



Institut für Qualitätssicherung und
Transparenz im Gesundheitswesen

Systemweit einheitliche Leistungserbringer- pseudonymisierung

Datenflussspezifikation V03

Erstellt im Auftrag des
Gemeinsamen Bundesausschusses

Stand: 09. Februar 2017

Impressum

Thema:

Datenflussspezifikation. Systemweit einheitliche Leistungserbringerpseudonymisierung V03

Auftraggeber:

Gemeinsamer Bundesausschuss

Datum der Abgabe:

09. Februar 2017

Herausgeber:

IQTIG – Institut für Qualitätssicherung
und Transparenz im Gesundheitswesen

Katharina-Heinroth-Ufer 1
10787 Berlin

Telefon: (030) 58 58 26-0
Telefax: (030) 58 58 26-999

info@iqtig.org

<http://www.iqtig.org>

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
Tabellenverzeichnis.....	4
Abbildungsverzeichnis.....	4
1 Einleitung.....	6
2 Systemweit einheitliche Leistungserbringerpseudonymisierung	7
2.1 Fachlicher Hintergrund	7
2.2 Verschlüsselungsverfahren zur Pseudonymisierung	8
2.3 Erzeugung und Nutzung der Schlüsselpaare/Zertifikate.....	8
2.4 Pseudonymisierung der LE-identifizierenden Daten	9
2.5 Depseudonymisierung der LE-identifizierenden Daten	9
3 Datenflüsse.....	10
3.1 Verteilung der öffentlichen Zertifikate zwischen den DAS	10
3.1.1 Vorbereitungen zur Übermittlung des öffentlichen Zertifikats	11
3.1.2 Übermittlung des Zertifikats an die DAS-KK/DAS-SV	12
3.1.3 Übermittlung des Zertifikats von der LQS/LKG an die DAS.....	13
3.1.4 Entschlüsselung des übermittelten Zertifikats.....	13
3.2 Zusatzdatenverwaltung.....	14
Anhang	18

Tabellenverzeichnis

Tabelle 8: Spaltenbedeutung der CSV-Datei.....	15
Tabelle 11: Gültige Länderkürzel	18
Tabelle 12: Gültige Datenannahmestellen.....	18

Abbildungsverzeichnis

Abbildung 1: Datenfluss der QS-Daten, Abrechnungsdaten der LE und Sozialdaten angelehnt an das serielle Datenflussmodell der Qesü-RL.....	7
Abbildung 2: Datenfluss zur Übertragung des öffentlichen Zertifikats	10
Abbildung 3: Konfiguration des GPacker zur Verschlüsselung des öffentlichen Zertifikats	12
Abbildung 4: Konfiguration des GPacker zur Entschlüsselung des öffentlichen Zertifikats	14

Informationen zu diesem Dokument

Darstellungsmittel

Im Folgenden sind Symbole und Darstellungen besonderer Informationen beschrieben.



Achtung

Beschreibt Ursache, Folge und Vermeidung einer besonderen Fehlanwendung, die zu Problemen bei der Implementierung oder Ähnlichem führen kann.

Beispiel:

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

Zielgruppe

Dieses Dokument richtet sich an Datenannahmestellen und an die mit der Umsetzung beauftragten Softwarehersteller.

Änderungen in der Version 02 (gegenüber Version 2015 V1.0)

- Anpassung des Dokuments an das Layout des Instituts nach §137a SGB V (IQTIG)
- Überarbeitung der Gesamtstruktur des Dokuments
- Ergänzung des Datenflusses zur Übermittlung der öffentlichen Zertifikate zwischen den Datenannahmestellen

Änderungen in der Version 03 (gegenüber Version 02)

- Anpassung der Tabelle mit den gültigen Datenannahmestellen

1 Einleitung

Die durch die Richtlinie zur einrichtungs- und sektorenübergreifenden Qualitätssicherung (Qesü-RL)¹ vorgenommene Ausdehnung der Qualitätssicherung vom stationären auf den vertragsärztlichen Bereich sowie die Einbeziehung von Sozialdaten bei den Krankenkassen in die Qualitätsauswertungen erfordern eine einheitliche Pseudonymisierung der leistungserbringeridentifizierenden Daten. Die systemweit einheitliche Pseudonymisierung bildet die Grundlage für die Zusammenführung der Qualitätssicherungsdaten (QS-Daten) aus den unterschiedlichen Datenquellen in der Bundesauswertungsstelle (BAS) zur Berechnung der Qualitätsindikatoren sowie für den Versand der Rückmeldeberichte von der BAS an die Leistungserbringer (LE). Die Qesü-RL fordert die systemweit einheitliche Leistungserbringerpseudonymisierung (LE-Pseudonymisierung) in § 3 Abs. 2 Satz 4 der Anlage zu Teil 1 der Richtlinie:

