

Leistungserbringer-pseudonymisierungsprogramm

Anwenderhandbuch v1.0

Stand: 9. September 2015

AQUA – Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH

Impressum

Kontaktdaten

AQUA – Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH
Maschmühlenweg 8–10
37073 Göttingen

Telefon: (+49) 0551 - 789 52-0
Telefax: (+49) 0551 - 789 52-10
office@aqua-institut.de
www.aqua-institut.de

Urheberrecht

Diese Dokumentation ist urheberrechtlich geschützt. Verwendete Markennamen sowie Software- und Hardwarebezeichnungen der jeweiligen Firmen unterliegen im Allgemeinen dem warenzeichenrechtlichen, markenrechtlichen und patentrechtlichen Schutz. Sofern Teile der Dokumentation zu Zitatzwecken verwendet werden, ist dies kenntlich zu machen:

AQUA-Institut GmbH: Leistungserbringerpseudonymisierungsprogramm – Anwenderhandbuch v1.0

Nähere Informationen sind den beiliegenden Nutzungsbedingungen zu entnehmen.

Information zur Dokumentation

Originalfassung
Version v1.0
Stand: 9. September 2015

Inhaltsverzeichnis

1 Einleitung 4
1.1 Zu diesem Handbuch 4
1.2 Zielgruppe 4
1.3 Produktbeschreibung 4
1.4 Anwendungsbereich 4
2 Installation 6
2.1 Systemvoraussetzungen 6
2.2 Installation durchführen 6
2.3 Customizing 6
3 Programmaufbau 7
3.1 Grafische Benutzeroberfläche 7
3.1.1 Vorkonfiguration des Programms 7
3.1.2 Schlüsselpaargenerierung 9
3.1.3 Durchführung der Pseudonymisierung 10
3.1.4 Durchführung der Depseudonymisierung 11
3.1.5 Pseudonyme an BAS übertragen 13
3.2 Konsolenanwendung 14
3.2.1 Konsolenaufruf 14
3.3 Programmierschnittstelle (Java-API) 15
3.3.1 Spezifikation der Zusatzdaten 15
4 Datensicherung und Daten-Reorganisation 18
5 Fehlerbeschreibung 19
6 Troubleshooting 22
Anhang 23

© 2015 AQUA-Institut GmbH

1 Einleitung

1.1 Zu diesem Handbuch

Darstellungsmittel
Im Folgenden sind Symbole und Darstellung besonderer Informationen beschrieben.



Warnhinweis

Ein Warnhinweis beschreibt die Gefahr eines Fehlgebrauchs der Anwendung und wie man ihn vermeidet.

Die Nichtbeachtung eines Warnhinweises kann zu schwerwiegenden Fehlern in der Anwendung oder des Systems führen.

Beispiel:

Beispiele sind ein Hilfsmittel, um zuvor vermittelte Informationen oder konkrete Abschnitte der Anwendung zu verdeutlichen.

1.2 Zielgruppe

Dieses Handbuch richtet sich an administrative Mitarbeiter der Datenannahmestellen (DAS) und Softwareentwickler.

1.3 Produktbeschreibung

Im Kern besteht die systemweit einheitliche Leistungserbringerpseudonymisierung aus einer Software, welche ein deterministisches, asymetrisches Verschlüsselungsverfahren zur Pseudonymisierung verwendet. Mit dem öffentlichen Schlüssel werden die Daten, mit denen die Leistungserbringer identifiziert werden können, pseudonymisiert (IKNR oder BSNR). Mit dem privaten Schlüssel können die Pseudonyme von der Datenannahmestelle der Landesgeschäftsstellen Qualitätssicherung depseudonymisiert werden.

Das Pseudonymisierungsprogramm verwendet zur Pseudonymisierung der leistungserbringeridentifizierenden Daten den RSA-Verschlüsselungsalgorithmus von Legion of the Bouncy Castle Inc. Dieser Algorithmus erfüllt sowohl die Anforderungen an die systemweit einheitliche Pseudonymisierung als auch die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Kriterien.

1.4 Anwendungsbereich

Das Pseudonymisierungsprogramm wurde für unterschiedliche Zielgruppen und Anwendungsmöglichkeiten in folgenden Varianten bereitgestellt:

- mit einer grafischen Benutzeroberfläche (siehe 3.1, *Grafische Benutzeroberfläche*)
- als Konsolenanwendung (siehe 3.2, *Konsolenanwendung*)
- als Programmierschnittstelle (siehe 3.3, *Programmierschnittstelle (Java-API)*)

Die grafische Benutzeroberfläche wurde für Testzwecke und die manuelle Integration der Leistungserbringerpseudonymisierung in den Datenfluss einer Datenannahmestelle erstellt. Eine Form der manuellen Integration wäre z.B. wenn eine DAS alle bekannten IKNR/BSNR mit

© 2015 AQUA-Institut GmbH

Hilfe der Benutzeroberfläche pseudonymisiert, so eine Mappingtabelle zwischen Pseudonym und Klartext erstellt und diese dann im Datenfluß einsetzt.

Die Konsolenanwendung wurde für die programmatische Integration der Leistungserbringerpseudonymisierung in nicht Java-basierte Datenflüsse bei den Datenannahmestellen erstellt.

Zusätzlich steht den Java-Entwicklern bei den Datenannahmestellen eine API (application programming interface/Programmierschnittstelle) zur Verfügung.

Zusatzinformationen zum Leistungserbringer wie Standorte oder Fachabteilungen können mit dem Tool über eine Webservice-Schnittstelle in Form von CSV-Dateien an die Bundesebene übertragen werden (Simple Object Access Protocol: SOAP).

© 2015 AQUA-Institut GmbH

2 Installation

2.1 Systemvoraussetzungen

Hardware
- mindestens 128 MB Arbeitsspeicher (RAM)
- mindestens 25 MB freier Festplattenspeicher

Software
- mindestens Java 7
  Weitere Informationen können der Webseite
  https://www.java.com/de/download/help/sysreq.xml entnommen werden.

2.2 Installation durchführen

Java
Das Pseudonymisierungsprogramm basiert auf der Programmiersprache Java. Zur Ausführung von Java-Programmen wird die Java Runtime Environment (JRE) zur Verfügung gestellt. Die JRE kann „online“ und „offline“ installiert werden.

Zur Installation sind die Anleitungen zu beachten, die in den Installationspaketen zur Verfügung stehen.

Offizielle Installationspakete können von der Webseite
http://www.java.com/de/download/manual.jsp heruntergeladen werden.

Pseudonymisierungsprogramm
Die grafische Benutzeroberfläche für das Pseudonymisierungsprogramm ist ein ausführbares Java-Programm und kann bei korrekt installierter Java-Laufzeitumgebung einfach mit einem Doppelklick (Windows-Systeme) gestartet werden.

