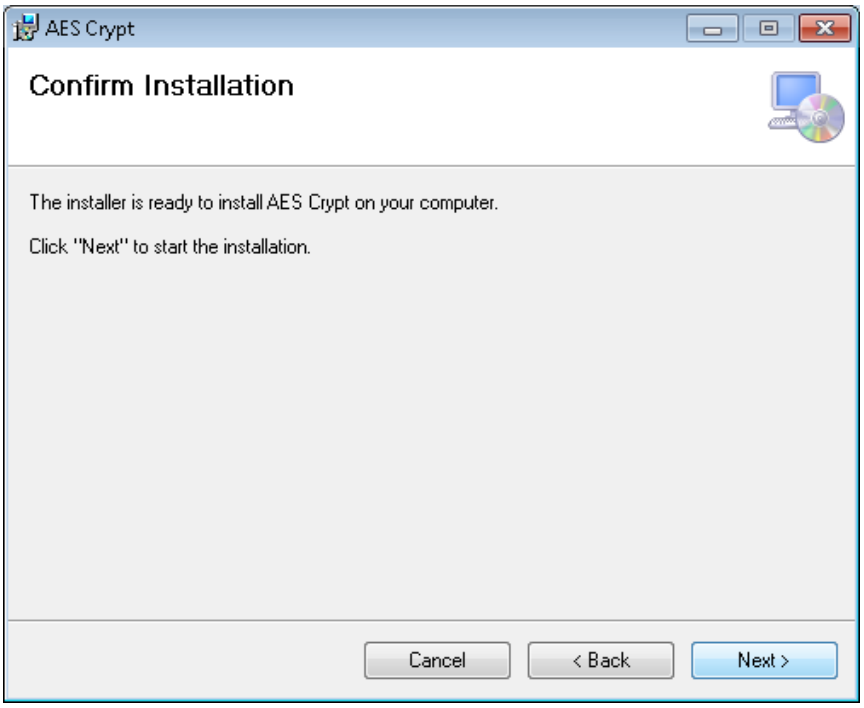
Je nach Version ihres Betriebssystems erscheint ein Sicherheitshinweis, in welchem Sie das Öffnen der Datei nochmals bestätigen.



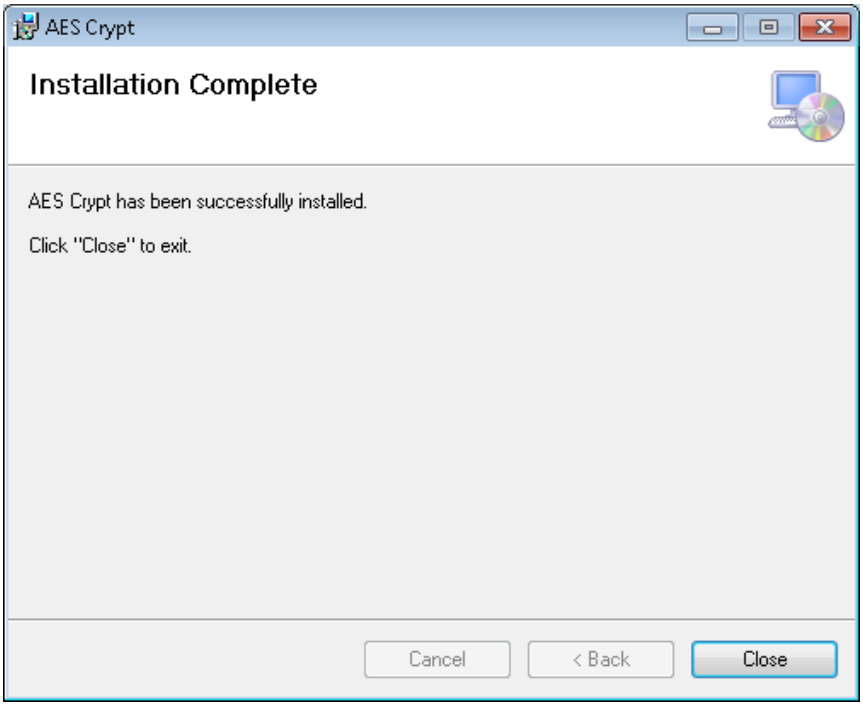
Es erscheint ein Fenster mit Hinweisen zur Lizenz. Bestätigen diesen mit Klick auf *Next*.



Im nächsten Schritt, können Sie den Installationspfad anpassen. Möchten Sie den Standardpfad verwenden (empfohlen), brauchen Sie lediglich mit einem weiteren Klick auf *Next* zu bestätigen.



Die Installation ist nun bereit. Bestätigen Sie mit Klick auf *Next*.



Nach erfolgreicher Installation können Sie das Installationsprogramm mit Klick auf *Close* schliessen. *AES Crypt* kann nun verwendet werden. Die heruntergeladene Installationsdatei benötigen Sie nun nicht mehr und können diese löschen.