

Datenflussspezifikation

Systemweit einheitliche Leistungserbringerpseudonymisierung

Stand: 9. September 2015

AQUA – Institut für angewandte Qualitätsförderung und Forschung im Gesundheitswesen GmbH

Inhaltsverzeichnis

1. Einleitung 3
2. Datenfluss im Rahmen der Qesü 4
   2.1. Schlüsselpaare 4
   2.2. Pseudonymisierung 4
   2.3. Rückmeldeberichte 5
3. Datenfluss der Zusatzdatenverwaltung 6
   3.1. Sicherheit 6
   3.2. Zusatzdaten zum Transfer 7

© 2015 AQUA-Institut GmbH

1. Einleitung

Die leistungserbringeridentifizierenden Daten werden gemäß der Qesü-Richtlinie von den Datenannahmestellen (DAS) systemweit einheitlich pseudonymisiert. Dies wird mithilfe eines Pseudonymisierungsprogramms (LEP) realisiert, welches von den DAS verwendet wird, um die leistungserbringeridentifizierenden Daten einerseits zu pseudonymisieren und andererseits auf dem Rückkanal (Rückmeldeberichte) wieder zu depseudonymisieren. Hierdurch wird erreicht, einzelne Berichte oder Protokolle den jeweiligen Leistungserbringern zuordnen zu können.

Mit diesem Dokument werden die dazu notwendigen Datenflüsse spezifiziert.

© 2015 AQUA-Institut GmbH

2. Datenfluss im Rahmen der Qesü

2.1. Schlüsselpaare

Die LQS[1]/KVen erzeugen mithilfe des PSP Schlüsselpaare. Der erzeugte private Schlüssel und das dazugehörende Passwort sind von der LQS/KV sicher zu verwahren, da der Verlust eine Repseudonymisierung aller bisher erzeugter Pseudonyme nach sich ziehen würde.

Der öffentliche Schlüssel wird von den LQS/KV an die entsprechende DAS-LE (falls abweichend), die DAS-SV und die DAS-KK übergeben. Wie die öffentlichen Schlüssel an die DAS-KK und DAS-SV übergeben werden, ist nicht Bestandteil dieser Spezifikation und muss direkt mit der jeweiligen Stelle abgestimmt werden.

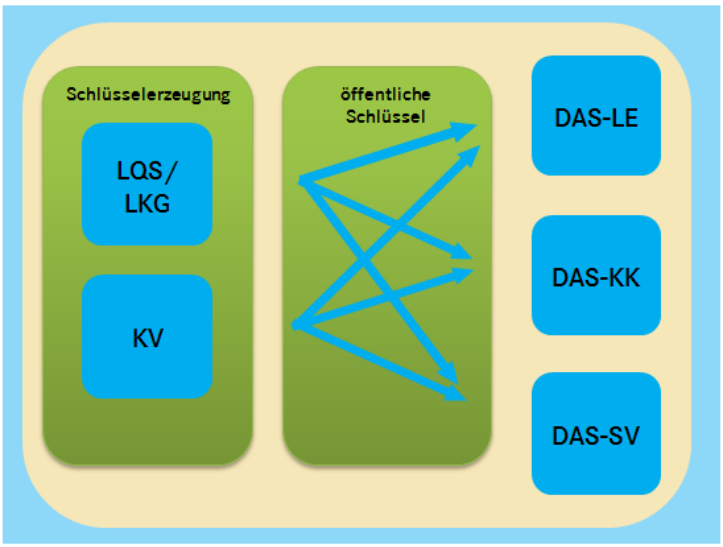


Abbildung 1: Datenfluss Schlüsselpaare

Achtung

Der öffentliche Schlüssel darf nur den im Datenfluss vorgesehenen Stellen zur Verfügung gestellt werden. Es ist. z.B. falsch diesen Schlüssel auf einer Webseite oder mit der Spezifikation öffentlich zu machen.

Der private Schlüssel dient nur dazu, Rückmeldeberichte mit Sozialdaten dem richtigen Leistungserbringer zuzuordnen zu können und darf daher Dritten nicht zur Verfügung gestellt werden.

2.2. Pseudonymisierung

Die DAS nutzen den öffentlichen Schlüssel um regionsbezogene, verfahrenseindeutige Pseudonyme zu erzeugen.

Dies kann während der Laufzeit der Datenverarbeitung geschehen oder initial durchgeführt und dann während der Datenverarbeitung aus einer bereitgestellten Mapping-Datei/Tabelle bezogen werden.