Für die Pseudonymisierung stimmen die Datenannahmestellen nach § 9 Absatz 1 Satz 2 der Richtlinie (KV² bzw. KZV³), die Datenannahmestellen nach § 9 Absatz 1 Satz 3 der Richtlinie (LQS⁴/LKG⁵) sowie die Datenannahmestelle nach § 9 Absatz 1 Satz 5 der Richtlinie (DAS-KK⁶) untereinander ein Verfahren ab, welches sicherstellt, dass die Datenannahmestellen den gleichen leistungserbringeridentifizierenden Daten jeweils das gleiche Pseudonym zuordnen.

Die Datenflussspezifikation zur systemweit einheitlichen Leistungserbringerpseudonymisierung beschreibt die Datenflüsse, Dateiformate zum Datenaustausch sowie algorithmische Grundlagen der LE-Pseudonymisierung. Das Dokument richtet sich an die o. g. Datenannahmestellen und an die mit der Umsetzung beauftragten Softwarehersteller.

Die Erzeugung von kryptografischen Schlüsseln und von Zertifikaten und die Pseudonymisierung sowie Depseudonymisierung von leistungserbringeridentifizierenden Daten werden mithilfe des Leistungserbringerpseudonymisierungsprogramms durchgeführt. Die Anwenderdokumentation für das Programm befindet sich in der Datei „Pseudonymisierungsprogramm.pdf“ und ergänzt die Datenflussspezifikation. Auf der Website <http://www.iqtig.org> kann die aktuelle Version des Programms, der Anwenderdokumentation und der Datenflussspezifikation als ZIP-Archiv heruntergeladen werden.

¹ <https://www.g-ba.de/informationen/richtlinien/72/>

² Kassenärztliche Vereinigung (KV)

³ Kassenzahnärztliche Vereinigung (KZV)

⁴ Landesgeschäftsstelle für Qualitätssicherung (LQS)

⁵ Landeskrankenhausgesellschaft (LKG)

⁶ Datenannahmestelle für die Krankenkassen (DAS-KK)

2 Systemweit einheitliche Leistungserbringerpseudonymisierung

In diesem Kapitel werden der fachliche Hintergrund, die verwendeten kryptografischen Verfahren zur Erzeugung der LE-Pseudonyme aus den Institutionskennzeichen (IKNR) bzw. den Betriebsstättennummern (BSNR) der LE sowie die Erzeugung und die Verwendung der hierfür benötigten Schlüsselpaare für die systemweit einheitliche LE-Pseudonymisierung beschrieben.

2.1 Fachlicher Hintergrund

Im Rahmen der Qesü-RL werden QS-Daten von Leistungserbringern (stationär, vertragsärztlich, selektivvertraglich) sowie Sozialdaten bei den Krankenkassen über die DAS auf Landesebene an die BAS übermittelt (siehe Abbildung 1). Die QS-Daten werden von den jeweiligen LE über die DAS und die Vertrauensstelle (VST) an die BAS übertragen. Die Sozialdaten bei den Krankenkassen werden aus den Abrechnungsdaten der LE bei den Krankenkassen erzeugt und anschließend an die BAS übermittelt. Die DAS sind für die Pseudonymisierung und Depseudonymisierung der LE-identifizierenden Daten zuständig. Die QS-Daten des stationären Bereichs, die QS-Daten des ambulanten Bereichs und die Sozialdaten bei den Krankenkassen werden jedoch über unterschiedliche DAS an die BAS übermittelt. Die systemweit einheitliche LE-Pseudonymisierung stellt sicher, dass demselben LE in den unterschiedlichen DAS dasselbe Pseudonym zugeordnet wird. Dies ist eine grundlegende Voraussetzung, um in der BAS die QS-Daten mit den entsprechenden Sozialdaten desselben LE zusammenzuführen und auswerten zu können.

