GPacker (Version 4.0.0)

Für alle Anwender, die händisch die Verschlüsselung durchführen müssen, stellt der GPacker mit seiner grafischen Oberfläche eine interaktive Alternative zur Verwendung der Programme XPacker und TPacker dar. Die beiden Programme werden nicht benötigt, wenn der GPacker eingesetzt wird.

Er ermöglicht mit Hilfe einer grafischen Oberfläche die Verschlüsselung und Komprimierung von QS-Dateien im XML-Format, die im Rahmen der Qesü-RL oder QSKH-RL erstellt worden sind.

Hinweis:
In diesem Dokument befinden sich mehrere Screenshots auf denen noch Version 3.0.0 abgebildet ist. Da es keine Änderungen an der Oberfläche im Versionsverlauf gab, haben diese weiterhin Gültigkeit.

Voraussetzungen

Das Programm setzt die Installation von Java 6 oder höherer Versionen voraus. Ferner werden – je nach Aktion – „private“ oder „öffentliche Schlüssel“ benötigt. Diese werden im folgenden Abschnitt erklärt.

Hintergrund der Verschlüsselung

Für die Ver- und Entschlüsselung werden sogenannte Schlüssel benötigt. Diese Schlüssel bestehen aus langen Zeichenketten und werden daher in Dateien abgelegt. Da nun mehrere Organisationen diese Dateien, aber nicht jede Organisation alle Daten darin sehen/lesen darf, werden Schlüsselpaare eingesetzt. Jedes Schlüsselpaar besteht aus zwei unterschiedlichen Typen von Schlüsseln:

- **Private Schlüssel:**
  Der eigene private Schlüssel darf niemals dem Kommunikationspartner gegeben werden.
- **Öffentlicher Schlüssel:**
  Nur der öffentliche Schlüssel darf dem Kommunikationspartner gegeben werden.

Wenn nun Daten des Absenders A für verschiedene Empfänger (E_1, E_2, usw.) verschlüsselt werden sollen, so benötigt man die öffentlichen Schlüssel von E_1 und E_2 zum Verschlüsseln der Daten von A: Der Bereich der nur für E_1 ist, wird mit dessen öffentlichem Schlüssel chiffriert. Analog mit dem Bereich für E_2 usw.

Wenn nun E_1 die Daten erhält, kann E_1 mit seinem eigenen privaten Schlüssel die für ihn bestimmten Daten entschlüsseln. Er kann nicht die für E_2 bestimmten Daten entschlüsseln.

Dieses Verfahren wird auch in der Qualitätssicherung eingesetzt. Die Leistungserbringer verschlüsseln Daten mit verschiedenen öffentlichen Schlüsseln der Empfänger, welche dann nur die für sie bestimmten Daten entschlüsseln und verarbeiten können.

Wichtige Hinweise

- Beim Verschlüsseln nur den öffentlichen Schlüssel des Empfängers einsetzen
- Beim Entschlüsseln nur den eigenen privaten Schlüssel einsetzen
- Niemals den eigenen privaten Schlüssel an Dritte geben
- Nur öffentliche Schlüssel an Dritte geben
- Die Schlüssel werden folgendermaßen bezeichnet:
  - Privater Schlüssel → Englisch: Private Key → Dateiendung: *.pri
  - Öffentlicher Schlüssel → Englisch: Public Key →Dateiendung: *.pub
- Die Bereiche, die unterschiedlich verschlüsselt werden müssen, werden auch als „Elemente“ in der Anwendung bezeichnet. Sie befinden sich rechts oben (siehe *Abbildung 2*).
- Wenn **Datei (.zip.aes)** ausgewählt wird, wird je nach ausgewählter Aktion die Datei für den Transport verschlüsselt bzw. aus dem Transportarchiv entschlüsselt.