Hierbei ist sicherzustellen, dass nur valide leistungserbringeridentifizierende Daten pseudonymisiert werden. Sollte bei der Datenerfassung beim Leistungserbringer ein Fehler aufgetreten sein oder ist vergessen worden die IKNR/BSNR der LQS/KV mitzuteilen, so ist

[1] In der Quesü gibt es pro Region/Bundesland immer eine DAS. Dies können sowohl LQS als auch LKG sein.

© 2015 AQUA-Institut GmbH

diese Datenlieferung dem Leistungserbringer mit der entsprechenden Fehlermeldung gemäß der Spezifikation zurückzusenden.

Ein Pseudonym besteht aus:

- Dem **Leistungserbringeridentifizierenden Datum**
- Dem Pseudonymisierungsverfahren
- Der **Art der Datenannahme** (LQS/KV)
- Dem **Bundesland**/der **Region**
- Den spezifizierten Trennzeichen ($$, ##)



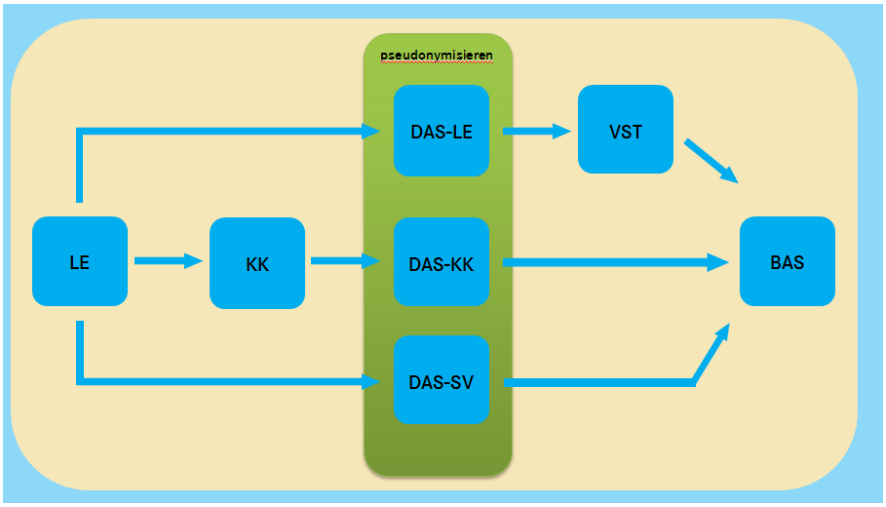


Abbildung 2: Datenfluss mit Pseudonymisierung

2.3. Rückmeldeberichte

Die Rückmeldeberichte der BAS werden zusammen mit einer Mappingdatei, welche die Pseudonyme und die Dateinamen der gelieferten Berichte enthält, an die LQS bzw. LKG/KV gesendet. Mit Hilfe des privaten Schlüssels können die Pseudonyme in der Mappingdatei depseudonymisiert und so die Berichte ihren Leistungserbringern zugeordnet werden.

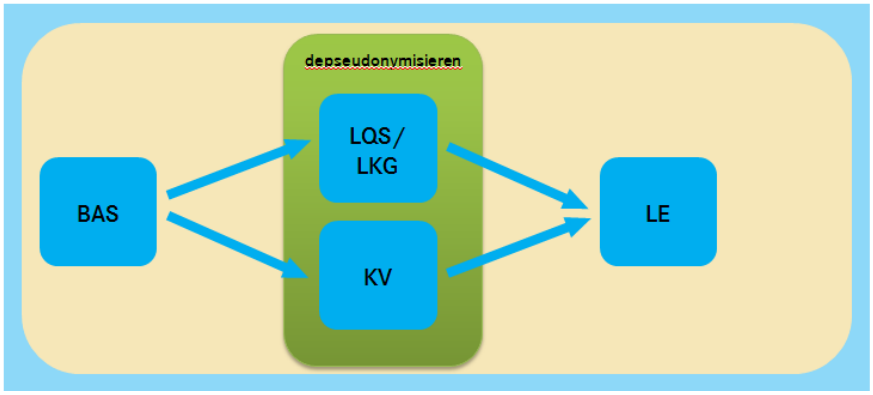


Abbildung 3: Datenfluss Rückkanal mit Depseudonymisierung

© 2015 AQUA-Institut GmbH

3. Datenfluss der Zusatzdatenverwaltung

Da es möglich ist, dass ein Leistungserbringer unterschiedliche leistungserbringeridentifizierende Daten besitzt (mehrere IKNR/BSNR), kann es auch vorkommen, dass bei der Abrechnung mit den Krankenkassen (KK) ein anderes leistungserbringeridentifizierendes Datum verwendet wird, als bei der Lieferung der QS-Daten an die LQS/KV. Dadurch würden unterschiedliche Pseudonyme eines Leistungserbringers an die BAS übersendet und diese zusammengehörenden Daten könnten nicht zusammengeführt werden. Daher wird ein Verfahren benötigt, welches die zusammengehörenden Pseudonyme der BAS bekannt macht.

