

Sehr geehrte Damen und Herren,

im Folgenden beschreiben wir Ihnen kurz alle nötigen Schritte, um QS-Daten im XML-Format im Rahmen der QSKH-RL für Mehrzeitpunktmessungen (im Folgenden XML-Verfahren genannt) per E-Mail versenden zu können.

Diese Beschreibung wurde um eine Erklärung ergänzt, wie Sie Ihr Datenpaket für die Übermittlung an die Daten entgegennehmende Stelle vorbereiten, wenn Ihre Erfassungssoftware beim Export keinerlei Verschlüsselung vornimmt (s. Anhang 1).

### **1. Anmeldung (Leistungserbringer)**

Die Übermittlung der Daten im XML-Verfahren kann nur noch im E-Mail-Verfahren erfolgen. Sollte Ihre Einrichtung bei uns bereits als Teilnehmer in der Datenübermittlung per E-Mail im herkömmlichen QSINDIREKT-Verfahren registriert sein, ist keine weitere Anmeldung notwendig. Andernfalls teilen Sie uns bitte per Post oder E-Mail (serviceline@bqs-institut.de) mit, dass Sie am E-Mail-Verfahren teilnehmen möchten. Aus Ihrem Schreiben müssen eindeutig Ihre Registriernummer sowie eine verbindliche E-Mail-Adresse, an die Sie später die Rückmeldung einer Datenlieferung erhalten, hervorgehen. Für die weiteren Schritte einer Neuregistrierung werden wir uns mit Ihnen in Verbindung setzen.

### **2. Versand des Schlüssels (BQS-Institut, Standort Hamburg)**

Mit der E-Mail, mit der Sie die erste Kundeninformation erhalten haben, haben wir Ihnen als Anhang auch den öffentlichen RSA-Schlüssel (QSLQXML\_BQS.pub) des BQS-Instituts als Daten annehmende Stelle zugesandt. Dieser kann inzwischen auch auf der Website der AQUA-Institut GmbH heruntergeladen werden. Dort wurde die Schlüsseldatei umbenannt und für jedes Bundesland einzeln hinterlegt. Beispielsweise für Hamburg heißt sie jetzt Pub\_key\_Datenannahmestelle\_HH\_BQS.pub.

Der Schlüssel dient zur Verschlüsselung der Qualitätssicherungsdaten (Teil der inneren Verschlüsselung) und kann u. U. in Ihrer Erfassungssoftware hinterlegt werden. Andernfalls lesen Sie bitte im Anhang 1 nach, wie Sie vorgehen müssen.

Weiterführende Informationen zum Verfahren insgesamt entnehmen Sie bitte dem Handbuch zur Datenübermittlung im XML-Verfahren, das Sie auf der Seite der AQUA-Institut GmbH herunterladen können:

[http://www.sgg.de/entwicklung/technische\\_entwicklung/stationaere\\_qs/follow-up-uebersicht.html](http://www.sgg.de/entwicklung/technische_entwicklung/stationaere_qs/follow-up-uebersicht.html)

### **3. Überprüfung Registrierungsdaten (Leistungserbringer)**

Falls sich Änderungen bei den Kontaktdaten ergeben haben, teilen Sie uns diese umgehend mit, da uns die Angaben zur verbindlichen E-Mailadresse und die Registriernummer als Grundlage für das XML-Verfahren dienen.

#### **4. Hinterlegung des BQS-Schlüssels in der Erfassungssoftware (Leistungserbringer)**

Den öffentlichen Schlüssel des BQS-Instituts (enthalten in der Datei QSLQSXML\_BQS.pub ) müssen Sie vor dem Export der QS-Daten im XML-Format in Ihrer Erfassungssoftware hinterlegen. Fragen Sie ggf. bei Ihrem Softwareanbieter nach, an welcher Stelle dies geschehen muss. Sollte Ihre Software die Verschlüsselung der Daten nicht übernehmen, lesen Sie bitte die Angaben in Anhang 1.