Das Konsolenprogramm kann ebenfalls einfach aufgerufen werden.

Zur Vereinfachung der Einbindung der API wurde diese mit ihrer Referenzimplementierung als Maven-Artefakt bereitgestellt, sodass sie in das entsprechende lokal verwendete Repository deployed werden kann.

Sollte eine Datenannahmestelle die API verwenden wollen, ohne Maven einzusetzen, so finden sich die Informationen über abhängige Bibliotheken in den pom.xml-Dateien.

2.3 Customizing

Die grafische Benutzeroberfläche speichert die Konfiguration des Programms in einer Eigenschaftsdatei (Properties). Diese wird im Benutzer-Heim-Verzeichnis angelegt.
Zum Beispiel unter Windows 7: C:\Users\M.Mustermann\pseudonym-config.properties

Beim ersten Start des Programms wird diese Datei aus den mitgelieferten Initialeinstellungen befüllt und kann per Texteditor oder die Konfigurationsseite der grafischen Benutzeroberfläche angepasst werden.

© 2015 AQUA-Institut GmbH

3 Programmaufbau

Das Pseudonymisierungsprogramm wird für unterschiedliche Zielgruppen und Anwendungsmöglichkeiten in folgenden Varianten bereitgestellt:

- Grafische Benutzeroberfläche
- Konsolenanwendung
- Programmierschnittstelle (Java-API)

3.1 Grafische Benutzeroberfläche

Datenannahmestellen können die grafische, interaktive Benutzeroberfläche nutzen, um das Pseudonymisierungsprogramm zu konfigurieren und Pseudonymisierungs- bzw. Depseudonymisierungsprozesse zu starten. Mit dem Programm können zudem weitere Zusatzinformationen an die Bundesauswertungsstelle (BAS) übermittelt werden.

3.1.1 Vorkonfiguration des Programms

Bei der erstmaligen Verwendung des Pseudonymisierungsprogramms ist es zur Verringerung redundanter Datenübergaben sinnvoll, die wiederkehrenden Dateneingaben vorzukonfigurieren. Eine Überschreibung der Standardkonfiguration ist bei jedem Anwendungsfall möglich.

Beim ersten Start wird die Konfigurationsdatei `pseudonym-config.properties` im Benutzer-Heimverzeichnis abgelegt. Die hierbei angegebenen Spalten und Zeilennummern beginnen mit Spalte 0 und Zeile 1.

Tabelle 1: Maske für die Vorkonfiguration

Feld	Beschreibung
`CSV-Datei-Spalte mit Eingangswert`	Im Falle der Pseudonymisierung steht in dieser Spalte der zu pseudonymisierende Klartext (IKNR/BSNR) und im Falle der Depseudonymisierung steht in dieser Spalte das Pseudonym.
`CSV-Datei-Spalte mit Ergebniswert`	Die Spalte der CSV-Datei, in die der Ergebniswert des Pseudonymisierungswerkzeuges eingetragen wird. Ist der Wert größer als die Anzahl der Spalten in der CSV-Datei, wird das Ergebnis als letzte Spalte in die CSV-Datei eingetragen. Ist der Wert kleiner als 0, wird der Eingangswert mit dem Ergebnis überschrieben.
`CSV-Datei-Spalte mit Pseudonymisierungsverfahren`	Gibt an, in welcher Spalte der CSV-Datei die Pseudonymisierungsmethode angegeben ist. Wird dieses Feld auf einen Wert kleiner 0 gestellt, so wird der Wert des Feldes „Pseudonymisierungsverfahren“ für die gesamte CSV-Datei angewendet.
`Das Passwort des Benutzers bei der BAS`	Das Passwort, das bei der BAS dem entsprechenden Benutzernamen zugeordnet ist.
`Datenannahmestellentyp`	Typ der Datenannahmestelle auswählen (LQS, KV, BAS)
`Der Benutzername bei der BAS`	Jeder DAS, LQS, KV, welche Zusatzdaten verwaltet, wird von der BAS ein Benutzername zugeordnet.
`Eingangs CSV-Dateiname`	Die zu bearbeitende CSV-Datei.

© 2015 AQUA-Institut GmbH

Feld	Beschreibung
Endgültigkeitsdatum des Schlüssels	Gibt an, bis zu welchem Datum das nächste erzeugte Schlüsselpaar gültig ist. Bleibt dieses Feld leer, ist das Schlüsselpaar ab der Erzeugung 20 Jahre lang gültig.
Ergebnis CSV-Dateiname	Die CSV-Datei, in welcher das Pseudonymisierungswerkzeug das pseudonymisierte bzw. depseudonymisierte Ergebnis ablegen soll.
Landeskennung	Landeskennung auswählen
Passwort mit dem der private Schlüssel geschützt wird	Der private Schlüssel wird verschlüsselt in einem X509-Zertifikat abgelegt. Das Passwort wird benötigt, um den privaten Schlüssel benutzen zu können.
Pseudonymisierungsverfahren	Das QS-Verfahren, auf welches sich die Pseudonymisierung bezieht.
Schlüssel Verzeichnis	Das Verzeichnis, in dem die Schlüssel abgelegt werden.
Startgültigkeitsdatum des Schlüssels	Gibt an, ab welchem Datum das nächste erzeugte Schlüsselpaar gültig ist.
Zeilennummer der CSV-Datei mit der die Pseudonymisierung beginnen soll.	Für den Fall, dass nicht die gesamte CSV-Datei pseudonymisiert werden soll, oder wenn es eine Kopfzeile mit Spaltennamen in der CSV-Datei gibt, kann angegeben werden, ab welcher Zeile die CSV-Datei bearbeitet werden soll.
Zusatzdaten CSV-Dateiname	Die CSV-Datei mit den Zusatzinformationen (Standortnummern, Haupt-IKNR/BSNR, Gültigkeit)