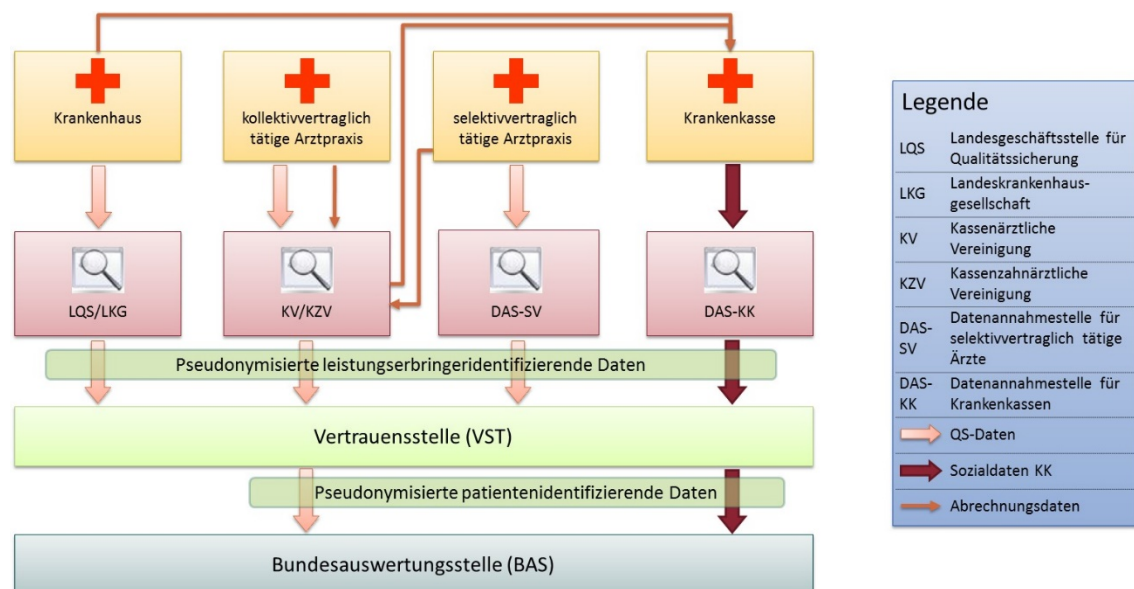


Abbildung 1: Datenfluss der QS-Daten, Abrechnungsdaten der LE und Sozialdaten angelehnt an das serielle Datenflussmodell der Qesü-RL

2.2 Verschlüsselungsverfahren zur Pseudonymisierung

Die Erstellung der LE-Pseudonyme wird mittels eines asymmetrischen (Public-Key-)Verschlüsselungsverfahrens durchgeführt. Im Gegensatz zu symmetrischen Verschlüsselungsverfahren wird kein gemeinsamer geheimer Schlüssel benötigt, den beide Kommunikationspartner kennen. Bei der asymmetrischen Verschlüsselung wird vom Benutzer (LQS/LKG/KV/KZV) ein Schlüsselpaar, bestehend aus einem privaten Schlüssel und einem öffentlichen Schlüssel, generiert. Die Schlüssel sind gemeinsam mit weiteren Informationen in Zertifikate eingebettet. Der private Schlüssel wird bei der Erzeugung des Schlüsselpaars mit einem Passwort geschützt. Der öffentliche Schlüssel wird an alle Kommunikationspartner verteilt. Mithilfe des öffentlichen Schlüssels können nun Daten verschlüsselt und sicher an den Besitzer des privaten Schlüssels übermittelt werden. Mit dem privaten Schlüssel und dem Passwort können die empfangenen Daten entschlüsselt werden. Die öffentlichen Schlüssel sind in Zertifikate eingebettet, die zusätzliche Metadaten enthalten.

Für die LE-Pseudonymisierung wird ein deterministisches, asymmetrisches Verschlüsselungsverfahren gebraucht. Verwendung findet der RSA-Verschlüsselungsalgorithmus von *Legion of the Bouncy Castle Inc*⁷. Dieser Algorithmus erfüllt sowohl die Anforderungen an die systemweit einheitliche Pseudonymisierung als auch die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Kriterien. Die deterministische Verschlüsselung nimmt in diesem Zusammenhang einen besonderen Stellenwert ein, da sichergestellt ist, dass die Verschlüsselung derselben LE-identifizierenden Daten mit dem gleichen öffentlichen Schlüssel bei verschiedenen DAS immer das gleiche Ergebnis produziert.



Achtung

Die Zertifikate mit den öffentlichen Schlüsseln dürfen nur den im Datenfluss vorgesehenen Stellen zur Verfügung gestellt werden. Es ist z. B. falsch, diese Zertifikate auf einer Website oder mit der Spezifikation zu veröffentlichen. In diesem Fall würde durch die Nutzung der deterministischen Verschlüsselung ein Besitzer von IKNR/BSNR die jeweiligen Pseudonyme erstellen können. Das Zertifikat, welches den privaten Schlüssel enthält, dient nur dazu, Rückmeldeberichte mit Sozialdaten dem richtigen Leistungserbringer zuordnen zu können, und darf daher Dritten nicht zur Verfügung gestellt werden.