#### **5. Passwort für Transportverschlüsselung (BQS-Institut, Standort Hamburg)**

Um die Transportverschlüsselung mit SQG\_TPacker Ihrer Datenlieferung vorzunehmen und die Protokolldateien öffnen zu können, ist es notwendig, ein Passwort zu haben, das Ihrer Einrichtung und dem BQS-Institut als Daten annehmende Stelle bekannt ist.

Hierfür wird die Ihrer Registriernummer im herkömmlichen QSINDIREKT-Verfahren zugeordnete Passphrase verwandt werden. Wenn Sie ein neuer Teilnehmer im E-Mail-Verfahren sind, senden wir Ihnen eine Passphrase in einer gesonderten Mail zu.

#### **6. Passwort für Transportverschlüsselung (Leistungserbringer)**

Dieses Passwort müssen Sie entweder in Ihrer Erfassungssoftware für die Transportverschlüsselung hinterlegen oder nach dem Export der Daten bei der Verschlüsselung der Transaktionsdateien mit Hilfe des von der AQUA-Institut GmbH bereitgestellten Tools SQG\_TPacker eingeben (s. Anhang 1). Bitte erkundigen Sie sich ggf. bei Ihrem Softwareanbieter.

Der SQG\_TPacker kann unter folgender Adresse heruntergeladen werden:

[http://www.sgg.de/entwicklung/technische\\_entwicklung/stationaere\\_qs/follow-up-uebersicht.html](http://www.sgg.de/entwicklung/technische_entwicklung/stationaere_qs/follow-up-uebersicht.html)

#### **7. Start der Datenübermittlung per E-Mail (Leistungserbringer)**

Sie können nun Ihre verschlüsselten Datenpakete, die mit der Passphrase aus Punkt 6 für den Transport verschlüsselt wurden, pro Registriernummer in einer E-Mail als Anlage einfügen.

Diese E-Mail senden Sie an [xmldata@bqs-institut.de](mailto:xmldata@bqs-institut.de).

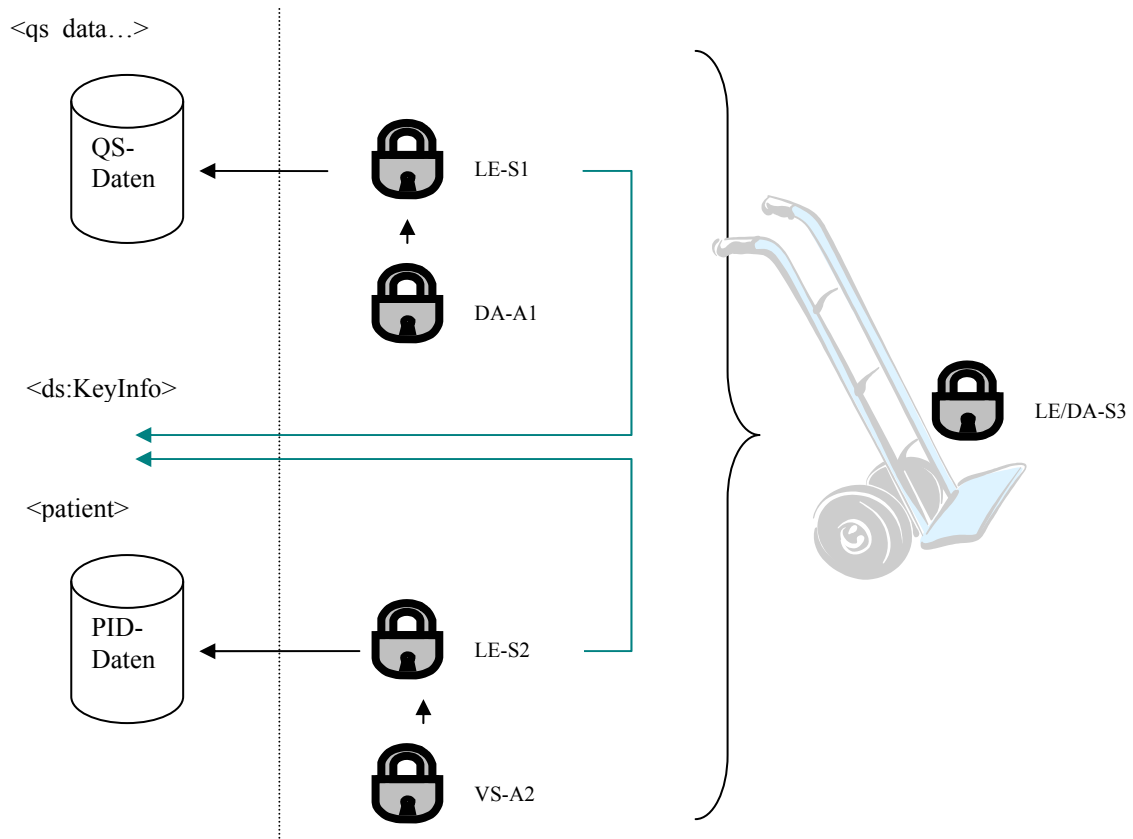
Im Betreff hinterlegen Sie bitte das Kürzel „LE-“ gefolgt von der Registriernummer, für die Sie dieses Datenpaket erstellt haben, also z. B. „LE-hh12345“.