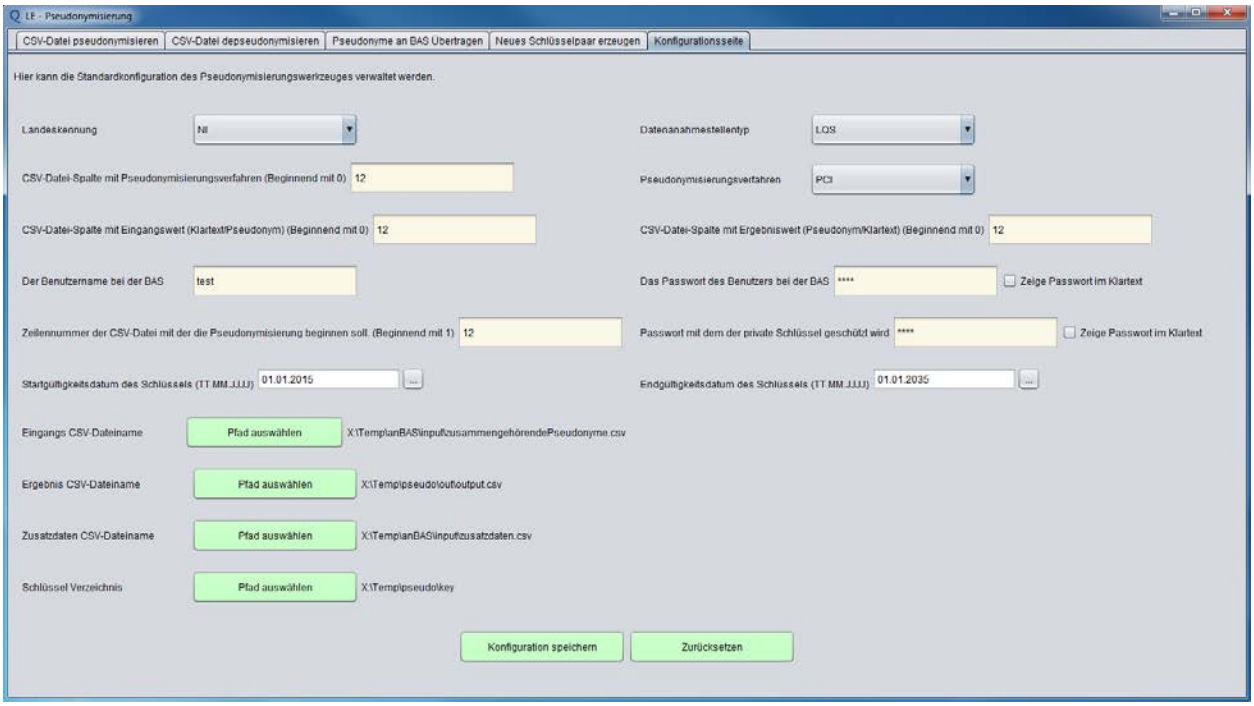


Abbildung 1: Fenstermaske für die Konfiguration

Beim Klick auf die Schaltfläche *Zurücksetzen* werden die Formularwerte auf die Werte der Eigenschaftsdatei zurückgesetzt.

© 2015 AQUA-Institut GmbH

3.1.2 Schlüsselpaargenerierung

Bei der Generierung der Schlüsselpaare (X.509-Zertifikate) sind folgende Hinweise zu berücksichtigen:

- Nur die Datenannahmestellen der Krankenhäuser (LQS/LKG) und die Kassenärztlichen Vereinigungen (KV) dürfen öffentliche und private Zertifikate generieren.
- DAS-KK erhält für den Regelbetrieb von den KVen und LQSen bzw. LKGen über einen sicheren Kanal die öffentlichen Zertifikate.
- Private Zertifikate dürfen nur vom Zertifikatsbesitzer selbst für die Despseudonymisierung verwendet werden.

Während der Generierung der Zertifikate werden einige Attribute abgefragt (Tabelle 2).

Tabelle 2: Fenstermaske: Schlüsselpaar erzeugen

Feld	Beschreibung
Datenannahmestellentyp	Art der Datenannahmestelle auswählen (LQS, KV, BAS).
Landeskennung	Landeskennung auswählen
Startgültigkeitsdatum des Schlüssels	Gibt an, ab welchem Datum das nächste erzeugte Schlüsselpaar gültig ist.
Endgültigkeitsdatum des Schlüssels	Gibt an, bis zu welchem Datum das nächste erzeugte Schlüsselpaar gültig ist. Bleibt dieses Feld leer, so bleibt das Schlüsselpaar ab der Erzeugung 20 Jahre lang gültig. Wir empfehlen den Gültigkeitszeitraum nicht zu kurz zu wählen, da sich mit jedem neuen Schlüssel die Pseudonyme ändern und erneut Listen von zusammengehörigen Pseudonymen an die BAS übertragen werden müssen.
Passwort mit dem der private Schlüssel geschützt wird	Der private Schlüssel wird verschlüsselt in einem X509-Zertifikat abgelegt. Das Passwort wird benutzt, um den privaten Schlüssel benutzen zu können. Sollte dieses Passwort verloren gehen, müssen die Daten des laufenden Erfassungsjahres repseudonymisiert und erneut an die BAS übertragen werden.
Schlüssel Verzeichnis	Das Verzeichnis, in dem die Schlüssel abgelegt werden.

Die Ausgabe besteht aus zwei Dateien, das öffentliche und das private Zertifikat. Die Dateien werden automatisch nach folgendem Schema benannt:

- Das öffentliche Zertifikat:

```
<Art-Datenannahme>$$<Bundeslandkürzel><Startgültigkeitsdatum>.cer
```

- Das private Zertifikat:

```
<Art-Datenannahme>$$<Bundeslandkürzel><Startgültigkeitsdatum>.p12
```

Beispiel (LQS Hamburg):
Öffentliches Zertifikat: `LQS$$HH20150501.cer`

Privates Zertifikat: `LQS$$HH20150501.p12`

© 2015 AQUA-Institut GmbH

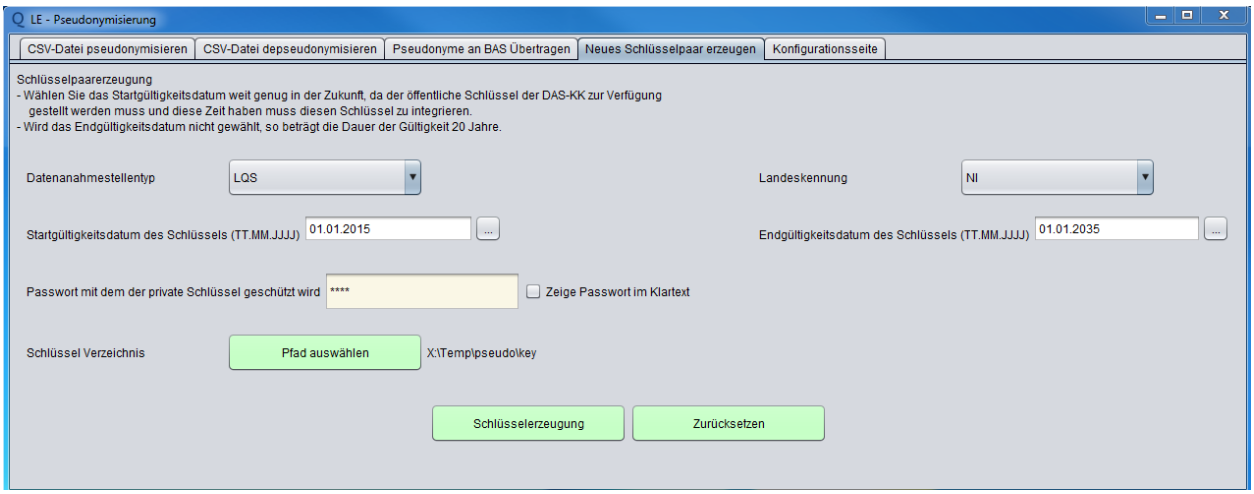


Abbildung 2: Fenstermaske für die Generierung der Zertifikate

Beim Klick auf die Schaltfläche *Zurücksetzen* werden die Formularwerte auf die Werte der Konfigurationsseite zurückgesetzt.

