Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

1.1 Inhalt und Zielgruppe des Dokuments

Das folgende Dokument beschreibt die technische Funktionsweise der Schnittstelle zu Arbeitgebern, Zahlstellen und sonstigen Meldepflichtigen (im Folgenden „AG“ genannt) des GKV-Kommunikationsservers, die Übertragungsprozesse, sowie den Aufbau der übertragenen Daten und Pakete. Die technische Tiefe der Beschreibung zielt auf Softwareersteller von Entgeltabrechnungsprogrammen ab. Das Dokument bietet zuerst einen grundsätzlichen Überblick über den GKV-Kommunikationsserver mit den entsprechenden Kommunikationsprozessen und beschreibt im Anschluss jeden Prozess detailliert.

1.2 Funktionsweise des Kommunikationsservers

XML allgemein und damit auch der von der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) propagierte Standard „eXTra“ gewinnen zunehmend an Bedeutung. Dazu wurde der GKV-Kommunikationsserver nicht nur als zentrale Stelle für den Rückmeldeweg konzipiert, sondern auch als ***„Tor“ zu den Datenaustauschverfahren***. Dieses „Tor“ nimmt Meldungen im eXTra-Standard an, die über das https-Protokoll transportiert werden. Der eXTra-Standard stellt alle Elemente, die vorher bereits im Auftragssatz existierten, im XML-Format zum Transport zur Verfügung. Der AG ist verpflichtet, in allen elektronischen Meldeverfahren mit der GKV, den berufsständischen Versorgungseinrichtungen, der Deutschen Gesetzlichen Unfallversicherung und der Bundesagentur für Arbeit über den GKV-Kommunikationsserver zu kommunizieren. Die weitere Kommunikation mit den DAVn ist Aufgabe des GKV-Kommunikationsservers.

Das folgende Schaubild veranschaulicht die Rolle des GKV-Kommunikationsservers als ***„Tor“-mit Maklerfunktion***:

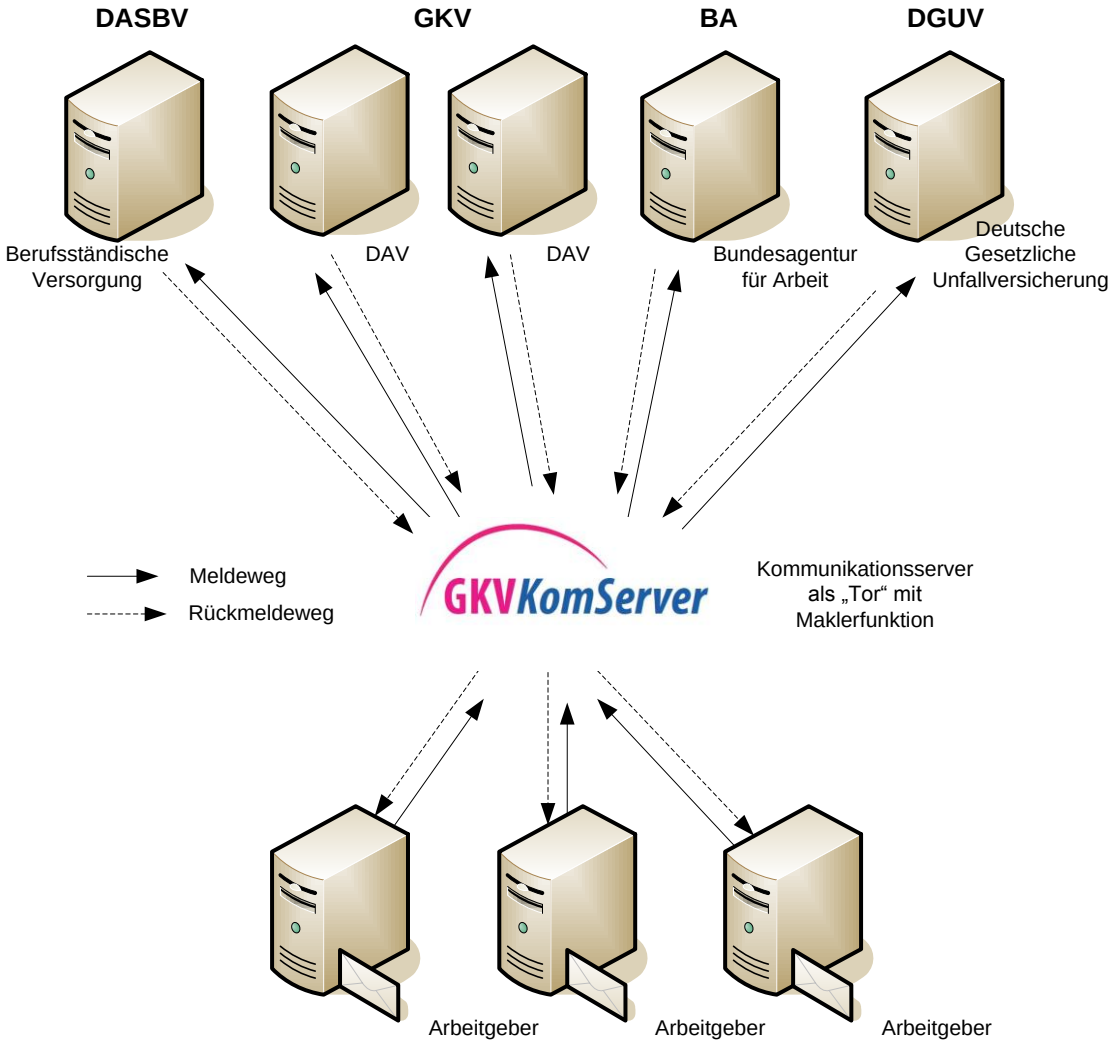

Abbildung 1: Der GKV-Kommunikationsserver als Makler zwischen AG und GKV

2 Grundsätzliche Informationen

Die Erstellung und Übermittlung der Meldungen kann durch den AG an einen Dritten delegiert werden, der in diesem Fall nicht nur als Absender sondern in allen Sätzen der Datenlieferung auch als „Ersteller“ der Datei auftreten muss.

Bei Meldungen der Krankenkassen an die AG, denen keine direkte AG-Meldung vorausging aber bereits vorher eine Meldung des AG an diese Krankenkasse durchgeführt wurde (z.B. im Zahlstellenmeldeverfahren), müssen die DAVn oder ihre Mitgliedskassen vermerken, welcher Empfänger (AG-Kommunikationspartner) für die Betriebsnummer (BBNR) des Verursachers zuständig ist. Dabei ist der Ersteller der letzten vorausgegangenen und fehlerlos verarbeiteten Meldung von der DAV als Empfänger anzugeben. Daraus ergibt sich, dass bei einem Wechsel des Erstellers diese Information den zuständigen Krankenkassen mitgeteilt werden muss. Wie diese Mitteilung erfolgen soll, ist dem jeweiligen Fachverfahren zu entnehmen.

In der aktuellen Fassung des gemeinsamen Rundschreibens „Gemeinsames Meldeverfahren zur Kranken-, Pflege-, Renten- und Arbeitslosenversicherung“[1] ist zum Datenaustausch mit Arbeitgebern geregelt worden, dass für die Verschlüsselung einer Rückmeldung jeder BBNR ein Zertifikat zugeordnet werden muss und ausschließlich das aktuellste Zertifikat für die BBNR des Empfängers verwendet darf. Daher muss jede Meldestelle mit einer eigenen BBNR und einem eigenen Zertifikat agieren.

Die BBNR des Absenders wird somit für die Verschlüsselung der Rückmeldedateien und als Abrufkriterium für den GKV-Kommunikationsserver zur Zuordnung der richtigen Rückmeldungen genutzt.