#### **8. Rückprotokollierung per E-Mail (BQS-Institut, Standort Hamburg)**

Nach kurzer Zeit erhalten Sie pro Transaktion eine automatische Eingangsbestätigung, die lediglich den Dateneingang zurückspiegelt, aber noch keine Aussage dazu enthält, ob die Daten auch importiert werden konnten. In einer später folgenden Antwortdatei erhalten Sie als Anlage eine mit dem Transportschlüssel verschlüsselte Antwortdatei, welche die Protokolldateien des Datenimports und entsprechende Anschreiben enthält.

Diese Antwortdatei können Sie entweder direkt mit Ihrer Exportsoftware einlesen oder Sie verwenden zum Entschlüsseln und Entpacken den SQG\_TPacker der AQUA Institut GmbH. Die Beschreibung hierzu erhalten Sie im Anhang 2.

## Verschlüsselungsschema im XML-Verfahren QSKH-RL Schnittstelle Leistungserbringer zu Daten annehmender Stelle



\*.XML

\*.AES

- |          |   |
|----------|---|
| LE-S1    | Zufälliger Schlüssel, der beim Leistungserbringer (LE) erzeugt wird, wenn die QS-Daten verschlüsselt werden.<br>Symmetrisches Verschlüsselungsverfahren.  |
| DA-A1    | Öffentlicher Schlüssel der Daten annehmenden Stelle (DA), mit dem der Schlüssel LE-S1 verschlüsselt wird.<br>Asymmetrisches Verschlüsselungsverfahren.  |
| LE-S2    | Zufälliger Schlüssel, der beim Leistungserbringer (LE) erzeugt wird, um die Personen identifizierenden Daten (PID) zu verschlüsseln.<br>Symmetrisches Verschlüsselungsverfahren.  |
| VS-A2    | Öffentlicher Schlüssel der Vertrauensstelle (VS), mit dem der Schlüssel LE-S2 verschlüsselt wird.<br>Asymmetrisches Verschlüsselungsverfahren.  |
| LE/DA-S3 | Schlüssel, der dem Leistungserbringer (LE) und der Daten entgegennehmenden Stelle (DA) der LQS bekannt ist, um die Transaktionsdateien für die Datenübermittlung zu verschlüsseln. Es ist die Passphrase des regulären/bisherigen Datenübermittlungsverfahrens.<br>Symmetrisches Verschlüsselungsverfahren. |

## Anhang 1 – Manuelle Verschlüsselung

Diese Beschreibung benötigen Sie nur, wenn Ihre Erfassungssoftware beim Export keinerlei Verschlüsselung vornimmt. In diesem Fall müssen Sie Ihr Datenpaket für die Übermittlung an die Daten entgegennehmende Stelle selbst vorbereiten. Punkt 4 aus der vorangegangenen Beschreibung entfällt dann. Er wird ersetzt durch das nun beschriebene Vorgehen.