2.3 Erzeugung und Nutzung der Schlüsselpaare/Zertifikate

Die Zertifikate mit den öffentlichen und privaten Schlüsseln werden bei den jeweiligen Institutionen auf Landesebene erzeugt (LQS/LKG/KV/KZV). Zur Erzeugung der Zertifikate wird das „Programm zur systemweit einheitlichen Leistungserbringerpseudonymisierung“ (PSP) genutzt. Eine Anleitung zur Nutzung des Programms befindet sich in der Datei „Pseudonymisierungsprogramm.pdf“.

⁷ <https://www.bouncycastle.org/>

Falls die LQS/LKG/KV/KZV nicht selbst die Funktion der DAS einnehmen, sind die entsprechenden öffentlichen Zertifikate an die jeweilige DAS zu übermitteln. Diese sind weiterhin an die DAS-KK und die DAS-SV zu übermitteln. Der Datenfluss zur Übermittlung der Zertifikate ist in Abschnitt 1.1 detailliert beschrieben.

2.4 Pseudonymisierung der LE-identifizierenden Daten

Die DAS nutzen das öffentliche Zertifikat, um regionsbezogene⁸ und für jedes QS-Verfahren eindeutige Pseudonyme zu erzeugen. Die Pseudonyme können während der Verarbeitung der Daten „on the fly“ mithilfe des Pseudonymisierungsprogramms erzeugt oder aus einer vorab generierten Mapping-Tabelle, welche das LE-identifizierende Datum und das zugehörige Pseudonym enthält, bezogen werden.

Hierbei ist sicherzustellen, dass nur valide LE-identifizierende Daten pseudonymisiert werden. Sollte bei der Datenerfassung beim Leistungserbringer ein Fehler aufgetreten sein oder ist vergessen worden, die IKNR/BSNR der LQS/LKG/KV/KZV mitzuteilen, so ist diese Datenlieferung dem Leistungserbringer mit der entsprechenden Fehlermeldung gemäß der Spezifikation zurückzusenden.

Ein LE-Pseudonym ist folgendermaßen aufgebaut:

- **Art der Datenannahme** (BAS/LQS/KV/SV)
- **Bundesland/Region**
- **spezifizierte Trennzeichen** (\$\$, ##)
- **Mit dem öffentlichen Schlüssel verschlüsselte IKNR/BSNR**

Beispiel:

LQS\$\$HH##fL1PqnoBIIAaM2bXSXvf1MOnhp4NhPx2sKqnIng

2.5 Depseudonymisierung der LE-identifizierenden Daten

Die Depseudonymisierung der LE-identifizierenden Daten wird bei den LQS/LKG/KV/KZV zum Versand der Rückmeldeberichte an die LE durchgeführt. Die Depseudonymisierung kann mithilfe des privaten Zertifikats der LQS/LKG/KV/KZV und des Pseudonymisierungsprogramms „on the fly“ während der Verarbeitung der Rückmeldeberichte oder mithilfe einer Mapping-Datei, die bei der Erzeugung der LE-Pseudonyme angelegt wurde, durchgeführt werden.

⁸ Gültige Regionen und Länderkürzel sind in Tabelle 11 gelistet.

3 Datenflüsse

3.1 Verteilung der öffentlichen Zertifikate zwischen den DAS

Die Schlüsselpaare zur LE-Pseudonymisierung, die in Zertifikate eingebettet sind, werden von den LQS/LKG/KV/KZV erstellt. Anschließend müssen die öffentlichen Zertifikate der zugehörigen DAS übermittelt werden, sofern diese getrennt betrieben werden. Die DAS-KK und die DAS-SV erstellen keine eigenen Schlüsselpaare, sondern nutzen die öffentlichen Zertifikate der LQS/LKG/KV/KZV. Dies erfordert, dass jede der eben genannten Stellen ihre öffentlichen Zertifikate an die DAS-KK und DAS-SV übermitteln müssen.

Zur Vermeidung zusätzlicher Belastungen in Bezug auf Softwareinstallation und Einarbeitungsaufwand für alle beteiligten Institutionen wird im Folgenden auf bereits etablierte Prozesse und Software zurückgegriffen (siehe Abbildung 2). Dieser Ablauf erfordert an einigen wenigen Stellen ein ungewöhnliches Vorgehen, stellt in der Gesamtbetrachtung jedoch die effizienteste Lösung dar. Die Nutzung bereits etablierter Software hat den zusätzlichen Vorteil, dass diese schon durch das BSI geprüft und abgenommen wurde.