3.1.3 Durchführung der Pseudonymisierung

Das Pseudonymisierungsprogramm nutzt den deterministischen, asymmetrischen RSA-Verschlüsselungsalgorithmus mit einer Schlüssellänge von 2048 Bit zur Erzeugung von Pseudonymen. Die resultierenden Binärdaten werden dann in einen Base64-kodierten Text überführt und als Pseudonym benutzt. Die einheitliche Pseudonymisierung ist von allen Datenannahmestellen gemäß Qesü-RL durchzuführen. Für die Krankenhäuser ist die IKNR zu pseudonymisieren, im kollektiv- bzw. selektivvertraglichen Bereich ist stattdessen die BSNR (XML-Element **BSNRAMBU**) zu pseudonymisieren. Die DAS für die Krankenkassen und die DAS für die selektivvertraglichen Arztpraxen (DAS-SV) besitzen keine eigenen Zertifikate und müssen die öffentlichen Zertifikate der DAS-LE auf Landesebene nutzen. Dazu müssen diese DAS entscheiden, ob es sich bei den leistungserbringeridentifizierenden Daten um ein IKNR oder BSNR handelt. IKNRs werden mit dem Schlüssel der LQS verschlüsselt, BSNRs mit dem Schlüssel der KV. Zusätzlich muss auch das Bundesland bekannt sein, damit der richtige Schlüssel auf Landesebene ausgewählt werden kann.

Weitere Informationen über die LE-Daten und der Aufbau der Exportdateien sind den entsprechenden Spezifikationen zu entnehmen.

Tabelle 3: Fenstermaske für die Pseudonymisierung

Feld	Beschreibung
`Datenannahmestellentyp`	Art der Datenannahmestelle auswählen(LQS, KV, BAS).
`Landeskennung`	Landeskennung auswählen
`CSV-Datei-Spalte mit Pseudonymisierungsverfahren`	Gibt an, in welcher Spalte der CSV-Datei die Pseudonymisierungsmethode angegeben ist. Wird dieses Feld auf einen Wert kleiner 0 gestellt, so wird der Wert des Feldes „Pseudonymisierungsverfahren“ für die gesamte CSV-Datei angewendet.
`Pseudonymisierungsverfahren`	Das QS-Verfahren, auf welches sich die Pseudonymisierung bezieht.

© 2015 AQUA-Institut GmbH

Feld	Beschreibung
CSV-Datei-Spalte mit Ergebniswert	Die Spalte der CSV-Datei, in welche der Ergebniswert des Pseudonymisierungswerkzeugs eingetragen wird. Ist der Wert größer als die Anzahl der Spalten in der CSV-Datei, so wird das Ergebnis als letzte Spalte in die CSV-Datei eingetragen. Ist der Wert kleiner als 0, so wird der Eingangswert mit dem Ergebnis überschrieben.
CSV-Datei-Spalte mit Eingangswert	Im Falle der Pseudonymisierung steht in dieser Spalte der zu pseudonymisierende Klartext (IKNR/BSNR) und im Falle der Depseudonymisierung steht in dieser Spalte das Pseudonym.
Zeilennummer der CSV-Datei mit der die Pseudonymisierung beginnen soll.	Für den Fall, dass nicht die gesamte CSV-Datei pseudonymisiert werden soll, oder wenn es eine Kopfzeile mit Spaltennamen in der CSV-Datei gibt, kann angegeben werden, ab welcher Zeile die CSV-Datei bearbeitet werden soll.
Eingangs CSV-Dateiname	Die zu bearbeitende CSV-Datei.
Ergebnis CSV-Dateiname	Die CSV-Datei, in welcher das Pseudonymisierungswerkzeug das pseudonymisierte bzw. depseudonymisierte Ergebnis ablegen soll.
Schlüssel Verzeichnis	Das Verzeichnis in dem die Schlüssel abgelegt werden.

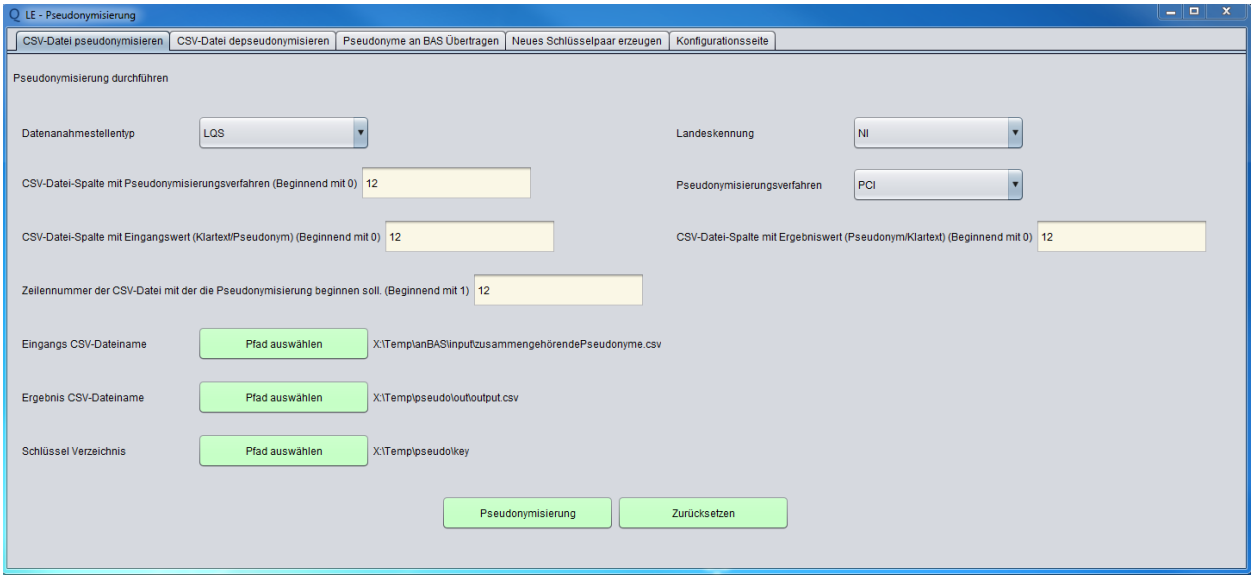


Abbildung 3: Fenstermaske für die Pseudonymisierung

Beim Klick auf die Schaltfläche *Zurücksetzen* werden die Formularwerte auf die Werte der Konfigurationsseite zurückgesetzt.