Die Arbeit mit den Programmen zur Verschlüsselung und zum Packen der Daten, die die AQUA-Institut GmbH zur Verfügung stellt, setzt voraus, dass Sie mit der Windows Befehls-Konsole umgehen können. Um die Erklärungen leichter verständlich zu machen, gehen wir von folgenden Annahmen aus:

- Ihr Benutzerverzeichnis ist  
C:\Dokumente und Einstellungen\Beispieluser
- Die Exportdatei im xml-Format heißt  
45664537-5642-9056-8676-456468327456.xml
- Das Programm für die innere Verschlüsselung der Daten heißt  
SQG\_XPacker.jar
- Das Programm für die Transportverschlüsselung heißt  
SQG\_TPacker.jar
- Sie besitzen den öffentlichen Schlüssel des BQS-Instituts, der Ihnen unter folgendem Namen zur Verfügung gestellt wurde (hier gehören Sie also zum Bundesland Hamburg):  
Pub\_key\_Datenannahmesstelle\_HH\_BQS.pub
- Sie besitzen den öffentlichen Schlüssel der Vertrauensstelle, der Ihnen unter folgendem Namen zur Verfügung gestellt wurde:  
Pub\_key\_Vertrauensstelle.pub
- Ihre Registriernummer ist hh00000
- Ihre Passphrase ist geheimpaket
- Es ist der 5. April 2012 kurz nach 10 Uhr (dies ist für die Bestimmung des Dateinamens relevant, den Sie an das BQS-Institut verschicken)

Die unten folgenden Schritte können Sie unter Unix analog in einem Terminalfenster durchführen.

Wenn Sie die Befehle unter einem anderen Betriebssystem (z. B. MacOSX) absetzen wollen, erkundigen Sie sich ggf. bei der AQUA Institut GmbH, ob und wie dies möglich ist.

## I. Arbeitsumgebung vorbereiten

- Erstellen Sie mit Hilfe des Datei-Explorers in dem Benutzerverzeichnis Ihres Rechners ein Unterverzeichnis namens xml.
- Dieses Verzeichnis gilt nun als Ihr Arbeitsverzeichnis:  
C:\Dokumente und Einstellungen\Beispieluser\xml
- Laden Sie die neueste Version der beiden Verschlüsselungsprogramme aus dem Internet herunter  
([http://www.sgg.de/entwicklung/technische\\_entwicklung/stationaere\\_qs/follow-up-uebersicht.html](http://www.sgg.de/entwicklung/technische_entwicklung/stationaere_qs/follow-up-uebersicht.html))
- Kopieren Sie die Programme SQG\_XPacker.jar und SQG\_TPacker.jar in Ihr Arbeitsverzeichnis.
- Kopieren Sie die beiden Schlüsseldateien  
Pub\_key\_Datenannahmesstelle\_HH\_BQS.pub und  
Pub\_key\_Vertrauensstelle.pub in Ihr Arbeitsverzeichnis
- Kopieren Sie die Exportdatei in Ihr Arbeitsverzeichnis
- Rufen Sie das Konsole-Fenster auf. Dazu gehen Sie auf Start -> Ausführen und tippen dort „cmd“ ein. Der kann u. U. je nach Windows-Version auf Ihrem Computer variieren.
- Wechseln Sie innerhalb der Konsole in Ihr Arbeitsverzeichnis:  
cd xml

## II. Innere Verschlüsselung vornehmen

Hierbei verschlüsseln Sie die Qualitätssicherungsdaten und die Personen identifizierenden Daten innerhalb des exportierten xml-Dokumentes. Tippen Sie die Befehle in das Konsolenfenster analog zu dem Beispiel ein, kopieren Sie sie nicht per cut & paste in Ihr Konsolenfenster, da Sie aufgrund des Zeilenumbruches sonst Probleme bei der Durchführung bekommen werden.