Die folgende Software wird benötigt:

- PSP – Pseudonymisierungsprogramm zur einheitlichen LE-Pseudonymisierung
- GParser – Programm zur Ver- und Entschlüsselung der öffentlichen Zertifikate

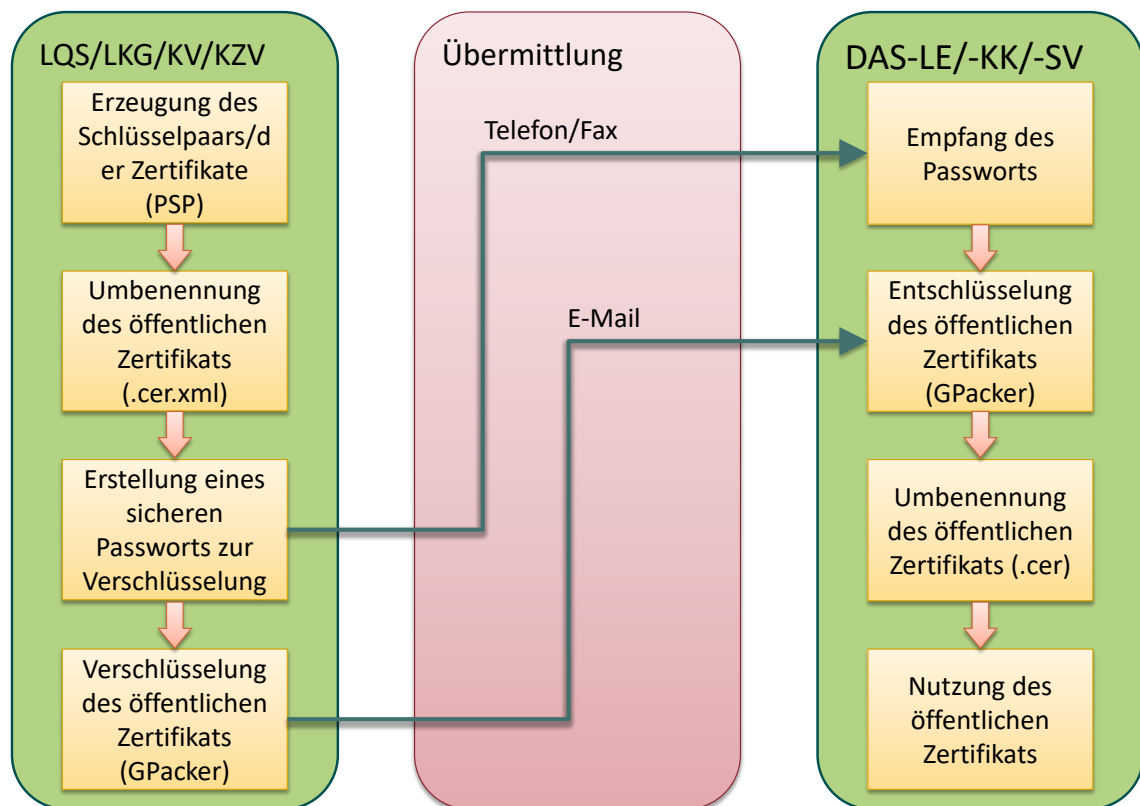


Abbildung 2: Datenfluss zur Übertragung des öffentlichen Zertifikats

3.1.1 Vorbereitungen zur Übermittlung des öffentlichen Zertifikats

Das öffentliche Zertifikat ist im Falle der LE-Pseudonymisierung lediglich für die beteiligten DAS verfügbar und darf nicht in die Hände Dritter gelangen. Deshalb ist das Zertifikat vor der Übertragung zu verschlüsseln.

An dieser Stelle wird davon ausgegangen, dass in der LQS/LKG/KV/KZV mit dem PSP bereits ein Schlüsselpaar erzeugt wurde und das Zertifikat mit dem privaten Schlüssel mit der Dateiendung .p12 sowie das Zertifikat mit dem öffentlichen Schlüssel mit der Dateiendung .cer vorliegen.



Achtung

Im Folgenden wird ausschließlich mit dem öffentlichen Zertifikat mit der Dateiendung .cer gearbeitet!