3.1.4 Durchführung der Depseudonymisierung

Analog zur Pseudonymisierung nutzt das Pseudonymisierungsprogramm denselben Algorithmus zur Depseudonymisierung der Leistungserbringerpseudonyme. Die Depseudonymisierung mit dem Pseudonymisierungsprogramm ist nur durch die LQS/LKG und die KVen durchzuführen. Die DAS-SV kann hingegen nur auf Mapping-Informationen zurückgreifen. Die Depseudonymisierung der LE-Pseudonyme in den Rückprotokollen bzw. in den Rückmeldeberichten ist gemäß Spezifikation erforderlich.

© 2015 AQUA-Institut GmbH

Tabelle 4: Maske für die Depseudonymisierung

Feld	Beschreibung
Datenannahmestellentyp	Art der Datenannahmestelle auswählen (LQS, KV, BAS).
Landeskennung	Landeskennung auswählen
Passwort mit dem der private Schlüssel geschützt wird	Der private Schlüssel wird verschlüsselt in einem X509-Zertifikat abgelegt. Das Passwort wird benutzt, um den privaten Schlüssel benutzen zu können.
CSV-Datei-Spalte mit Ergebniswert	Die Spalte der CSV-Datei, in welche der Ergebniswert des Pseudonymisierungswerkzeugs eingetragen wird. Ist der Wert größer als die Anzahl der Spalten in der CSV-Datei, so wird das Ergebnis als letzte Spalte in die CSV-Datei eingetragen. Ist der Wert kleiner als 0, so wird der Eingangswert mit dem Ergebnis überschrieben.
CSV-Datei-Spalte mit Eingangswert	Im Falle der Pseudonymisierung steht in dieser Spalte der zu pseudonymisierende Klartext (IKNR/BSNR) und im Falle der Depseudonymisierung steht in dieser Spalte das Pseudonym.
Zeilennummer der CSV-Datei mit der die Pseudonymisierung beginnen soll.	Für den Fall, dass nicht die gesamte CSV-Datei pseudonymisiert werden soll, oder wenn es eine Kopfzeile mit Spaltennamen in der CSV-Datei gibt, kann angegeben werden, ab welcher Zeile die CSV-Datei bearbeitet werden soll.
Eingangs CSV-Dateiname	Die zu bearbeitende CSV-Datei.
Ergebnis CSV-Dateiname	Die CSV-Datei, in welcher das Pseudonymisierungswerkzeug das pseudonymisierte bzw. depseudonymisierte Ergebnis ablegen soll.
Schlüssel Verzeichnis	Das Verzeichnis, in dem die Schlüssel abgelegt werden.

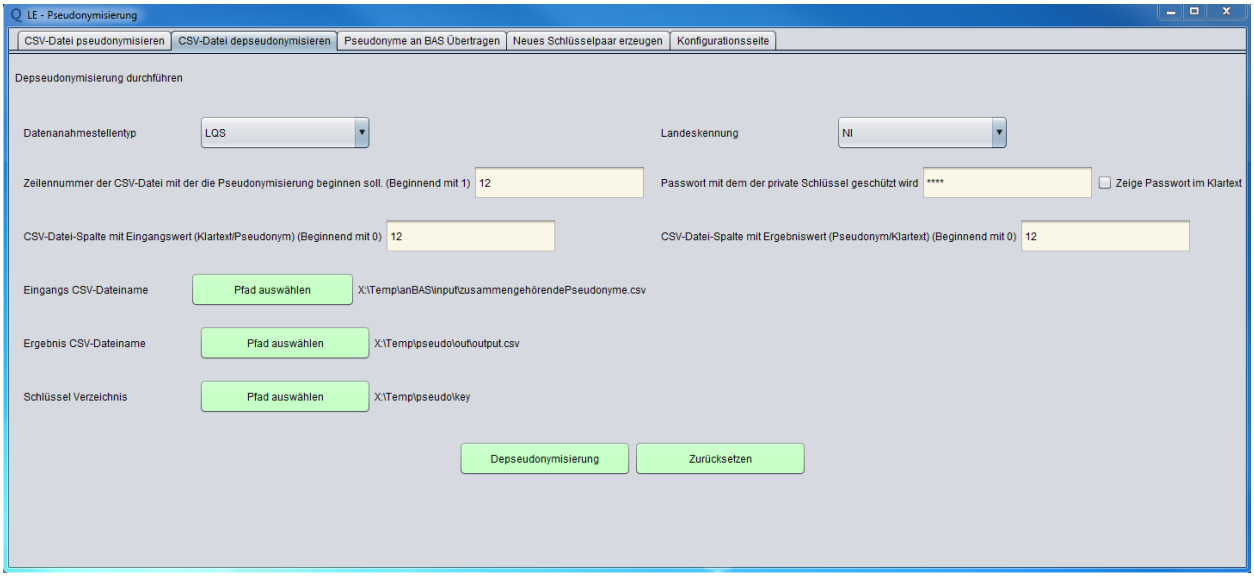


Abbildung 4: Fenstermaske für die Depseudonymisierung

Beim Klick auf *Zurücksetzen* werden die Formularwerte auf die Werte der Konfigurationsseite zurück gesetzt.

© 2015 AQUA-Institut GmbH

3.1.5 Pseudonyme an BAS übertragen

Näheres dazu in der Spezifikation der Zusatzdaten (siehe 3.3.1, *Spezifikation der Zusatzdaten*).

Vor der Übermittlung der Daten werden einige Attribute abgefragt (Tabelle 2).

Tabelle 5: Fenstermaske: Schlüsselpaar erzeugen

Feld	Beschreibung
`Datenannahmestellentyp`	Art der Datenannahmestelle auswählen (LQS, KV, BAS)
`Landeskennung`	Landeskennung auswählen
`Eingangs CSV-Dateiname`	Die zu bearbeitende CSV-Datei.
`Zusatzdaten CSV-Dateiname`	Die CSV-Datei mit den Zusatzinformationen (Standortnummern, Haupt-IKNR/BSNR, Gültigkeit)
`Schlüssel Verzeichnis`	Das Verzeichnis, in dem die Schlüssel abgelegt werden.
`Der Benutzername bei der BAS`	Jeder DAS,LQS,KV, welche Zusatzdaten verwaltet, erhält einen Benutzernamen von der BAS zugeordnet.
`Passwort mit dem der private Schlüssel geschützt wird`	Der private Schlüssel wird verschlüsselt in einem X509-Zertifikat abgelegt. Das Passwort wird benutzt, um den privaten Schlüssel benutzen zu können.