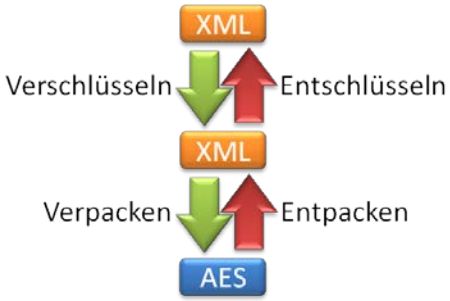

Abbildung 1 Ver- Entschlüsseln und Ver- Entpacken.

- Das AQUA-Institut sammelt die öffentlichen Schlüssel der Datenservices der Beteiligten und stellt diese unter http://www.sqg.de/datenservice/spezifikationen-downloads/verfahrensjahr-<Verfahrensjahr>/xml_datenservices.html[1] zur Verfügung.
- Im entpackten Archiv finden Sie die Schlüssel unter dem relativen Pfad: „\Verschlüsselungsprogramm\Schlüssel\“.

[1] <Verfahrensjahr> ist hierbei durch das aktuelle Verfahrensjahr – z.B. 2014 – zu ersetzen.

Datei-Formate und Prozesse

Grundsätzlich handelt es sich um XML-Dateien, welche vom Leistungserbringer erzeugt werden. Bevor diese jedoch zur Datenannahmestelle transportiert werden können, müssen sie aus Datenschutzgründen bearbeitet werden:

- Zum einen wird in den Dateien eine Verschlüsselung vorgenommen. Verschiedene Bereiche/Elemente werden – wie zuvor beschrieben – mit den öffentlichen Schlüsseln der Empfänger chiffriert. Obwohl sich alle Informationen für alle Beteiligten innerhalb einer XML-Datei befinden, ist sichergestellt, dass Unbefugte diese Bereiche/Elemente nicht einsehen können – wohl aber der Empfänger, der die Dateien mit seinem privaten Schlüssel dechiffriert. Dieser Schritt ist nur notwendig, wenn in der Datei dokumentierte QS-Fälle mit patientenidentifizierenden Daten (PID) enthalten sind.

  Wichtig:

  - Sind keine QS-Daten in der Datei enthalten (wie z.B. bei Sollstatistiken oder Protokollen), kann dieser Schritt übersprungen werden.
  - Vor und nach der Chiffrierung/Dechiffrierung handelt es sich immer um XML-Dateien.

- Zusätzlich wird die Datei noch für den Transport per Email „verpackt“. Hierbei wird die Gesamtdatei mit einem symmetrischen Verfahren verschlüsselt. Dazu werden die Registrierungsnummer und das Transport-Passwort benötigt, welches der Absender im Zuge der Registrierung beim Empfänger erhalten hat.

  Wichtig:

  - Dieser Schritt ist immer auszuführen, wenn Dateien per Internet oder auf anderen unsicheren Kanälen transportiert werden.
  - Die verpackten Dateien werden im binären AES-Format gespeichert, welches eine sichere Verpackung auf unsicheren Wegen darstellt.

Programmablauf

Die folgenden Szenarien beschreiben den korrekten Ablauf zur Nutzung des GPackers aus Sicht eines Leistungserbringers.