[1] http://www.gkv-datenaustausch.de/Gemeinsame_Grundsaetze.gkvnet

3 Technische Spezifikation der Schnittstellen des GKV-Kommunikationsservers

3.1 Übertragungsprotokoll

Der GKV-Kommunikationsserver beinhaltet einen Webserver-Dienst, welcher Anfragen per „POST- Methode“[2] auf Port 443 (https) unter einer dedizierten URL erwartet. Übertragen werden können XML-Dateien im eXTra-Format. Aktuell wird die Version 1.4 des eXTra-Formats unterstützt. Diese ist, je nach Geschäftsfall, unter folgenden URLs erreichbar:

- **Abgabe von Meldungen:**

  eXTra 1.4: https://verarbeitung.gkv-kommunikationsserver.de/meldung/extra14.meldung

- **Anfrage von Rückmeldungen:**

  eXTra 1.4: https://verarbeitung.gkv-kommunikationsserver.de/anfrage/extra14.anfrage

- **Abgabe der Empfangsquittung:**

  eXTra 1.4: https://verarbeitung.gkv-kommunikationsserver.de/quittung/extra14.quittung

[2] http://tools.ietf.org/html/rfc2616

3.2 Datenformat XML (Extensible Markup Language)

XML wird als Basisformat verwendet, um die zu übertragenden Daten in eine geordnete Struktur zu bringen. An der Arbeitgeberschnittstelle des KomServer wird, wie bereits erwähnt, das profilierte eXTra-Format (XML) für den Datenaustausch verwendet. Als Vorlage für die einzelnen Kommunikationsprozesse werden sog. Schema-Dateien verwendet. Die Schemadateien (*.xsd)[3] beinhalten die Rahmenvorgaben für die anschließende, mit Daten gefüllte XML-Datei und werden für die Validierung der XML-Dateien verwendet werden. Eine Validierung der erzeugten XML-Dateien wird durch den GKV-Kommunikationsserver durchgeführt. Wünschenswert ist eine „Vorvalidierung“ durch die Arbeitgeber-Software, um fehlerhafte XML-Dateien bereits vor dem Versand zu erkennen und zu korrigieren.

[3] http://www.w3.org/XML/Schema

3.3 Datenformat eXTra-Standard

eXTra ist ein einheitliches XML-basiertes Transportverfahren. eXTra stellt XML-Strukturelemente für verschiedene Übertragungsmodelle bereit. Das Modell von eXTra beinhaltet sechs Rollen und drei Ebenen. Die Rollenfunktion sind auf Senderseite der Erzeuger (fachlicher Sender), der logische und der physische Sender. Auf Empfängerseite gibt es den physischen und den logischen Empfänger sowie den Verwerter (fachlicher Empfänger). Die drei Ebenen sind die Nachrichtenebene, die Logistikebene und die Transportebene, über die sich die jeweiligen Kommunikationspartner austauschen.

eXTra betrachtet den Transport der fachlichen Daten vom Erzeuger (fachlicher Sender) bis zum Verwerter (fachlicher Empfänger). eXTra beschränkt sich in seinen Vorgaben auf den logischen Transport zwischen einem physischen Sender und Empfänger.

Der GKV-Kommunikationsserver nutzt ausschließlich die Logistikebene und die Transportebene des eXTra-Verfahrens, die Nachrichtenebene wird nicht verwendet.

Die für die Arbeitgeberschnittstelle des GKV-Kommunikationsservers benötigten und durch die ITSG vorgegebenen Schema- und Beispieldateien im eXTra-Format werden in den jeweils aktuellen Versionen unter „http://www.extra-standard.de“ veröffentlicht.

3.4 Verschlüsselungsverfahren

Der GKV-Kommunikationsserver unterstützt ausschließlich die Vorgaben der „Anlage 16 („Security Schnittstelle“) in der aktuell gültigen Version zur Verschlüsselung der im eXTra-Schema enthaltenen Nutzdaten.

3.5 Zertifikatsformat

Der GKV-Kommunikationsserver verwendet ausschließlich Zertifikate nach der „Anlage 16 („Security Schnittstelle“) in der aktuell gültigen Version. Das Zertifikat wird auch die Client-Authentisierung beim Aufbau der https-Verbindung verwendet. Serverseitig wird an dieser Stelle ein Standard-SSL-Zertifikat verwendet.

3.6 Kodierungsverfahren

Nutzdaten, Statusanfragen und Empfangsquittungen werden standardmäßig mit dem Kodierungsverfahren Base64 kodiert und somit in unabhängige ASCII-Zeichenketten gebracht. Bei der Base64-Kodierung sind keine Whitespaces oder Zeilenumbrüche zulässig. Die Zeichen werden nach ISO 8859-1 kodiert.

3.7 AG Schnittstelle

3.7.1 Überblick

Bei https werden die Nachrichten über eine auf Transportebene verschlüsselte SSL-Verbindung übertragen werden. Diese Verbindung wird mittels des sogenannten SSL Handshake Protocol aufgebaut, das die folgenden Funktionen erfüllt:

- Identifikation und Authentifizierung beider Kommunikationspartner
- Aushandeln zu benutzender kryptografischer Algorithmen und Schlüssel

Im Folgenden werden die Unterschiede beim Senden von Meldungen bzw. Statusanfragen und Quittungen an den KomServer über https in allgemeiner Form dargestellt.

3.7.2 Verbindungsaufbau

Das https-Protokoll besitzt mit dem SSL Handshake Protocol einen Mechanismus, mit dem ein sicherer Kommunikationskanal aufgebaut werden kann, noch bevor die ersten Bits des Anwendungsdatenstromes ausgetauscht werden. Im letzten Schritt des Authentifizierungsprozesses wird ein eindeutiger Schlüssel (Session Key) erstellt, der anschließend für die Verschlüsselung der Nachricht(en) verwendet wird.
Der Handshake kann in vier Phasen unterteilt werden:

Phase 1: Der Client schickt zum Server ein „client_hello“, und der Server antwortet dem Client mit einem „server_hello“.

Phase 2: Der Server identifiziert sich gegenüber dem Client, indem er sein Zertifikat an den Client übermittelt. Außerdem kann der Server den Client dazu auffordern seinerseits ein Zertifikat zur Authentifizierung zu schicken (CertificateRequest).

Phase 3: Der Client verifiziert das erhaltene Serverzertifikat. Bei Misserfolg oder wenn die Vertrauenswürdigkeit des Zertifikats nicht eindeutig gegeben ist, sollte die Verbindung abgebrochen werden. Sofern vom Server ein Clientzertifikat angefordert wurde wird auch dieser dieses verifizieren. Besitzt der Client kein Zertifikat, so antwortet der Server mit einem „NoCertificate“ alert.

Phase 4: Diese Phase schließt den Handshake mit dem Festlegen des einmaligen Session Key ab. Das ist ein einmalig benutzbarer symmetrischer Schlüssel, der während der Verbindung zum Ver- und Entschlüsseln der Daten genutzt wird. Die Nachrichten, die die Kommunikationspartner sich nun gegenseitig zusenden, werden nur noch verschlüsselt übertragen.

Die Verwendung des SSL-Client-Zertifikats für den Aufbau einer SSL-Verbindung zum KomServer ist zwingend erforderlich!

3.7.3 Implementierungshinweise

Für das SSL Handshake Protocol existieren je nach der clientseitig verwendeten Technologie verschiedene Implementierungen. Folgende allgemeine Hinweise müssen bei der Konfiguration der SSL-Verbindung beachtet werden:

Der AG muss beim Aufbau der https-Verbindung und der damit verbundenen SSL-Client-Authentifizierung das von einem registrierten Trustcenter zum Datenaustausch mit der Sozialversicherung auf dessen Betriebsnummer ausgestellte Zertifikat als „SSL-Client-Zertifikat“ an den KomServer übermitteln. Hierbei gilt zu beachten, dass diese Art der Kommunikation ggf. vorerst in der internen Firewall des AG durch die dortige IT Abteilung freizuschalten ist.Der AG muss im Gegenzug das vom KomServer übermittelte Serverzertifikat prüfenund die Verbindung bei erkannten Fehlern beenden. Hierfür müssen ggf. die Root-Zertifikate für die „Vertrauenswürdige Stammzertifizierungsstellen“ sowie „Zwischenzertifizierungsstellen“ zuvor in der eingesetzten Software eingespielt werden. Sie erhalten diese unter folgendem Link:

http://www.itsg.de/tc_root_zertifikate.html

Die Verschlüsselung der Nutzdaten ist auch bei der Verwendung von https zwingend erforderlich. Die Statusanfragen und Quittungen werden jedoch nicht auf Nutzdatenebene verschlüsselt, diese werden lediglich BASE64-codiert.