Für die Verschlüsselung der medizinischen Daten im XML müssen Sie eingeben:  
java -jar SQG\_XPacker.jar -e -f 45664537-5642-9056-8676-456468327456.xml  
-o 45664537-5642-9056-8676-456468327456.xmlE  
-k Pub\_key\_Datenannahmesstelle\_HH\_BQS.pub  
-t qs\_data -2 encryption

Für die Verschlüsselung der Patienten identifizierenden Daten müssen Sie eingeben:  
java -jar SQG\_XPacker.jar -e -f 45664537-5642-9056-8676-456468327456.xmlE  
-o 45664537-5642-9056-8676-456468327456.xmlE2  
-k Pub\_key\_Vertrauensstelle.pub  
-t patient -2 encryption

Die Datei, die Sie für den Versand an das BQS-Institut weiterverarbeiten müssen, heißt:

45664537-5642-9056-8676-456468327456.xmlE2

### III. Transport-Verschlüsselung vornehmen

Für die Transportverschlüsselung müssen Sie eingeben:

```
java -jar SQG_TPacker.jar -ze -f 45664537-5642-9056-8676-456468327456.xmlE2  
-o T-hh00000 -p geheimpaket
```

Die dabei entstehende Datei heißt:

```
T-hh000002012_04_05_100213.zip.aes
```

Schicken Sie diese per E-Mail an das BQS-Institut wie es in Kapitel 7 beschrieben ist.

### IV. Aufräumen

Wenn Sie die Datei verschickt haben, können Sie diese Dateien aus Ihrem Arbeitsverzeichnis löschen oder archivieren:

```
45664537-5642-9056-8676-456468327456.xml  
45664537-5642-9056-8676-456468327456.xmlE  
45664537-5642-9056-8676-456468327456.xmlE2  
T-hh000002012_04_05_100213.zip.aes
```

## Anhang 2 – Manuelle Entschlüsselung

Wenn Sie ein Rückprotokoll zu Ihrer Datenlieferung erhalten und Ihre Software die Antwortdatei im Zuge des Einlesens nicht entschlüsselt, müssen Sie dies von Hand erledigen. In dem Zuge wird die Datei auch entpackt.

Das unten aufgeführte Beispiel für das Entschlüsseln und Entpacken der Antwortdatei geht davon aus, dass diese folgenden Namen trägt  
A-hh000002012\_04\_15\_150223.zip.aes  
und dass die Passphrase zur Entschlüsselung wieder „geheimpaket“ ist.

Rufen Sie, wie unter „I. Arbeitsumgebung vorbereiten“ beschrieben, das Konsolefenster auf und wechseln Sie in Ihr Arbeitsverzeichnis.

Kopieren Sie die Antwortdatei in Ihr Arbeitsverzeichnis.

Setzen Sie dort folgenden Befehl ab:

```
java -jar SQG_TPacker -ze -f A-hh000002012_04_15_150223.zip.aes  
-p geheimpaket
```

Es entsteht die Datei 45664537-5642-9056-8676-456468327456.xml.  
Diese können Sie von dort abholen, um sie in Ihr Softwaresystem zu laden.

Unter Unix ist das Vorgehen analog in einem Terminalfenster durchzuführen.

Wenn Sie den Befehl unter einem anderen Betriebssystem (z. B. MacOSX) absetzen wollen, erkundigen Sie sich ggf. bei der AQUA Institut GmbH, ob und wie dies möglich ist.

Herzliche Grüße aus Hamburg  
Ihr BQS-Team