Das private Zertifikat darf unter keinen Umständen an Dritte weitergegeben werden! Sollte dies dennoch geschehen oder ein Schlüssel durch kompromittierte Systeme in die Hände unbefugter Dritter geraten, sind eine neue Schlüsselpaargenerierung mit anschließendem Austausch nach dem hier beschriebenen Verfahren und eine Re-Pseudonymisierung der bereits pseudonymisierten LE-Daten notwendig.

Es wird nun das Programm GParser verwendet, um das öffentliche Zertifikat mit einer symmetrischen Verschlüsselung⁹ und einem frei wählbaren Passwort zu verschlüsseln. Der GParser in der aktuellen Version ist nicht für die Übertragung der Zertifikate ausgelegt, d. h., es ist nur möglich, XML-Dateien zu verschlüsseln, jedoch nicht CER-Dateien. Mit den folgenden Schritten lässt sich das Problem allerdings umgehen:

1. Anfertigung einer Kopie des öffentlichen Zertifikats
2. Umbenennung der kopierten Datei durch Hinzufügen der Dateiendung .xml (.cer.xml)
3. Beantwortung der Frage, ob die Dateiendung wirklich umbenannt werden soll, mit „ja“

Anschließend kann die Datei mithilfe des GParser verschlüsselt werden. Hierzu muss der GParser folgendermaßen konfiguriert werden (siehe auch Abbildung 3):

- Eingabedatei: Auswahl der eben erstellten CER.XML-Datei
- Aktion: „Verschlüsseln“
- Rolle: „Dieses Auswahlfeld nicht ändern“
- Zu ver-/entschlüsseln: Häkchen setzen bei „Datei (.zip.aes)“
- Registrierungs-Nummer: beliebige Zeichenfolge, die echte Registrierungs-Nummer ist nicht notwendig
- Transport-Passwort: Passwort, das den Passwortrichtlinien entspricht (siehe unten)
- Ausgabeordner: Angabe des Pfades, an dem die Ausgabedatei abgelegt werden soll

⁹ Zur Verschlüsselung wird der Advanced Encryption Standard (AES) genutzt

Abbildung 3: Konfiguration des GPack zur Verschlüsselung des öffentlichen Zertifikats



Achtung Passwortrichtlinien

Die Passwörter zur Verschlüsselung müssen folgenden Bedingungen genügen:

- Mindestlänge: 12 Zeichen
- bestehend aus Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen

Nach der Verschlüsselung mit dem GPack befindet sich die verschlüsselte Ausgabedatei im Ausgabeordner. Für das in Abbildung 3 gezeigte Beispiel heißt die Ausgabedatei T-TEST-2016_03_11_151842.zip.aes. Diese Datei kann nun per E-Mail versendet werden.

3.1.2 Übermittlung des Zertifikats an die DAS-KK/DAS-SV

Die Übermittlung des öffentlichen Zertifikats an die DAS-KK/DAS-SV erfordert eine getrennte Übertragung der verschlüsselten Zertifikatsdatei und des Verschlüsselungspassworts über verschiedene Kommunikationskanäle.

Übertragung der verschlüsselten Zertifikatsdatei

Die verschlüsselte Zertifikatsdatei wird per E-Mail an die DAS-KK bzw. DAS-SV übermittelt. Die aktuelle Kontaktadresse ist auf der folgenden Website zu finden:

<http://www.vertrauensstelle-gba.de/kontakt.html>

Übermittlung des Passworts

Das Passwort zur Entschlüsselung wird entweder telefonisch oder per Fax an die DAS-KK bzw. DAS-SV übermittelt. Vor dem Versand des Passworts per Fax sollte die Übermittlung telefonisch angekündigt werden. Die aktuellen Telefon- und Faxnummern sind auf der Kontaktwebsite hinterlegt:

<http://www.vertrauensstelle-gba.de/kontakt.html>

3.1.3 Übermittlung des Zertifikats von der LQS/LKG an die DAS

Im Falle dass die LQS/LKG/KV/KZV nicht die Funktion der DAS übernehmen, ist es nötig, das öffentliche Zertifikat von der jeweiligen Institution an die entsprechende DAS zu übermitteln. Dieser Abschnitt definiert eine Übermittlung des Zertifikats angelehnt an die Übermittlung des Zertifikats an die DAS-KK bzw. DAS-SV. Sollten bereits sichere Kommunikationswege zwischen LQS/LKG/KV/KZV und der entsprechenden DAS etabliert worden sein, können diese alternativ genutzt werden.