Bei dem Zertifikat handelt es sich um ein SSL-Serverzertifikat, welches nur zur Verschlüsselung der Kommunikation eingesetzt wird. Das Zertifikat des KomServers kann sich– z.B. nach Ablauf des Gültigkeitszeitraums – ändern.

3.7.4 Zusammenfassung

Die folgende Tabelle fasst die wesentlichen Punkte zusammen, die bei der Kommunikation mit dem GKV-Kommunikationsserver über https beachtet werden müssen:

https-Schnittstelle
Unterstützt ausschließlich eXTra-Standard 1.4
Authentifizierung mittels SSL Handshake Protokoll; siehe Kapitel 3.7.2. AG-Zertifikat muss nur bei Meldungen in eXTra-Struktur integriert werden
Nur Quittung und Statusanfrage: Nutzdaten müssen lediglich Base64-kodiert werden Kennzeichnung im (Encryption) Algorithm-Element: `<xplg:Algorithm id="http://www.extra-standard.de/transforms/encryption/NONE"/>`
URL: https://...

4 Kommunikationsprozesse zwischen Arbeitgeber und GKV-Kommunikationsserver

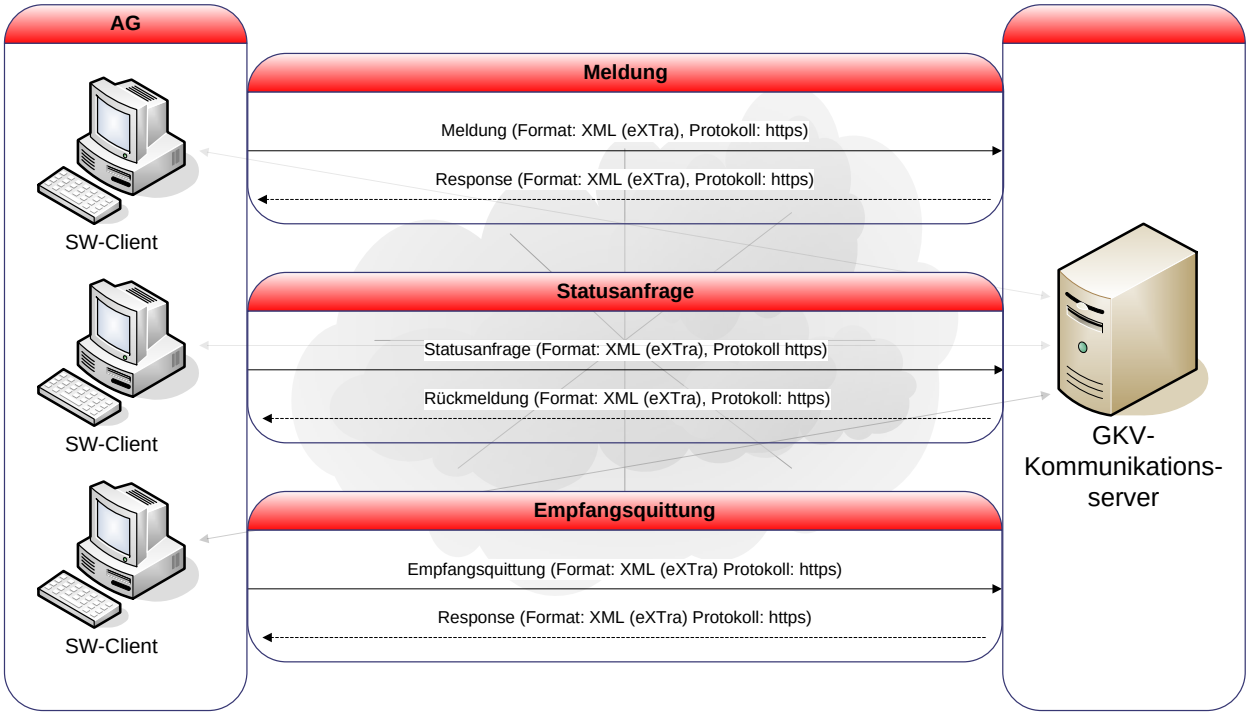

Abbildung 2: Übersicht der Kommunikationsprozesse zwischen Arbeitgeber und GKV-Kommunikationsserver

4.1 Meldungen

Die Meldungen des AG werden in einer XML-Datei an den GKV-Kommunikationsserver übermittelt. Der Aufbau der XML-Datei ist konform zum eXTra-Standard. Der GKV-Kommunikationsserver ist dabei in der Lage, Nachrichten bis zu einer Gesamtgröße von 20 MB zu verarbeiten und den Kommunikationskanal bis zu 180 Sekunden für Datenübertragungen offen zu halten.

Der GKV-Kommunikationsserver führt beim Empfang des Requests eine Schemaprüfung der XML-Dateien durch und leitet, nach erfolgreicher Prüfung, die Daten in einem internen Verfahren an die entsprechende DAV weiter.

Folgende Abbildung verdeutlicht den Verarbeitungs- und Kommunikationsweg zwischen den einzelnen Stellen:

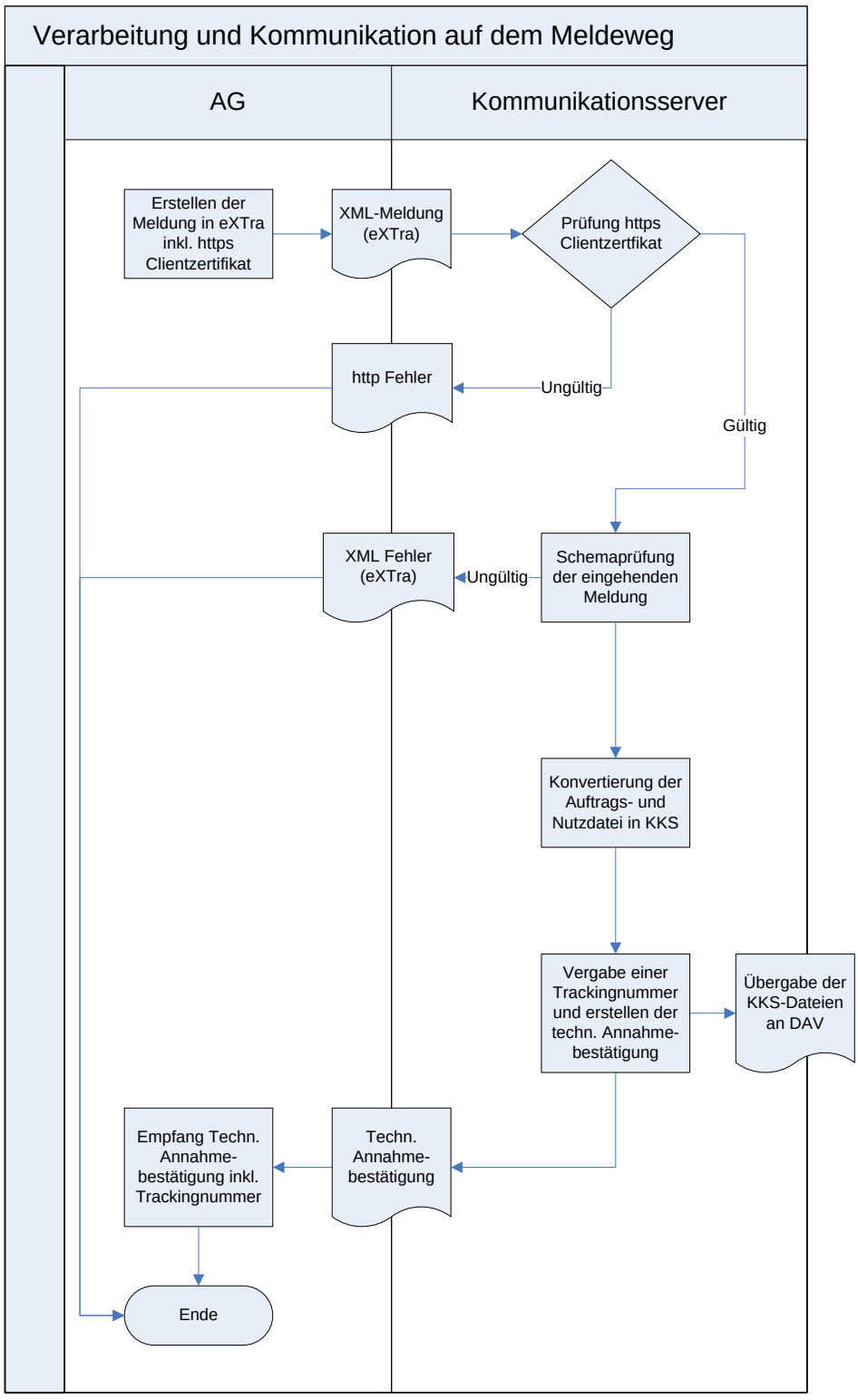

Abbildung 3: Flussdiagramm zum Verarbeitungsablauf der Meldungen des AG

4.1.1 Aufbau der Meldung

Die Meldung des AG erfolgt in einer XML-Datei nach dem eXTra-Standard. Die Adressierung der Meldedatei erfolgt an die gemäß der Anlage 17 „Datenannahmestellen von Meldungen nach der DEÜV, DÜBAK und von Beitragsnachweisen“ zum gemeinsamen Rundschreiben „Gemeinsames Meldeverfahren zur Kranken-, Pflege-, Renten- und Arbeitslosenversicherung“[4] zuständige DAV und muss auch vom AG für diese DAV verschlüsselt werden. Der Inhalt der Meldedatei ist in den jeweiligen Fachverfahren definiert.

[4] https://www.gkv-datenaustausch.de/arbeitgeber/deuev/gemeinsame_rundschreiben/gemeinsame_rundschreiben.jsp

4.1.2 Übertragung der Meldungen

Die Aufgabe des KomServers ist es, Meldungsdaten an die Endempfänger, die Datenannahme- und Verteilstellen der gesetzlichen Krankenkassen (DAVn), weiterzuleiten. Der AG signiert daher jede einzelne Meldung und verschlüsselt sie unter Verwendung des PKCS#7-Standards für die Empfänger-DAV. Der Arbeitgeber sendet die signierten und verschlüsselten Daten anschließend über eine https-Verbindung an den KomServer.

Vor dem eigentlichen Datentransfer wird eine sichere SSL-Verbindung zwischen AG und KomServer aufgebaut (siehe Kapitel 3.7.2), über die die AG-Daten anschließend an den KomServer übermittelt werden.

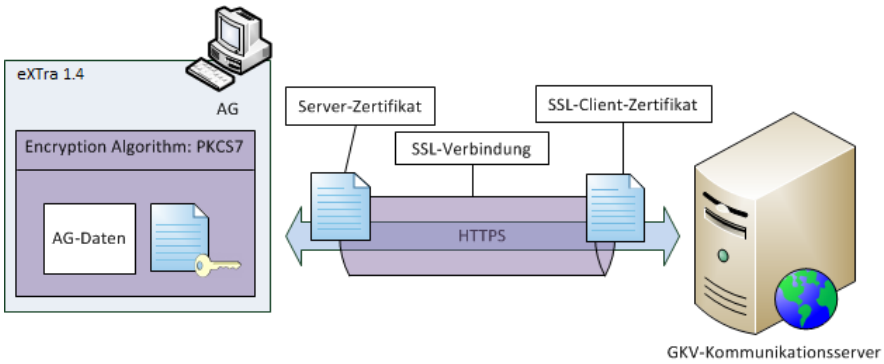

Abbildung 4: Senden einer Meldung an den KomServer

Die Lieferung der XML-Datei wird vom Webserver-Dienst des GKV-Kommunikationsservers über https unter der im Kapitel 3.1 angegebenen dedizierten URL zur Datenannahme entgegen genommen. Die Kommunikation zwischen AG und GKV-Kommunikationsserver basiert auf einem „POST-Request“[5] ohne die Angabe von Namen-Wert-Paaren und ohne die Angabe von http-Argumenten in der URL. Der https-Request und die https-Response müssen als Binary-Request ausgeführt werden, wobei der Http-Header lediglich die Attribute "Content-Type" und "Content-Length" enthalten muss. Der Http-Body enthält ausschließlich die zu übermittelnden Daten.

- **Inhalt des Http-Headers:**
  Content-Type: application/octet-stream
  Content-Length: Größe des http-body in Bytes
- **Inhalt des Http-Body:**
  Der Inhalt des Http-Body ist das eXtra-Datenpaket.

[5] http://tools.ietf.org/html/rfc2616

4.1.3 Prüfungen des GKV-Kommunikationsserver bei Meldungen

4.1.3.1 Schemaprüfung der übertragenen XML-Datei

Der GKV-Kommunikationsserver prüft die vom AG gelieferte XML-Datei (eXTra-Request) gegen das entsprechende XML-Schema. Wenn Fehler in der Struktur der angelieferten XML-Datei gefunden oder Wertebereiche verletzt werden, wird eine Antwort für den AG erstellt, die im Element „Report“ auf Transportebene die entsprechende Fehlermeldung beinhaltet. Hier werden lediglich die mit der Kommunikation verbundenen Fehler zurückgemeldet (z.B. „DAV nicht bekannt“).

Kann der GKV-Kommunikationsserver keine eXTra-Antwort an den AG erstellen, wird als Antwort eine „Error.xml“ (im Anhang A XML-Schema- und Beispieldateiengenauer beschrieben) erstellt.

Achtung: Der Inhalt der Meldung wird in beiden Fällen auf dem GKV-Kommunikationsserver verworfen.

4.1.4 Verarbeitung der Meldungen durch den GKV-Kommunikationsserver

Nach erfolgreicher Schemaprüfung wird auf dem GKV-Kommunikationsserver die Paketebene auf fachliche und technische Fehler überprüft. Dabei beschränkt sich die technische Fehlerprüfung nur auf die korrekte Dekodierung des Elements „Base64CharSequence“. Wenn Fehler bei der Prüfung auftreten, wird für das jeweilige Paket eine Antwort für den AG erstellt, die im Element „Report“ auf Paketebene die entsprechende Fehlermeldung beinhaltet. Sobald die Prüfung abgeschlossen ist, werden die verschlüsselten Nutzdaten und Steuerungsdaten aus der XML-Datei extrahiert und den DAVn zur weiteren Verarbeitung zur Verfügung gestellt. Eine Prüfung der Nutzdaten erfolgt durch den GKV-Kommunikationsserver in diesem Fall nicht, da diese verschlüsselt sind und die notwendigen Schlüssel nur der jeweiligen DAV zur Verfügung stehen.

In jeder Meldung können mehrere Pakete mit jeweils einer Nutzdatendatei übermittelt werden. Da die Ablehnung der Nutzdaten auf Paketebene erfolgt, ist es möglich, dass innerhalb einer Lieferung einige Pakete akzeptiert und andere abgelehnt werden.

4.1.5 Vergabe einer eindeutigen TrackingID

Nach erfolgreicher Prüfung erstellt der GKV-Kommunikationsserver eine eindeutige 23-stellige Trackingnummer (ResponseID auf Paketebene) zu jeder Nutzdatendatei . Diese kann genutzt werden, um den Status der Meldung und Quittung bei der jeweiligen DAV-Hotline abzufragen und um die zugehörige Rückmeldung der DAV der Meldung zuordnen zu können.

4.1.6 Antwort des GKV-Kommunikationsservers an den AG

Die Response des GKV-Kommunikationsservers wird als XML-Datei nach dem eXTra-Standard erstellt. Sowohl die XML-Schemadatei, als auch eine XML-Beispieldatei für die Response sind im Abschnitt Anhang A XML-Schema- und Beispieldateien zu finden.

Als Antwort erhält der AG eine technische Annahmebestätigung der Daten („Acknowledgement“) vom GKV-Kommunikationsserver. Diese sagt ausschließlich aus, dass die Daten in einer korrekten XML-Struktur übermittelt wurden und vom GKV-Kommunikationsserver der adressierten DAV zugestellt werden. Die Annahmebestätigung trifft keine Aussage darüber, ob die Daten durch die DAV entschlüsselt und verarbeitet werden konnten und ob mit einem zugelassenen Zertifikat signiert wurden. Im Element „ResponseID“ wird auf Paketebene die vom GKV-Kommunikationsserver vergebene TrackingID an den AG zurück gemeldet. Zusätzlich vergibt der GKV-Kommunikationsserver eine Sendungsnummer (ResponseID) für die Transportebene. Die ResponseID der Transportebene entspricht dem gleich Aufbau der TrackingID auf Paketebene, wird aber nicht weiter verwendet.