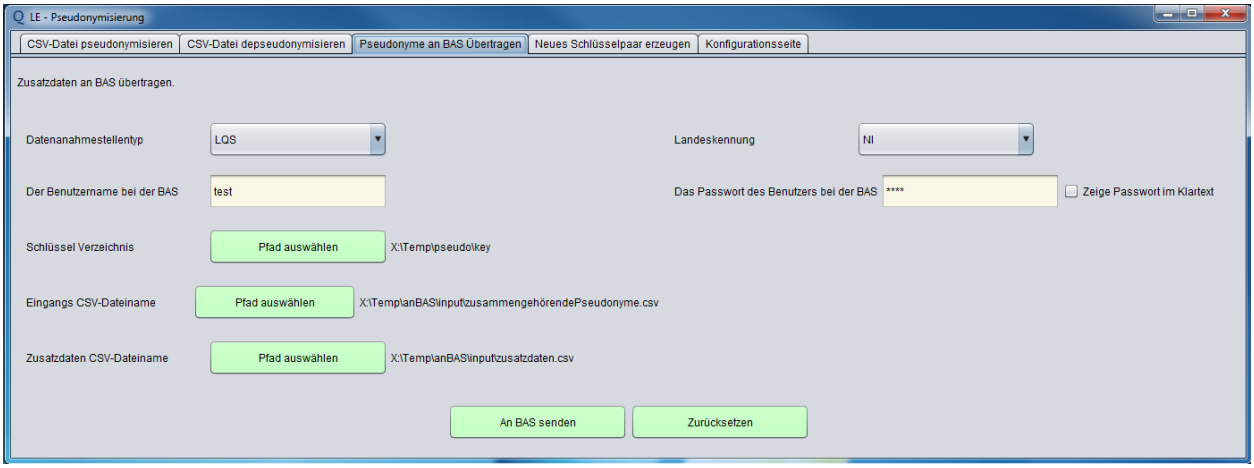


Abbildung 5: Fenstermaske für die Übermittlung der Zusatzinformationen an die BAS

Beim Klick auf *Zurücksetzen* werden die Formularwerte auf die Werte der Konfigurationsseite zurück gesetzt.

© 2015 AQUA-Institut GmbH

3.2 Konsolenanwendung

Die Datenannahmestellen können das Pseudonymisierungsprogramm als Konsolenapplikation in eine „Nicht-Java“-Datenverarbeitungskette integrieren. Das Programm wird in diesem Fall dafür benutzt, eine CSV-Datei mit einer Liste von LE-Daten zu pseudonymisieren bzw. zu depseudonymisieren. Hierbei wird ein System-Return-Code erzeugt, der die jeweiligen Erfolgs- oder Fehlerfälle ausgibt. Durch Konsolen-Parameter oder wahlweise eine Eigenschaftsdatei (Properties-File) erhält das Pseudonymisierungsprogramm sowohl die Information über den Zugriffsort der CSV-Datei als auch über den Speicherort der Ergebnisdatei.

3.2.1 Konsolenaufruf

Abhängig von den durchzuführenden Aktionen ist die Kommandozeile entsprechend anzupassen. Folgende Tabelle gibt einen Überblick über die einzelnen Anwendungsfälle.

Tabelle 6: Anwendungsfälle

Use-Case	Kommandozeile
Generierung der Zertifikate	java -jar pseudonymisierung-console.jar -a LQS -b 30.06.2015 -c C:\pseudo\key -l BW -s test -z
Pseudonymisierung	java -jar pseudonymisierung-console.jar -a LQS -c C:\pseudo\key -l NI -i C:\pseudo\input.csv -j 2 -k 1 -p -r C:\pseudo\out\outk.csv -t "-1" -w PCI
Depseudonymisierung	java -jar pseudonymisierung-console.jar -a LQS -c C:\pseudo\key -d -l NI -i C:\pseudo\depseu.csv -j 2 -k 1 -r C:\pseudo\out\outdepseuk.csv -t "-1" -s test
Übermittlung der Zusatzdaten an die BAS	java -jar pseudonymisierung-console.jar -h -a LQS -c C:\pseudo\key -l NI -l C:\pseudo\pseudonymMappings.csv -m C:\pseudo\zusatzDaten.csv -n username -q password

Tabelle 7: Parameter

Parameter	Bedeutung
-a,--das <arg>	Datenannahmestelle, deren Zertifikate benutzt werden sollen. Gültige Werte sind LQS, BAS, KV, SV (siehe Anhang).
-b,--sdate <arg>	Beginn der Gültigkeit des zu erzeugenden Schlüssel-Zertifikats.
-c,--certificates <arg>	Verzeichnis für die Schlüsseldateien.
-d,--depseudo	Startet das Programm im Depseudonymisierungs-Modus.
-e,--edate <arg>	Ende der Gültigkeit des zu erzeugenden Schlüssel-Zertifikats.
-f,--cert <arg>	Zertifikat, welches verwendet werden soll.
-i,--input <arg>	CSV-Datei, welche pseudonymisiert bzw. depseudonymisiert werden soll, im Falle der Pseudonymisierung oder Depseudonymisierung. CSV-Datei, welche pro Zeile eine Liste von zusammengehörenden IKNR/BSNR enthält, für den Fall, dass Zusatzdaten an die BAS übertragen werden sollen.
-j,--rowStart <arg>	Zeile der CSV-Datei, ab der die Datei bearbeitet werden soll (Beginnend mit 1).
-k,--inputSpalte <arg>	Spalte in der CSV-Datei mit den Eingangsdaten (Klartext bei Pseudonymisierung, Pseudonym bei Depseudonymisierung) (Beginnend mit 0).
-l,--Länderkürzel <arg>	Länderkürzel (DAS-LE-Identität) Gültige Werte sind: AU, SH, HH, NI, HB, NW, NO, WL, HE, RP, BW, BA, SL, BE, BB, MV, SN, ST, TH, BAS (siehe Anhang)

© 2015 AQUA-Institut GmbH

Parameter	Bedeutung
`-o,--properties <arg>`	Dateipfad der zu benutzenden Properties-Datei.
`-p,--pseudo`	Startet das Programm im Pseudonymisierungsmodus.
`-r,--output <arg>`	Ziel der Ergebnis-CSV-Datei
`-s,--certpassword <arg>`	Passwort der Zertifikatsdatei
`-t,--outputSpalte <arg>`	Die Spalte der CSV-Datei, in welche der Ergebniswert des Pseudonymisierungswerkzeuges eingetragen wird. Ist der Wert größer als die Anzahl der Spalten in der CSV-Datei, so wird das Ergebnis als letzte Spalte in die CSV-Datei eingetragen. Ist der Wert kleiner als 0, so wird der Eingangswert mit dem Ergebnis überschrieben.
`-v,--verfahrenSpalte <arg>`	Spalte in der CSV-Datei mit Verfahrenskürzel
`-w,--verfahren <arg>`	Verfahrenskürzel, welches benutzt werden soll. Gültige Werte sind: PCI, DV, IV (siehe Anhang).
`-z,--creaCert`	Erzeugt ein neues Zertifikat.
`-h, --send`	Sendet die aktuellen Einträge der Zusatzdatenverwaltung an die BAS.
`-m, –-addData <arg>`	Die Zusatzdaten-CSV-Datei.
`-n, –-user <arg>`	>Der Benutzername bei der BAS
`-q, --password <arg>`	Das Benutzerpasswort bei der BAS.