Eine Übersicht der DAS ist in der QS-DOK-Datenbank der Basisspezifikation in der Tabelle `Institution` hinterlegt. Eine Zuordnung der DAS zu den jeweiligen QS-Verfahren befindet sich in der QS-DOK-Datenbank in der Tabelle `DatenserviceModul`.

Übertragung der verschlüsselten Zertifikatsdatei

Die verschlüsselte Zertifikatsdatei wird per E-Mail gesendet. Die Zieladresse wird von den jeweiligen Parteien bilateral ausgetauscht.

Übermittlung des Passworts

Das Passwort zur Entschlüsselung kann entweder telefonisch oder per Fax übermittelt werden. Die jeweiligen Ansprechpartner, Telefonnummern oder Faxnummern werden selbstständig zwischen den entsprechenden Parteien ausgetauscht.

3.1.4 Entschlüsselung des übermittelten Zertifikats

Der Empfänger ist im Besitz des verschlüsselten Zertifikats und des Passworts zur Entschlüsselung. Die Entschlüsselung wird mithilfe des GPackit folgendermaßen durchgeführt (siehe auch Abbildung 4):

- Eingabedatei: die per E-Mail empfangene ZIP.AES-Datei
- Aktion: „Entschlüsseln“ (wird automatisch ausgewählt)
- Transport-Passwort: das per Telefon/Fax übermittelte Passwort
- Ausgabeordner: Ordner, in dem die CER.XML-Datei abgelegt wird

Nach erfolgreicher Entschlüsselung des Zertifikats muss die Dateiendung wieder auf `.cer` geändert werden. Das Zertifikat mit dem öffentlichen Schlüssel kann nun genutzt werden.

Abbildung 4: Konfiguration des GParser zur Entschlüsselung des öffentlichen Zertifikats

3.2 Zusatzdatenverwaltung



Achtung

Start der Übermittlung der Zusatzdaten voraussichtlich ab Oktober 2016

Zur Übermittlung der Zusatzdaten von der DAS an das IQTIG wird bei der DAS das Pseudonymisierungsprogramm benötigt, welches sich zu einem Webservice beim IQTIG verbindet. Der Webservice beim IQTIG wird voraussichtlich im **Oktober 2016** mit der Veröffentlichung des DIMDI-Updates der Basisspezifikation in Betrieb genommen werden. Bis zum genannten Zeitpunkt ist eine Übertragung der Zusatzdaten an das IQTIG nicht möglich.

Ein LE kann unter Umständen mehrere LE-identifizierende Daten (mehrere IKNR/BSNR) besitzen. Dies kann dazu führen, dass bei der Abrechnung mit den Krankenkassen ein anderes LE-identifizierendes Datum verwendet wird als bei der Lieferung der QS-Daten an die LQS/KV. Dadurch würden unterschiedliche Pseudonyme eines Leistungserbringers an die BAS übersendet, was dazu führt, dass zusammengehörende Daten nicht zusammengeführt werden können. Daher wird ein Verfahren benötigt, welches die zusammengehörenden Pseudonyme der BAS bekannt macht.



Achtung

Datenlieferfrist zur Übermittlung der Zusatzdaten an das IQTIG

Die Zusatzdaten sind von den jeweiligen DAS bis spätestens **28. Februar** des Folgejahres an das IQTIG zu übermitteln!

Bei der Registrierung des LE bei der LQS/LKG/KV/KZV werden alle vorhandenen LE-identifizierenden Daten erfasst und als Listen zusammengehöriger IKNR/BSNR in der jeweiligen Landes-

stelle geführt. Die Listen bestehen aus Listen von zusammengehörigen Pseudonymen, Standortnummern, Gültigkeitszeiträumen der LE-identifizierenden Daten und ähnlichen Metadaten und werden in zwei separaten CSV-Dateien abgebildet.

Die Zusatzdatenverwaltung arbeitet mit zwei CSV-Dateien, Zusatzdaten.csv und Pseudomapping.csv, in denen die LQS/LKG/KV/KZV die LE-identifizierenden Daten erfassen, um sie an die BAS zu übermitteln. Beide Dateien sind obligatorisch, um die Daten an die BAS übermitteln zu können!