4.2 Statusanfrage und Rückmeldungen

Als „Statusanfrage“ wird eine Anfrage (Request) des AG an den GKV-Kommunikationsserver bezeichnet, ob neue Rückmeldungen für seine Betriebsnummer vorliegen. Als „Rückmeldung“ werden sowohl die Verarbeitungsbestätigungen und Fehlermeldungen zu AG-Meldungen (inkl. der technischen Fehlerrückmeldungen) als auch Meldungen der SV-Träger an die AG bezeichnet.

Die Statusanfrage wird nach dem eXTra-Standard aufgebaut. Beim Aufbau der https-Verbindung wird der sendende AG auf Basis des SSL Handshakes authentisiert. Ist der AG identifiziert und berechtigt, werden die entsprechenden Rückmeldungen der DAVn an den AG übermittelt.

Die Rückmeldungen an den AG werden spätestens nach 25 Sekunden als XML-Datei nach dem eXTra-Standard über die bis zu 180 Sekunden für Datenübertragungen offen gehaltene https-Verbindung übertragen.

Die nachfolgende Abbildung verdeutlicht den Verarbeitungs- und Kommunikationsweg zwischen den einzelnen Stellen:

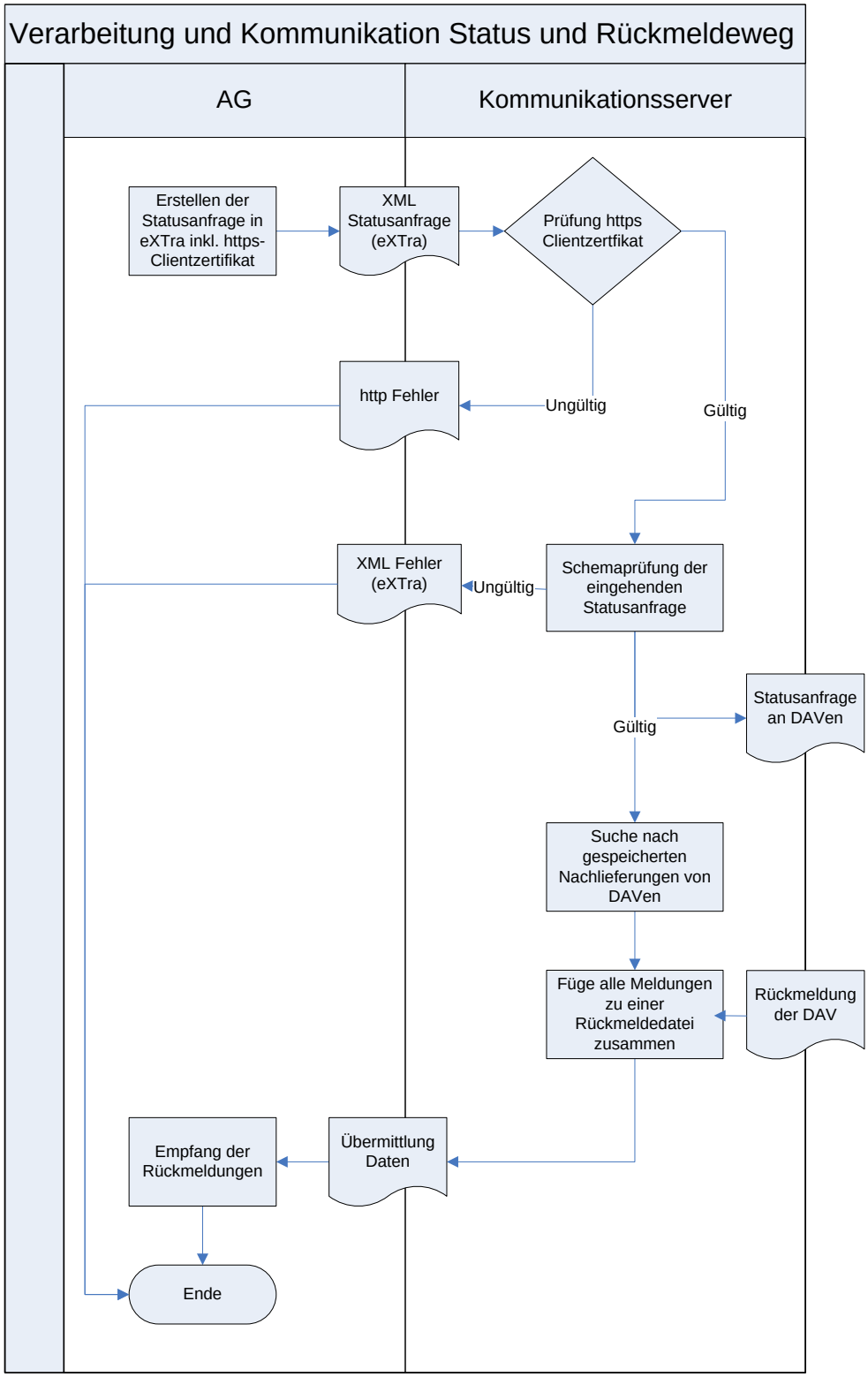

Abbildung 5: Flussdiagramm zum Verarbeitungsablauf der Statusanfrage und Rückmeldung.

Achtung: Eine Statusanfrage ist pro DAV und pro Verfahren nur einmal innerhalb von 15 Minuten möglich. Weitere Anfragen innerhalb von 15 Minuten werden mit einer Informationsnachricht vom GKV-Kommunikationsserver beantwortet.

4.2.1 Aufbau einer Statusanfrage für die Übertragung

Die Statusanfrage erfolgt in einer XML-Datei nach dem eXTra-Standard. Die Nachricht wird Base64-kodiert und im Element „Base64CharSequence“ in die eXTra-Nachricht eingehängt.
In der XML-Datei können folgende Filterkriterien vom AG mitgegeben werden:

- BBNR der DAV
- Verfahrenskennung

Dabei kann alternativ entweder nur ein Filterkriterium, beide Kriterien oder kein Kriterium angegeben werden. Jedes Filterkriterium kann nur einmal angegeben werden. Wird kein Kriterium angegeben, werden dem AG alle offenen Rückmeldungen aller DAVn aus allen Fachverfahren, die der GKV-Kommunikationsserver unterstützt, übermittelt.

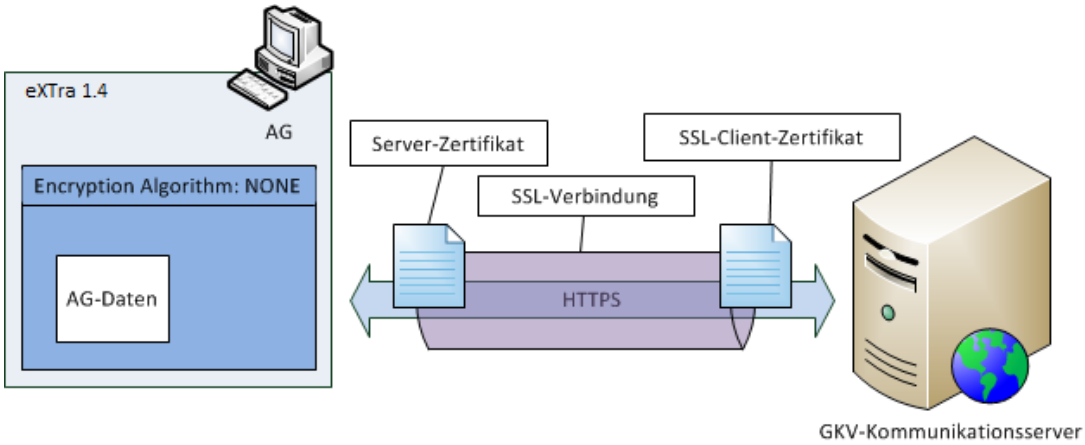

Abbildung 6: Senden einer Statusanfrage oder Quittung an den KomServer über https