Szenario 1 – Versand von QS-Daten

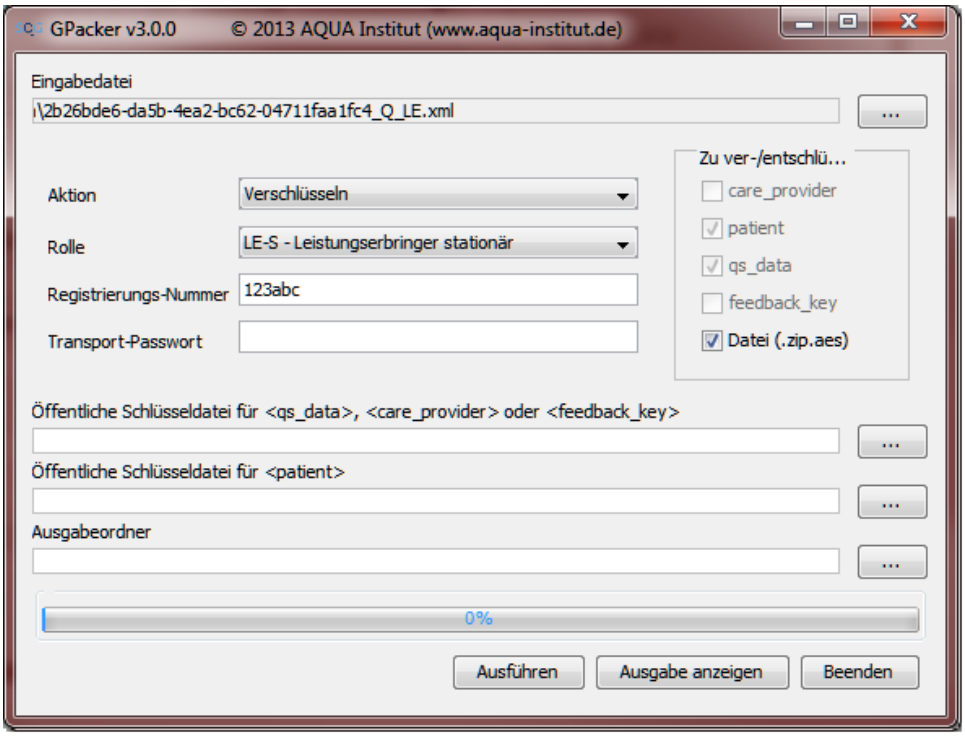

Abbildung 2 Szenario 1 – Versand von QS-Daten

1. Wählen Sie über die Schaltfläche für „Eingabedatei“ eine XML-Export-Datei aus, wie sie aus dem QS-Dokumentationsprogramm exportiert wird.
2. Wählen Sie im Drop-down-Menü „Rolle“ den „LE-Leistungserbringer stationär oder „LE-Leistungserbringer ambulant“ aus.
3. Aktivieren Sie rechts unter „zu ver-/entschlüsseln“ die Checkbox „Datei (.zip.aes)“.
4. Setzen Sie im Textfeld „Transport-Passwort“ das für Ihre Registrierung ausgetauschte, geheime Passwort ein.
5. Wählen Sie über die Schaltfläche für „Private Schlüsseldatei für <qs_data>, <care_provider> oder <feedback_key>“ den öffentlichen Schlüssel Ihrer Datenannahmestelle aus.
6. Wählen Sie über die Schaltfläche für „Private Schlüsseldatei für <patient>“ den öffentlichen Schlüssel Ihrer Vertrauensstelle aus.
7. Wählen Sie den Ausgabeordner über die entsprechende Schaltfläche aus.
8. Klicken Sie auf die Schaltfläche „Ausführen“.