3.3 Programmierschnittstelle (Java-API)

Sämtliche Funktionen des Pseudonymisierungsprogramms können über eine Programmierschnittstelle (API) aufgerufen und direkt in einem Java-Umfeld verwendet werden.

Die Beschreibung der einzelnen Funktionen kann der Javadocs-Dokumentation entnommen werden.

Das Pseudonymisierungsprogramm besteht aus einer API und der Referenzimplementierung (`pseudonymisierung-impl.jar`)
Die Zusatzdatenverwaltungsreferenzimplementierung ist in `pseudonymisierung-zus-cli.jar` zu finden.

Da die Kommunikation mit den Servern der BAS bestimmten Sicherheitskriterien genügen muss, wurden bei der Implementierung des Zusatzdatenverwaltungsklienten Frameworks mit geprüften Sicherheitskomponenten eingesetzt. Im Falle des Zusatzdatenverwaltungsklienten ist dies das Spring-Boot-Framework in der Version 1.2.4 Diejenigen DAS, welche die Zusatzdaten aus einem eigenen Java-Programm heraus übermitteln wollen, müssen daher das genannte Framework für ihr Java-Programm nutzen oder auf den Konsolen-Client zurückgreifen.

3.3.1 Spezifikation der Zusatzdatens

Die Zusatzdaten bestehen aus Listen von zusammengehörigen Pseudonymen, Standortnummern, Gültigkeitszeiträumen der leistungerbringeridentifizierenden Daten und ähnlichen Metadaten.

Um die Datenstruktur mit dem CSV-Datenmodell abbilden zu können, werden zwei getrennte CSV-Dateien benutzt.

© 2015 AQUA-Institut GmbH

pseudoMappings.csv

In der ersten Datei werden pro Zeile die zusammengehörenden leistungserbringeridentifizierenden Daten (IKNR/BSNR) eines Leistungserbringers aufgelistet.

Vor der Übertragung werden diese Daten automatisch anhand des aktuellen, öffentlichen Schlüssels und aller möglichen Pseudonymisierungsverfahren pseudonymisiert.

Beispiel:

```
123456789;888888888;999999999;;;
234567891;345678912;;;;
456789123;;;;;
567891234;678912345;;;;
```

Zusatzdaten.csv

In der zweiten Datei werden zu den einzelnen leistungserbringeridentifizierenden Daten die Zusatzdaten erfasst.



Achtung

Möglicher Übertragungsfehler der von der Bundesauswertungsstelle (BAS) benötigten Daten an die BAS.

Die CSV-Datei muss eine Überschrift besitzen.

Beispiel:

```
pseudonym;ist HauptPseudonym;Standortnummern;g ltig ab;g ltig
bis;notiz
123456789;1;01,02,03;01.01.2015;;
888888888;0;02;01.01.2000;;
999999999;0;;01.01.2000;31.12.2014;zusammenlegung zweier KHs
234567891;1;01,02;;;
345678912;0;02;;;
456789123;1;01,02;;;
567891234;1;99,01;;;
678912345;0;01;;;
```

© 2015 AQUA-Institut GmbH

Die Spalten der CSV-Datei besitzen folgende Bedeutung:

Tabelle 8: Spaltenbedeutung der CSV-Datei

Spalte	Beschreibung
`pseudonym`	Das leistungserbringeridentifizierende Datum, welches vor der Übermittlung an die BAS automatisch pseudonymisiert wird.
`ist HauptPseudonym`	1, wenn das Pseudonym dieses leistungserbringeridentifizierenden Datums (IKNR/BSNR) als Haupt-Pseudonym gekennzeichnet werden soll. Sonst 0
`Standortnummern`	(optional) Die für dieses leistungserbringeridentifizierende Datum gültigen Standortnummern
`Gültig ab`	(optional) Sollte dieses leistungserbringeridentifizierende Datum erst ab einem bestimmten Datum gültig sein, kann dies hier in der Form <tt.MM.yyyy> vermerkt werden.
`Gültig bis`	(optional) Sollte dieses leistungserbringeridentifizierende Datum nur bis zu einem bestimmten Datum gültig sein, kann dies hier in der Form <tt.MM.yyyy> vermerkt werden.
`Notiz`	(optional) Eine Notiz, welche bei der Fehlersuche helfen könnte wie z.B. „Verkauf eines Standorts, daher IKNR nur gültig bis“

© 2015 AQUA-Institut GmbH

4 Datensicherung und Daten-Reorganisation

Das Programm der grafischen Benutzeroberfläche des Pseudonymisierungsprogramms besteht nur aus zwei Dateien:

- ausführbares Java-Programm
- Eigenschaftsdatei im Benutzer-Heim-Verzeichnis

Weitere Dateien sind aus Sicht des Pseudonymisierungsprogramms bei der Datensicherung oder Datenreorganisierung nicht zu berücksichtigen.

© 2015 AQUA-Institut GmbH

5 Fehlerbeschreibung

Sollte das Programm bei einem Doppelklick nicht starten oder das „Öffnen mit“-Fenster von Windows geöffnet werden, ist möglicherweise die Java-Laufzeitumgebung nicht korrekt installiert. In diesem Fall wenden Sie sich bitte an Ihren Systemadministrator.

Geschweifte Klammern **{}** in der Spalte „Bedeutung“ von Tabelle 9 werden vom Programm dynamisch sinnvoll ersetzt.