Beim Senden von Statusanfragen und Empfangsquittungen über die https-Schnittstelle des KomServers sind die AG-Daten weder verschlüsselt noch signiert. Der Nachrichteninhalt von Empfangsquittungen und Statusanfragen an den GKV-Kommunikationsserver über das https-Protokoll wird daher lediglich Base64-kodiert:

```
<xcpt:Base64CharSequence>[Base64 kodierte Nachricht]
</xcpt:Base64CharSequence>
```

Um dem KomServer mitzuteilen, dass die AG-Daten in der XML-Struktur unverschlüsselt sind, müssen die Angaben zum Verschlüsselungsalgorithmus auf „NONE“ gesetzt werden. Dies geschieht über folgende Angabe innerhalb des <Encryption>-Elements:

```
<xplg:Algorithm id="http://www.extra-
standard.de/transforms/encryption/NONE"></xplg:Algorithm>
```

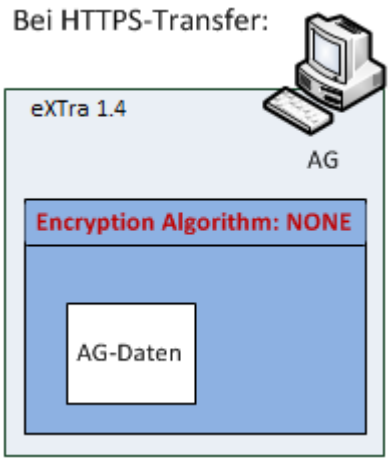

Abbildung 7: Aufbau von Statusanfragen und Empfangsquittungen bei Kommunikation über https

Achtung: Eine Statusanfrage ist pro DAV und pro Verfahren nur einmal innerhalb von 15 Minuten möglich. Weitere Anfragen innerhalb von 15 Minuten werden mit einer Informationsnachricht vom GKV-Kommunikationsserver beantwortet.

4.2.2 Übertragung der Statusanfrage an den GKV-Kommunikationsserver

Die Lieferung der XML-Datei (eXTra-Request) wird vom Webserver des GKV-Kommunikationsservers über https unter einer dedizierten URL zur Datenannahme entgegen genommen. Die Kommunikation zwischen AG und GKV-Kommunikationsserver basiert auf einem „POST-Request“[6] ohne die Angabe von Namen-Wert-Paaren und ohne die Angabe von http-Argumenten in der URL. Der http-Request und die http-Response müssen als Binary-Request ausgeführt werden, wobei der Http-Header lediglich die Attribute "Content-Type" und "Content-Length" enthalten muss. Der Http-Body enthält ausschließlich die zu übermittelnden Daten.

- **Inhalt des Http-Headers:**
  Content-Type: application/octet-stream
  Content-Length: <Größe des http-body in Bytes)

[6] http://tools.ietf.org/html/rfc2616

- **Inhalt des Http-Body:**
  Der Inhalt des Http-Body ist das eXtra-Datenpaket.

4.2.3 Prüfungen des GKV-Kommunikationsservers bei Statusanfragen

4.2.3.1 Schemaprüfung der XML-Datei

Der GKV-Kommunikationsserver prüft zuerst die vom AG gelieferte XML-Datei (eXTra-Request) auf Transportebene gegen das entsprechende XML-Schema. Ist diese XML-Datei valide, wird im Anschluss die im Body beinhaltete XML-Datei gegen das entsprechende Schema geprüft. Falls Fehler in der Struktur der angelieferten inneren XML-Datei gefunden oder Wertebereiche verletzt werden, wird eine eXTra-Response für den AG erstellt, die im Element „Report“ auf Transportebene die entsprechende Fehlermeldung beinhaltet (siehe Anhang B Statuscodes des GKV-Kommunikationsservers). Kann der GKV-Kommunikationsserver keine eXTra-Antwort an den AG erstellen, wird als Antwort eine „Error.xml“ (im Anhang A XML-Schema- und Beispieldateien genauer beschrieben) erstellt. Der Inhalt der Meldung wird auf dem GKV-Kommunikationsserver verworfen.

4.2.3.2 Rückmeldungen von Fehlermeldungen der Prüfungen

Wenn Fehler während den Prüfungen auftreten, wird eine Antwort (eXTra-Response) für den AG erstellt, die im Element „Report“ auf Transportebene den entsprechenden Statuscode und die entsprechende Fehlermeldung beinhaltet.
Erst nach den im Abschnitt 4.2.3 beschriebenen Prüfungen wird die Anfrage zur weiteren Bearbeitung im System weitergeleitet.

4.2.4 Antwort des GKV-Kommunikationsservers an den AG

Die Rückmeldung (Response) in Form einer XML-Datei wird nach dem eXTra-Standard erstellt. Beim Erstellen der Rückantwort an den AG werden alle zur Anfrage gehörenden Rückmeldungen der DAVn zu einer gemeinsamen Antwort zusammengefügt. Dabei kann es sich um fachliche oder technische Rückmeldungen der DAVn handeln. Der Inhalt der fachlichen Rückantworten ist in den jeweiligen Fachverfahren definiert. Jede Rückantwort einer DAV stellt innerhalb der eXTra-Antwort ein eigenes Paket dar.

Der Inhalt des Elements „Base64CharSequence“ auf Paketebene wird nach PKCS#7-Standard signiert, für den Empfänger verschlüsselt und anschließend Base64-kodiert. Bei technischen Fehlerrückmeldungen ist das Element nicht vorhanden.

Die fertige Rückmeldung wird anschließend über den offenen https-Kanal dem AG als eXTra-Response zurückgeliefert.

Bei der Rückmeldung sind Timeout-Kriterien zu beachten. Nach den Erfahrungen der Softwareersteller ist eine längere Übertragungs-/Verarbeitungsdauer kritisch, da in vielen Rechenzentren offene https-Verbindungen automatisch geschlossen werden.

Daher wird folgendermaßen vorgegangen:

- Die Antwortzeit für die Rückmeldung GKV-Kommunikationsserver an AG wird auf maximal 40 Sekunden festgelegt, in dem der KomServer auf Rückmeldungen der DAVn wartet.
- Nach Ablauf dieses Zeitrahmens[7] erstellt der GKV-Kommunikationsserver die Rückantwort an den AG mit dem Hinweis, dass möglicherweise noch weitere Rückmeldungen vorliegen und der AG innerhalb der nächsten 24 Stunden erneut anfragen möge.
- Der GKV-Kommunikationsserver nimmt auch nach Ablauf dieser Frist die Antwort der DAV entgegen und puffert sie für max. 24 Stunden.
- Sollte in den nächsten 24 Stunden eine erneute Statusanfrage durch den AG gestellt werden, wird keine Online-Abfrage bei der DAV vorgenommen. Stattdessen werden die zwischengepufferten Rückmeldungen dem AG übergeben.

Sobald die Rückmeldungen zum AG übertragen wurden, werden sie auf dem GKV-Kommunikationsserver gelöscht.
Es werden pro Statusanfrage maximal 200 Nutzdatendateien von der DAV als Rückantwort an den GKV-Kommunikationsserver zurückgesendet. Diese werden nach Datum sortiert und die Ältesten als erstes an den AG geliefert. Falls mehr als 200 Nutzdatendateien für die anfragende BBNR vorhanden sind, werden diese bei der nächsten Anfrage, nach der Empfangsquittung der bisher übertragenen Nutzdatendateien, gesendet. Dabei erfolgt auch eine Information innerhalb der eXTra-Response an den AG, dass noch weitere Daten zum Abruf bereitstehen und diese, nach erfolgreicher Quittierung der bereits abgerufenen Rückmeldungen, in einer zweiten Statusanfrage vom AG abgeholt werden können. Sollten noch weitere Rückmeldungen für den anfragenden AG bereitstehen, kann eine weitere Statusanfrage auch nach 15 Minuten an den GKV-Kommunikationsserver gestellt werden.