Szenario 2 – Empfang des Rückprotokolls

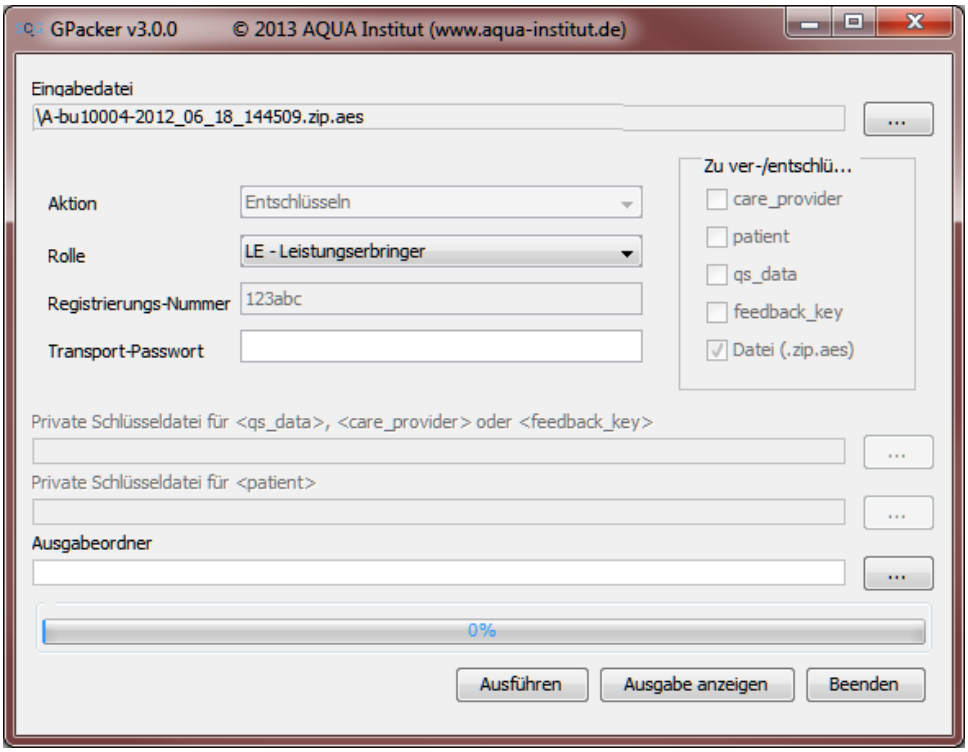

Abbildung 3 Szenario 2 – Empfang des Rückprotokolls

1. Wählen Sie über die Schaltfläche für „Eingabedatei“ eine Eingabedatei aus, wie sie von der Datenannahmestelle als Datenflussprotokoll verschickt wird.
2. Wählen Sie im Drop-down-Menü „Rolle“ den „LE-Leistungserbringer“ aus.
3. Setzen Sie im Textfeld „Transport-Passwort“ das für Ihre Registrierung ausgetauschte, geheime Passwort ein.
4. Wählen Sie den Ausgabeordner über die Schaltfläche „Ausgabeordner“ aus.
5. Klicken Sie auf die Schaltfläche „Ausführen“.

Die angestoßene Entschlüsselung kann, je nach Größe der Datei und Geschwindigkeit Ihres Rechners, mehrere Minuten dauern. Wenn das Entschlüsseln abgeschlossen ist, wird dieses in der Oberfläche dargestellt.

Sonderfälle bei Datenlieferungen

Wenn im GPacker keine Rolle ausgewählt wird, so kann der Anwender das Tool erweitert nutzen: Die Elemente (siehe *Abbildung 4*) können dann einzeln angewählt werden, wenn eine Aktion mit Ver-/Entschlüsseln gewählt wurde. Dieser Expertenmodus ist nur für erfahrende Anwender geeignet.

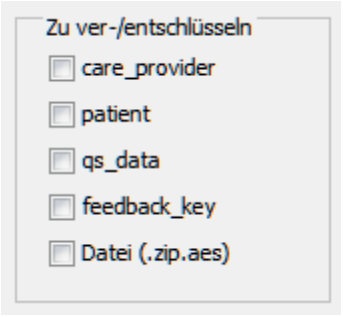

Abbildung 4 Auswahl der zu verschlüsselnden Elemente

Im folgenden Abschnitt wird die Nutzung des GPackers für verschiedene Rollen und Ereignisse in Form von Anwendungsbeispielen dargestellt. Anschließend werden die Aktionen fachlich beschrieben.

Anwendungsbeispiele

Die folgenden Anwendungsbeispiele sollen häufige Szenarien aus dem Alltag der Beteiligten im Datenfluss wiedergeben. Die Fälle sind gruppiert nach der Rolle des Anwenders.