Zusatzdaten.csv

In der Datei Zusatzdaten.csv werden die Zusatzdaten zu den einzelnen LE-identifizierenden Daten erfasst. Sie ist die führende Datei. Die Inhalte der Zusatzdaten.csv werden vor der Übertragung an die BAS automatisch mithilfe des aktuellen öffentlichen Schlüssels der jeweiligen LQS/LKG/KV/KZV für jeweils alle aktuell gültigen Pseudonymisierungsverfahren pseudonymisiert, in eine für die Übertragung geeignete Datenstruktur überführt und um die Inhalte der Datei Pseudomapping.csv angereichert. In der Zusatzdaten.csv müssen lediglich die Haupt-LE-identifizierenden Daten vorhanden sein. Weitere LE-identifizierende Daten sind in der Datei Pseudomapping.csv zu erfassen. Sollte ein LE nur ein LE-identifizierendes Datum besitzen, muss dieses nicht in der Pseudomapping.csv enthalten sein.

Beispiel: Zusatzdaten.csv

```
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;;;
```



Achtung

Die CSV-Datei muss eine Kopfzeile besitzen!

Die Spalten der CSV-Datei besitzen folgende Bedeutung:

Tabelle 1: Spaltenbedeutung der CSV-Datei

Spalte	Beschreibung
pseudonym	Das LE-identifizierende Datum, welches vor der Übermittlung an die BAS automatisch pseudonymisiert wird.
ist HauptPseudonym	<ul style="list-style-type: none"> 1, wenn das Pseudonym dieses LE-identifizierenden Datums (IKNR/BSNR) als Haupt-Pseudonym gekennzeichnet werden soll. sonst 0

Spalte	Beschreibung
Standortnummern	(optional) Die für dieses LE-identifizierende Datum gültigen Standortnummern.
gültig ab	(optional) Sollte dieses LE-identifizierende Datum erst ab einem bestimmten Datum gültig sein, kann dies hier in der Form <dd.MM.yyyy> vermerkt werden.
gültig bis	(optional) Sollte dieses LE-identifizierende Datum nur bis zu einem bestimmten Datum gültig sein, kann dies hier in der Form <dd.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“.

Pseudomapping.csv

In der Datei `Pseudomapping.csv` werden pro Zeile die zusammengehörenden LE-identifizierenden Daten (IKNR/BSNR) eines LE unverschlüsselt aufgelistet. Die Haupt-IKNR bzw. Haupt-BSNR steht an erster Stelle, gefolgt von den zusätzlichen IKNR/BSNR (siehe Beispiel:Pseudomapping.csv).

Vor der Übertragung der Daten an die BAS werden die IKNR/BSNR durch das Pseudonymisierungsprogramm automatisch mithilfe des aktuellen öffentlichen Schlüssels der jeweiligen LQS/LKG/KV/KZV pseudonymisiert. Hierbei werden jedes Hauptpseudonym und alle zugehörigen Pseudonyme automatisch für jeweils alle aktuell gültigen Pseudonymisierungsverfahren pseudonymisiert und an die BAS versendet.

Beispiel: Pseudomapping.csv

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

```

Übermittlung der Pseudonyme an die BAS

Mithilfe des PSP kann die 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 Validitätszeiträumen, an die BAS gesendet werden können. Das zur Verfügung gestellte Pseudonymisierungsprogramm kann diesen Webservice bedienen und es den Datenannahmestellen der Leistungserbringer (DAS-LE), LQS, LKG, KV und KZV so erleichtern, die benötigten Daten an die BAS zu liefern.

Der SOAP-Webservice bei der BAS ist gegen Angriffe abgesichert. Jede zur Datenlieferung berechnete Stelle erhält von der BAS einen Benutzernamen und ein Passwort für die Benutzung des SOAP-Webservice. 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.

Anhang

Tabelle 2: Gültige Länderkürzel

Kürzel	Bedeutung
BU	Bundesweit
BA	Bayern
BB	Brandenburg
BE	Berlin
BW	Baden-Württemberg
HB	Bremen
HE	Hessen
HH	Hamburg
MV	Mecklenburg-Vorpommern
NI	Niedersachsen
NO	Nordrhein
NW	Nordrhein-Westfalen
RP	Rheinland-Pfalz
SH	Schleswig-Holstein
SL	Saarland
SN	Sachsen
ST	Sachsen-Anhalt
TH	Thüringen
WL	Westfalen-Lippe
TESTLAND	Zur Nutzung auf den Testdatenstrecken zwischen Softwareanbietern und Datenannahmestellen

Tabelle 3: Gültige Datenannahmestellen

Kürzel	Datenannahmestelle
LQS	Landesgeschäftsstelle für Qualitätssicherung
BAS	Bundesauswertungsstelle
KV	Kassenärztliche Vereinigung
SV	Datenannahmestelle für selektivvertraglich erbrachte Leistungen