4.2.5 Technische Fehlerrückmeldungen

Bei technischen Fehlerrückmeldungen handelt es sich um Rückmeldungen der DAV auf eine vorherige Meldung, welche während der Verarbeitung in der DAV aus diversen Gründen nicht verarbeitet werden konnte. Bisher bestand für die DAVn keine Möglichkeit, eine qualifizierte Information über ein technisches Problem bei der Verarbeitung von Meldungen, über den GKV-Kommunikationsserver an den AG zurück zu geben. Diese Lücke wird mit der Verwendung von technischen Fehlerrückmeldungen geschlossen.

[7] Falls alle DAVn vor dem Ende dieser Frist ihre Antwort gesendet haben, muss das Ende natürlich nicht abgewartet werden.

Damit bekommt der Absender einer Meldung in jedem Fall eine Rückmeldung auf seine Sendung, denn entweder wird die Meldung erfolgreich verarbeitet und gelangt mit Verarbeitungsbestätigung ins Fachverfahren, oder die meldet eine technische Fehlerrückmeldung an den Absender zurück.

Die möglichen Fehlercodes mit den jeweiligen Fehlertexten sind im Anhang B Statuscodes des GKV-Kommunikationsservers aufgeführt.

4.3 Empfangsquittung

Die „Empfangsquittung“ bezeichnet die Bestätigung des AG, dass er die Rückmeldung der DAV über den GKV-Kommunikationsserver erhalten hat. Die Empfangsquittungen werden analog zu Meldungen und Statusanfragen nachdem eXTra-Standard aufgebaut und können über https an den GKV-Kommunikationsserver übertragen werden.
Die Quittierung durch den AG ist zwingend notwendig! Bei Ausbleiben der Empfangsquittung wird die betreffende und bereits abgerufene Rückmeldung bei jeder neuen Statusanfrage erneut zugestellt. Dies betrifft alle bereits abgerufenen aber nicht quittierten Rückmeldungen bei jeder neuen Statusanfrage und erzeugt damit unnötige Systemlast.
Als freiwilliger Service wird der AG von manchen DAVn nach einer Frist mittels einer Erinnerungsmail informiert, dass Rückmeldungen für ihn vorliegen und diese abzuholen und zu quittieren sind. Nach 30 Tagen werden die Rückmeldungen auf dem GKV-Kommunikationsserver gelöscht und können durch den AG nicht mehr elektronisch abgerufen werden.

Die nachfolgende Abbildung verdeutlicht den Verarbeitungs- und Kommunikationsweg zwischen den einzelnen Stellen und die Prozessschritte, welche im Folgenden noch genauer erläutert werden:

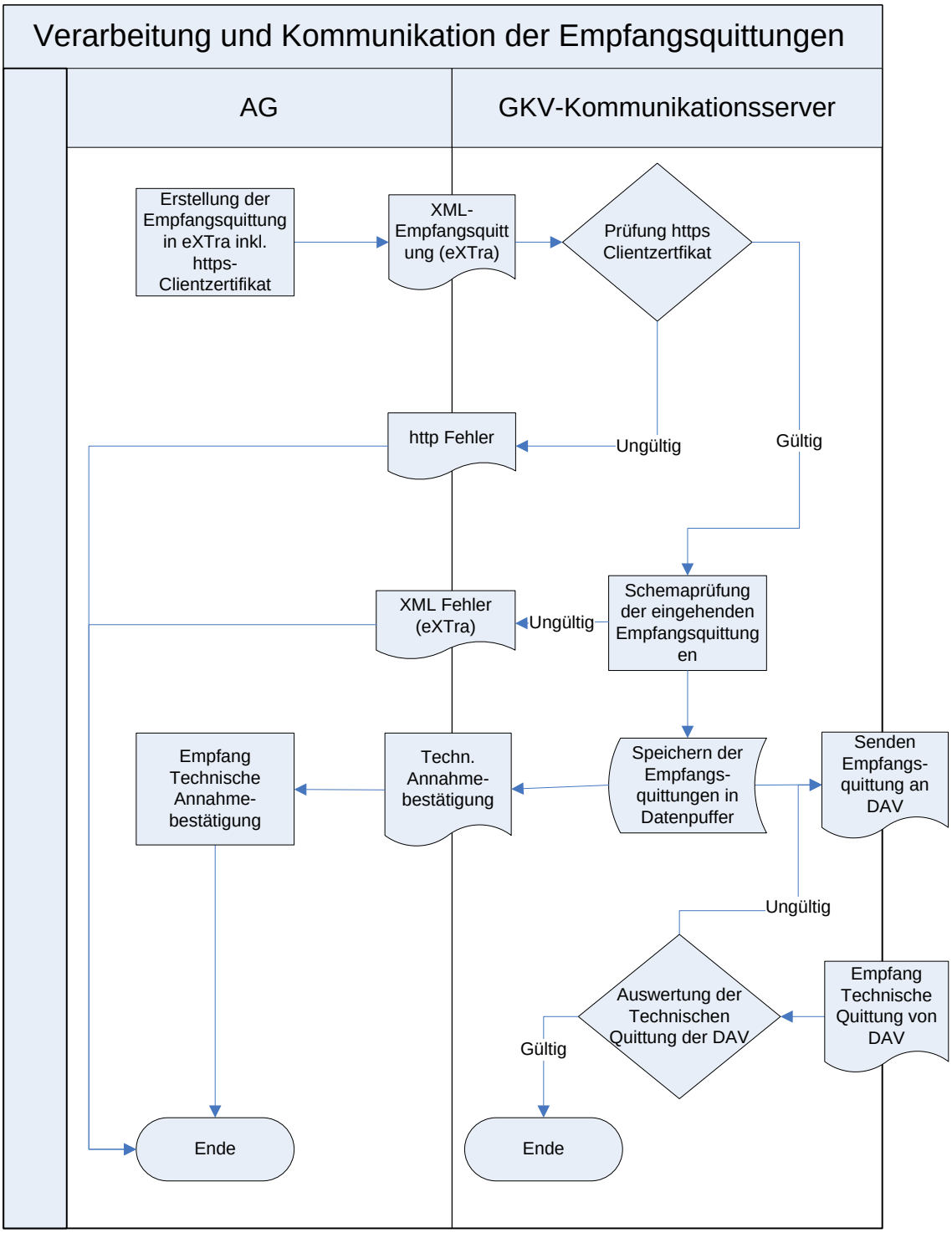

Abbildung 8: Flussdiagramm zum Verarbeitungsablauf der Empfangsquittungen

4.3.1 Aufbau der Empfangsquittung für die Übertragung

Die Empfangsquittung wird vom AG als XML-Datei nach den eXTra-Vorgaben erstellt. Diese enthält die TrackingIDs der zu quittierenden Rückmeldungen als einziges Quittierungskriterium. Die Daten dürfen nicht auf Nachrichtenebene verschlüsselt werden, da dies bereits durch das https-Protokoll auf Transportebene geschieht.

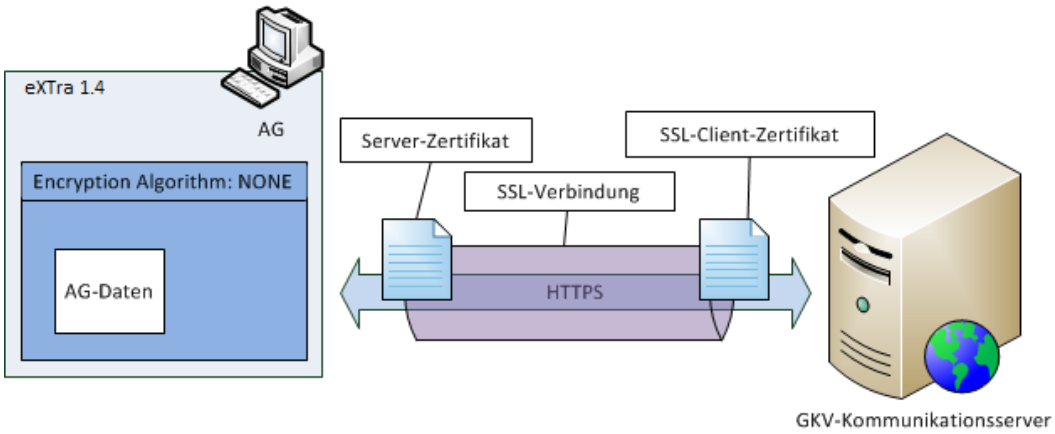

Abbildung 9: Senden einer Empfangsquittung an den KomServer über https

Beim Senden von Statusanfragen und Empfangsquittungen über die https-Schnittstelle des KomServers sind die AG-Daten weder verschlüsselt noch signiert. Der Nachrichteninhalt von Quittungen und Statusanfragen an den GKV-Kommunikationsserver über das https-Protokoll wird daher lediglich Base64-kodiert:

```
<xcpt:Base64CharSequence>[Base64 kodierte Nachricht]
</xcpt:Base64CharSequence>
```