- **Leistungserbringer (Kliniken/Praxen)**

  - QS-Daten wurden mit dem KIS[2] oder PVS[3] erstellt und sollen nun an die Datenannahmestelle verschickt werden.
  - Im GPacker muss folgende Aktion in den entsprechenden Tabellen ausgewählt werden:

	Stationär		**Ambulant**	
Aktion	„Verschlüsseln“			
Elemente	**Name**	**Öffentl. Schlüssel**	**Name**	**Öffentl. Schlüssel**
	qs_data	Datenannahmestelle	qs_data feedback_key	Bundesauswertungstelle
	patient	Vertrauensstelle	patient	Vertrauensstelle
Option „Datei (.zip.aes)“	gesetzt			

  - **Beispiel 1**
    Der Anwender ist im stationären Sektor tätig. Er muss die Elemente qs_data und patient auswählen und diese mit dem öffentlichen Schlüssel der Datenannahmestelle (qs_data) und der Vertrauensstelle (patient) verschlüsseln.
  - **Beipiel 2**
    Der Anwender ist im ambulanten Sektor tätig. Er muss die Elemente qs_data, feedback_key und patient auswählen und diese mit den öffentlichen Schlüsseln der Bundesauswertungsstelle (qs_data, feedback_key) und der Vertrauensstelle (patient) verschlüsseln.
    ➔ Siehe unten: „Aktionen - Verschlüsseln mit Auswahl-Option ‚Datei (.zip.aes)‘ und weiteren Elementen“
  - Die QS-Sollstatistik wurde mit dem KIS oder PVS erstellt und soll nun an die Datenannahmestelle verschickt werden.
    ➔ Siehe unten: „Aktionen - Verschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“

    Die Empfangsbestätigung oder das Datenflussprotokoll wurde zur Verfügung gestellt und muss nun entpackt werden.
    ➔ Siehe unten: „Aktionen - Verschlüsseln nur mi Auswahl-Option ‚Datei (.zip.aes)‘“

[2] KIS = Krankenhaus-Informations-System
[3] PVS=Praxis-Verwaltungs-System

- **Datenannahmestellen**

  - QS-Paket aus dem stationären Bereich bearbeiten:
    ➔ Siehe unten, „Aktionen“: „Verschlüsseln mit Auswahl-Option ‚Datei (.zip.aes)‘ und weiteren Elementen“ mit dem Element „qs_data“. Dabei bitte eigenen, privaten Schlüssel verwenden.
  - QS-Paket aus dem ambulanten Bereich bearbeiten:
    ➔ Siehe unten, „Aktionen“: „Verschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“
  - Qs-Daten aus dem stationären Sektor zur Weiterleitung an die Vertrauensstelle verschlüsseln und verpacken.
    ➔ Siehe unten, „Aktionen“ „Verschlüsseln mit Auswahl-Option ‚Datei (.zip.aes)‘ und weiteren Elementen“ mit den Elementen „qs_data“ + „care_provider“. Dabei öffentlichen Schlüssel der Bundesauswertungsstelle verwenden.
  - QS-Daten aus dem ambulanten Sektor zur Weiterleitung an die Vertrauensstelle verschlüsseln und verpacken.
    ➔ Sie unten, „Aktionen“: „Verschlüsseln mit Auswahl-Option ‚Datei (.zip.aes) und weiteren Elementen“ mit dem Element „care_provider“. Dabei öffentlichen Schlüssel der Bundesauswertungsstelle verwenden.
  - Sollstatistik entschlüsseln
    ➔ Siehe unten, „Aktionen“: „Entschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“
  - Sollstatistik zur Weiterleitung an Bundesauswertungsstelle verschlüsseln.
    ➔ Siehe unten, „Aktionen“: „Verschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“
  - Datenflussprotokoll der Bundesauswertungsstelle entschlüsseln.
    ➔ Siehe unten, „Aktionen“: „Entschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“
  - Datenflussprotokoll der Bundesauswertungsstelle für den Leistungserbringer verschlüsseln.
    ➔ Siehe unten, „Aktionen“: „Verschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“
  - Empfangsbestätigung der Vertrauensstelle entschlüsseln.
    ➔ Siehe unten, „Aktionen“: „Entschlüsseln nur mit Auswahl-Option ‚Datei (.zip.aes)‘“