Beispiel:

Bedeutung:

```
Bei der Verarbeitung der CSV-Datei {} ist ein Fehler in Zeile
{} aufgetreten.
```

Wird ersetzt durch:

```
Bei der Verarbeitung der CSV-Datei c:/temp/Muster.csv ist ein
Fehler in Zeile 25 aufgetreten.
```

Tabelle 9: Fehlercodes

Fehlercode	Bedeutung	Fehlerbehebung	
		Erläuterung	Trouble shooting*
1000	Unbekannt		X
1	Konnte *certificate.startdate* nicht konvertieren.	*certificate.startdate* ist im falschen Format angegeben.	
2	Konnte keine Schlüsselpaare erzeugen.		X
4	Konnte den öffentlichen Schlüssel nicht schreiben.	Auf das angegebene ‚Schlüssel Verzeichnis‘ (`registration.dir`) konnte nicht schreibend zugegriffen werden.	
5	Konnte den PKCS12 Schlüssel nicht schreiben.	Auf das angegebene ‚Schlüssel Verzeichnis‘ (`registration.dir`) konnte nicht schreibend zugegriffen werden.	
6	Konnte den öffentlichen Schlüssel nicht lesen.		X
7	Der Schlüssel existiert schon.	-	
9	Unbekannter Zertifikatstyp	-	
10	Die im Schlüssel enthaltenen Metadaten enthalten falsche Angaben zur Datenannahmestelle.	-	
12	Die Daten konnten nicht pseudonymisiert werden.		X
13	Die Daten konnten nicht depseudonymisiert werden.		X

© 2015 AQUA-Institut GmbH

Fehlercode	Bedeutung	Fehlerbehebung	
		Erläuterung	Trouble shooting*
14	Falscher Dateiname für den öffentlichen Schlüssel.	-	
15	Registrationsverzeichnis existiert nicht.	-	
16	Das angegebene Registrationverzeichnis ist kein Verzeichnis.	-	
17	Fehler beim Erzeugen des privaten Schlüssels.		X
18	Fehler beim Laden des privaten Schlüssels. Entweder das Passwort ist falsch oder das Zertifikat ist defekt.	-	
19	Der Klartext {} konnte nicht vom Verfahren getrennt werden.	Das gerade depseudonymisierte Pseudonym ist aus einem nicht der Spezifikation entsprechendem Klartext erzeugt worden. Bitte benachrichtigen Sie die BAS über diesen Vorfall.	
20	Die Property mit dem Namen {} wird benötigt.	-	
21	Die Property mit dem Namen {} muss ein Integer-Wert enthalten.	-	
22	CSV-Datei {} konnte nicht gefunden werden.	-	
26	Es gibt keine Länderkürzel mit dem Namen oder Kürzel {}.	-	
27	Es gibt kein Modul mit dem Kürzel {}.	-	
28	Es gibt kein Verfahren mit dem Kürzel {}.	-	
29	Es gibt keine Datenannahmestelle mit dem Anfangskürzel {}.	-	
30	Keine Schlüssel für die Datenannahme {} {} im Verzeichnis {} gefunden.	-	
32	In der LQS kann kein Bundesland {} ausgewählt werden.	-	
33	In der KV kann kein Bundesland {} ausgewählt werden.	-	
34	Die CSV-Datei hat nur {} Spalten in {} wurde {} angegeben.	-	
35	Es wurde kein Zertifikat gefunden, welches zum angegebenen Datum {} valid ist.	-	
36	Die benutzte Datumsformatierung ist nicht valid {} muss `dd.MM.yyyy` genügen.	-	
37	Das Pseudonym {} konnte nicht von der Zertifikats-ID getrennt werden.	Das angegebene Pseudonym entspricht nicht der Spezifikation. Bitte benachrichtigen Sie die BAS über diesen Vorfall.	

© 2015 AQUA-Institut GmbH

Fehlercode	Bedeutung	Fehlerbehebung	
		Erläuterung	Trouble shooting*
38	Die Zertifikats-ID {} ist invalid.	Die angegebene Zertifikats-ID entspricht nicht der Spezifikation. Bitte benachrichtigen Sie die BAS über diesen Vorfall.	
39	Das Pseudonym wurde von einer anderen Datenannahmestelle pseudonymisiert. Die Zertifikats-ID der fremden DAS lautet {} .	-	
40	Zeile {} in CSV-Datei {} ist nicht korrekt formatiert.	-	
41	In der CSV-Datei {} in der Zeile {} fehlt ein Hauptpseudonym.	-	
42	Bei der Übertragung der Daten an die BAS ist ein Fehler aufgetreten: {}		X
43	Bei der Verarbeitung derCSV-Datei {} ist ein Fehler in Zeile {} aufgetreten.		X
1001	Konsolen-Argument 'p', 'd' oder 'z' erforderlich!	-	
1002	Konsolen-Argument {} erforderlich!	-	

* Mit Troubleshooting markierten Fehlercodes werden im Kapitel „Troubleshooting“ beschrieben.

© 2015 AQUA-Institut GmbH

6 Troubleshooting

Bei der Verwendung der grafischen Benutzeroberfläche oder des Konsolenprogramms, wird im gleichen Verzeichnis eine pseudonymisierungs.log-Datei geschrieben. In dieser Datei werden Programmvorgänge und Fehler protokolliert. Die dieses Protokoll beinhaltende Datei ist der Schlüssel zur Fehleranalyse.

Wird die Referenzimplementierung verwendet, sollte das Slf4j-Logging-Framework konfiguriert werden, damit auch hier die entsprechenden Informationen protokolliert werden.

Die meisten möglichen Fehlermeldungen sind selbsterklärend. Wird auf dieses Kapitel verwiesen, macht ein Blick in diese Logdatei Sinn.

Sofern die Fehleranalyse von der Datenannahmestelle nicht allein bewältigt werden kann, sollte diese Datei nach Auftreten des Fehlers gesichert und bei Unterstützungsanfragen an die BAS mitgesendet werden.

© 2015 AQUA-Institut GmbH

Anhang

Gültige Pseudonymisierungsverfahren

Kürzel	Verfahren
PCI	PCI
DV	Direkte Verfahren
IV	Indirekte Verfahren

Gültige Länderkürzel

Kürzel	Bedeutung
AU	Ausland
SH	Schleswig-Holstein
HH	Hamburg
NI	Niedersachsen
HB	Bremen
NW	Nordrhein-Westfalen
NO	Nordrhein
WL	Westfalen-Lippe
HE	Hessen
RP	Rheinland-Pfalz
BW	Baden-Württemberg
BA	Bayern
SL	Saarland
BE	Berlin
BB	Brandenburg
MV	Mecklenburg-Vorpommern
SN	Sachsen
ST	Sachsen-Anhalt
TH	Thüringen
BAS	Bundesweit

Gültige Datenannahmestellen

Kürzel	Datenannahmestelle
LQS	Landesqualitätsstelle
BAS	Bundesannahmestelle
KV	Kassenärztliche Vereinigung
SV	Datenannahme für Selektivvertragliche Ärzte

© 2015 AQUA-Institut GmbH