Da sich jeder Leistungserbringer bei der LQS/KV registriert, soll durch diese Registrierung bei den LQS/KV pro Leistungserbringer eine Liste zusammengehörender IKNR bzw. BSNR geführt werden.

Mit Hilfe des PSP kann diese Liste einfach als Liste von zusammengehörenden Pseudonymen an die BAS übertragen werden.

Für die Zusatzdatenverwaltung bei der BAS stellt diese einen SOAP-Webservice zur Verfügung, über welchen Listen von zusammengehörigen Pseudonymen und Zusatzdaten, wie Standortnummern und Validitätszeiträume, an die BAS gesendet werden können.

Das zur Verfügung gestellte Pseudonymisierungsprogramm kann diesen Webservice bedienen und es den DAS-LE/LQS/KV so erleichtern die benötigten Daten an die BAS zu liefern.

3.1. Sicherheit

Der SOAP-Webservice bei der BAS ist gegen Angriffe abgesichert. Jede zur Datenlieferung berechtigte Stelle erhält von der BAS einen Benutzernamen und ein Passwort für die Benutzung des SOAP-Webservices. Zudem findet die Übermittlung der Daten verschlüsselt statt. Hierzu wird der gesamte SOAP-ENV: Body mit dem AES-Algorithmus im CBC-Verfahren mit einem PKCS5-Padding verschlüsselt.

Der Schlüsselstring kann mit jeder Version des Verschlüsselungsprogramms ausgetauscht werden.

© 2015 AQUA-Institut GmbH

So wird z.B. aus der SOAP Nachricht:

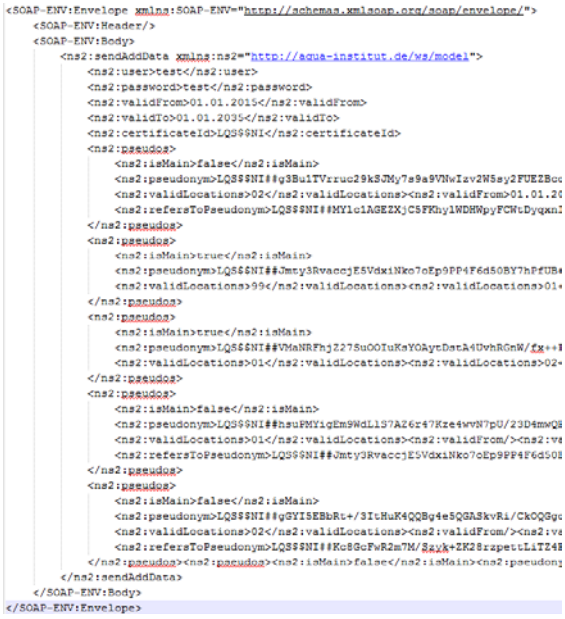


Abbildung 4 SOAP-Nachricht (unverschlüsselt)

Folgende verschlüsselte SOAP Message:

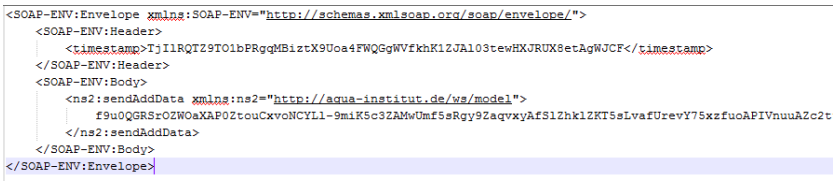


Abbildung 5 SOAP-Nachricht (verschlüsselt)

3.2. Zusatzdaten zum Transfer

pseudoMapping.csv

Die Zusatzdaten bestehen aus Listen von zusammengehörigen Pseudonymen, Standortnummern, Gültigkeitszeiträumen der leistungserbringeridentifizierenden Daten und ähnlichen Metadaten. Da das Datenmodell für CSV-Dateien geeignet sein muss, werden zwei getrennte CSV-Dateien benutzt um die Datenstruktur abzubilden.

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.

Beispiel

```
pseudonym;ist HauptPseudonym;Standortnummern;gültig ab;gültig
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