Aktionen

Verschlüsseln mit Auswahl-Option „Datei (.zip.aes)“ und weiteren Elementen

Feld	Beschreibung
Registrierungs-Nummer Transport-Passwort	Leistungserbringer: Geben Sie hier die Registriernummer und das Passwort an, welche Sie bei der Registrierung von der Datenannahmestelle erhalten haben. Datenannahmestelle: Geben Sie hier die Registriernummer und das Passwort an, welche Sie bei der Registrierung von der Bundesauswertungsstelle erhalten haben.
Elemente	Das Feld wird automatisch korrekt vorbelegt, wenn die gewählte Rolle des Anwenders korrekt selektiert wurde. Bei leerer Rolle gelangt der Anwender in den Expertenmodus und kann die Elemente selber wählen.
Eingabedatei	Wählen Sie hier die XML-Datei aus, die verschlüsselt werden soll.
Ausgabeordner	Der Ausgabeorder wird nach der Auswahl der Eingabedatei automatisch gefüllt, kann aber verändert werden. Hier wird die neue Datei abgelegt.
Öffentliche Schlüsseldatei der Datenannahmestelle oder der Vertrauensstelle oder der Bundesauswertungsstelle	Geben Sie hier den öffentlichen Schlüssel der entsprechenden Stelle ein. Die Dateiendung der öffentlichen Schlüssel ist „.pub“. Wenn Sie das AQUA-Schlüsselpaket einsetzen, heißt die Datei bei Datenannahmestellen „Pub_key_Datenannahmestelle_ <Ländercode>.pub“, sonst „Pub_key_<Stelle>.pub“.
Option „Datei (.zip.aes)	gesetzt

Entschlüsseln mit Auswahl-Option „Datei (.zip.aes)“ und weiteren Elementen

Feld	Beschreibung
Transport-Passwort	Leistungserbringer: Geben Sie hier das Passwort an, welche Sie bei der Registrierung von der Datenannahmestelle erhalten haben. Datenannahmestelle: Geben Sie hier das Passwort an, welche Sie bei der Registrierung von der Bundesauswertungsstelle erhalten haben.
Elemente	Das Feld wird automatisch korrekt vorbelegt, wenn die gewählte Rolle des Anwenders korrekt selektiert wurde. Bei leerer Rolle gelangt der Anwender in den Expertenmodus und kann die Elemente selber wählen.
Eingabedatei	Wählen Sie hier die .zip.aes-Datei (verschlüsselte XML-Datei) aus, die entschlüsselt werden soll.

Feld	Beschreibung
Ausgabeordner	Der Ausgabeorder wird nach der Auswahl der Eingabedatei automatisch gefüllt, kann aber verändert werden. Hier wird die neue Datei abgelegt.
Private Schlüsseldatei	Geben Sie hier Ihren privaten Schlüssel ein. Die Dateiendung Ihres Schlüssels ist „.pri“. Siehe auch Anwendungsfälle weiter oben.
Option „Datei (.zip.aes)	gesetzt

Verschlüsseln nur mit Auswahl-Option „Datei (.zip.aes)“

Feld	Beschreibung
Registrierungs-Nummer Transport-Passwort	Leistungserbringer: Geben Sie hier die Registriernummer und das Passwort an, welche Sie bei der Registrierung von der Datenannahmestelle erhalten haben. Datenannahmestelle: Geben Sie hier die Registriernummer und das Passwort an, welche Sie bei der Registrierung von der Bundesauswertungsstelle erhalten haben.
Eingabedatei	Wählen Sie hier die XML-Datei aus, die verschlüsselt werden soll.
Ausgabeordner	Der Ausgabeorder wird nach der Auswahl der Eingabedatei automatisch gefüllt, kann aber verändert werden. Hier wird die neue Datei abgelegt.
Option „Datei (.zip.aes)	gesetzt

Entschlüsseln nur mit Auswahl-Option „Datei (.zip.aes)“

Feld	Beschreibung
Transport-Passwort	Leistungserbringer: Geben Sie hier das Passwort an, welche Sie bei der Registrierung von der Datenannahmestelle erhalten haben. Datenannahmestelle: Geben Sie hier das Passwort an, welche Sie bei der Registrierung von der Bundesauswertungsstelle erhalten haben.
Eingabedatei	Wählen Sie hier die zip.aes-Datei aus, welche entschlüsselt werden soll.
Ausgabeordner	Der Ausgabeorder wird nach der Auswahl der Eingabedatei automatisch gefüllt, kann aber verändert werden. Hier wird die neue Datei abgelegt.
Option „Datei (.zip.aes)	gesetzt

Verschlüsseln ohne Auswahl-Option „Datei (.zip.aes)“

Feld	Beschreibung
Elemente	Das Feld wird automatisch korrekt vorbelegt, wenn die gewählte Rolle des Anwenders korrekt selektiert wurde. Bei leerer Rolle gelangt der Anwender in den Expertenmodus und kann die Elemente selber wählen.
Eingabedatei	Wählen Sie hier die XML-Datei aus, die verschlüsselt werden soll.
Ausgabedatei	Die Ausgabedatei wird nach der Auswahl der Eingabedatei automatisch gefüllt, kann aber verändert werden. Unter diesem Pfad und Namen wird die neue Datei abgelegt.
Öffentliche Schlüsseldatei der Datenannahmestelle oder der Vertrauensstelle oder der Bundesauswertungsstelle	Geben Sie hier den öffentlichen Schlüssel der entsprechenden Selle ein. Die Dateiendung der öffentlichen Schlüssel ist „.pub“. Wenn Sie das AQUA-Schlüsselpaket einsetzen sollten, heißt die Datei bei Datenannahmesstellen „Pub_key_Datenannahmestelle_ <Ländercode>.pub“, sonst „Pub_key_<Stelle>.pub“
Option „Datei (.zip.aes)	nicht gesetzt

Entschlüsseln ohne Auswahl-Option „Datei (.zip.aes)“

Feld	Beschreibung
Elemente	Das Feld wird automatisch korrekt vorbelegt, wenn die gewählte Rolle des Anwenders korrekt selektiert wurde. Bei leerer Rolle gelangt der Anwender in den Expertenmodus und kann die Elemente selber wählen.
Eingabedatei	Wählen Sie hier XML-Datei aus, die entschlüsselt werden soll.
Ausgabedatei	Die Ausgabedatei wird nach der Auswahl der Eingabedatei automatisch gefüllt und kann trotzdem verändert werden. Unter diesem Pfad und Namen wird die neue Datei abgelegt.
Private Schlüsseldatei	Geben Sie hier Ihren privaten Schlüssel ein. Die Dateiendung der Ihres Schlüssels ist „.pri“. Siehe auch Anwendungsfälle weiter oben.
Option „Datei (.zip.aes)	nicht gesetzt

Fehlermeldungen

Meldung	Erläuterung
Es konnten keine temporären Dateien erstellt werden!	Es wurde kein Ordner zur Erzeugung temporärer Dateien gefunden.
Die Eingabedatei konnte nicht gefunden werden!	Der GPacker konnte die Eingabedabei nicht finden oder nicht öffnen.
Der Ausgabeordner ist eine Datei!	Bei dieser Aktion wird keine Ausgabedatei benötigt, sondern lediglich ein Ausgabeordner.
Die Ausgabedatei ist ein Ordner!	Bei dieser Aktion wird kein Ausgabeordner benötigt, sondern lediglich eine Ausgabedatei.
Bitte „Registrierungsnummer“ angeben!	Es muss bei dieser Aktion eine Registriernummer angegeben werden. Dieses wurde Ihnen bei der Registrierung mitgeteilt.
Bitte „Transport-Passwort“ angeben!	Es muss bei dieser Aktion ein Transport-Passwort angegeben werden. Dieses wurde Ihnen bei der Registrierung mitgeteilt.