Um dem KomServer mitzuteilen, dass die AG-Daten in der XML-Struktur unverschlüsselt sind, müssen die Angaben zum Verschlüsselungsalgorithmus auf „NONE“ gesetzt werden. Dies geschieht über folgende Angabe innerhalb des <Encryption>-Elements:

```
<xplg:Algorithm id="http://www.extra-
standard.de/transforms/encryption/NONE"></xplg:Algorithm>
```

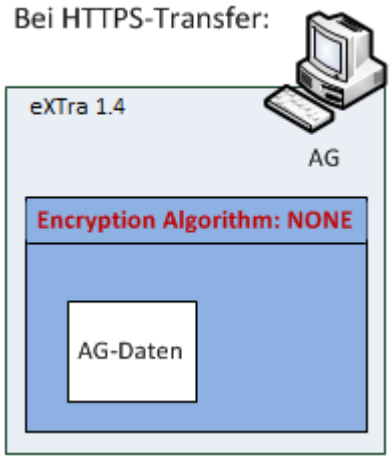

Abbildung 10: Aufbau von Statusanfragen und Quittungen bei Kommunikation über https

4.3.2 Übertragung der Empfangsquittung an den GKV-Kommunikationsserver

Die Lieferung der XML-Datei wird vom Webserver-Dienst des GKV-Kommunikationsservers über https unter einer dedizierten URL zur Datenannahme entgegen genommen. Die Kommunikation zwischen AG und GKV-Kommunikationsserver basiert auf einem „POST-Request“[8] ohne die Angabe von Namen-Wert-Paaren und ohne die Angabe von http-Argumenten in der URL. Der http-Request und die http-Response müssen als Binary-Request ausgeführt werden, wobei der Http-Header lediglich die Attribute "Content-Type" und "Content-Length" enthalten muss. Der Http-Body enthält ausschließlich die zu übermittelnden Daten.

- **Inhalt des Http-Headers:**
  Content-Type: application/octet-stream
  Content-Length: <Größe des http-body in Bytes)
- **Inhalt des Http-Body:**
  Der Inhalt des Http-Body ist das eXtra-Datenpaket.

4.3.3 Prüfungen des GKV-Kommunikationsservers bei Empfangsquittungen

4.3.3.1 Schemaprüfung der XML-Datei

Der GKV-Kommunikationsserver prüft die gelieferte XML-Datei auf Transportebene gegen das entsprechende XML-Schema. Wenn Fehler in der Struktur der angelieferten XML-Datei gefunden oder Wertebereiche verletzt werden, wird eine eXTra-Antwort für den AG erstellt, die im Element „Report“ auf Transportebene die entsprechende Fehlermeldung beinhaltet. Hier werden lediglich die mit der Kommunikation verbundenen Fehler zurückgemeldet (z.B. „TrackingID konnte keiner DAV zugeordnet werden“).

[8] http://tools.ietf.org/html/rfc2616

Kann der GKV-Kommunikationsserver keine eXTra-Antwort an den AG erstellen, wird als Response eine „Error.xml“ (im Anhang A XML-Schema- und Beispieldateien genauer beschrieben) erstellt. Der Inhalt der Meldung wird auf dem GKV-Kommunikationsserver verworfen.

4.3.4 Zerlegung der Empfangsquittung in Teilquittungen GKV-Kommunikationsserver -> DAVn

Die Empfangsquittung besteht aus den Einzelquittungen. Aufgrund einer internen Zuordnungstabelle der TrackingIDs kann der GKV-Kommunikationsserver zuordnen, welche DAV Empfänger dieser Einzelquittung ist. Der GKV-Kommunikationsserver teilt die Einzelquittungen so auf, dass jede DAV nur die für sie bestimmten Empfangsquittungen erhält.

4.3.5 Antwort des GKV-Kommunikationsservers an den AG

Die Antwort (Response) des GKV-Kommunikationsservers wird als XML-Datei nach dem eXTra-Standard erstellt. Eine XML-Beispieldatei und eine XML-Schemadatei für die Response werden im aktuellen eXTra-Format zur Verfügung gestellt. Die Response ist an dieser Stelle nur eine technische Annahmebestätigung, dass jede Quittung erfolgreich einer DAV zugeordnet werden konnten.

Alle nachgelagerten Prüfungen bei der DAV (z.B. „existiert eine Nutzdatendatei zu dieser Dateifolgenummer“) werden nicht berücksichtigt.

4.4 Verfügbarkeitsanzeige

Um für Arbeitgeber die Verfügbarkeit der Arbeitgeberschnittstelle transparent zu machen, wurde die sog. Verfügbarkeitsanzeige online gestellt. Über diese Anzeige lässt sich der Status der Verfügbarkeit der Arbeitgeberschnittstelle abrufen, sowie die Historie des Status in der Vergangenheit nachvollziehen. Die Verfügbarkeitsanzeige wird aktuell über eine Webseite abgebildet. Diese Webseite ist unter dem Menüpunkt: „Verfügbarkeit“ auf dem Webportal des GKV-Kommunikationsservers unter „https://www.gkv-kommunikationsserver.de“ erreichbar.

Anhang A XML-Schema- und Beispieldateien

Aktuelle Schema- und Beispieldateien sind unter http://www.extra-standard.de -> Menüpunkt " Registrierte Verfahren" -> „GKV-Kommunikationsserver – Arbeitgeberverfahren" zu finden. Bzgl. des Versands von Testdaten beachten sie bitte die entsprechenden Hinweise in den Beispieldateien und den Schemata.

Anhang B Statuscodes des GKV-Kommunikationsservers

Statuscode	**Text**
1) Info-Meldungen	
I000	Die Verarbeitung auf dem GKV-Kommunikationsserver wurde erfolgreich durchgeführt.
I001	Es sind keine Daten für die angefragte Betriebsnummer vorhanden.
I002	Es sind ggf. weitere Daten für die angefragte Betriebsnummer vorhanden. Bitte fragen Sie nach 15 Minuten erneut an.
I003	Es sind weitere Daten für die angefragte Betriebsnummer vorhanden.
I004	Doppelte Statusanfrage innerhalb von {0} - bitte versuchen Sie es zu einem späteren Zeitpunkt erneut.
I005	Es liegen keine Daten zu dieser Anfrage vor
I006	Die übermittelte „RequestID" ist nicht eindeutig
2) Fehlermeldungen	
a) Allgemein	
E100	Interner Fehler des GKV-Kommunikationsservers aufgetreten.
E101	Zeitgleiche Statusanfrage an der Arbeitgeberschnittstelle.
E102	Zeitüberschreitung der Statusanfrage an der Arbeitgeberschnittstelle."
E103	Dieser eXTra-Standard wird nicht mehr unterstützt, bitte verwenden Sie die neueste eXTra-Version.
E104	Der Empfänger ist unbekannt oder für das angegebene Verfahren nicht zugelassen.
E105	Die Empfangsquittung konnte keiner Rückmeldung im System zugeordnet werden.
E106	Versuch der Quittierung von ungültigen Daten.
E107	Die gesendete Arbeitgeber-Betriebsnummer der Quittungsliste stimmt nicht mit der Arbeitgeber-Betriebsnummer der zugeordneten Rückmeldung überein.
E108	Der Sender ist für das angegebene Verfahren nicht zugelassen
E109	BBNR Abs.-Eigner aus eXTra-Header nicht identisch mit Zertifikatsinhalt
b) Parser / Datenformat	
E200	Es ist ein Fehler bei der Verarbeitung der Inhalte der eXTra-XML-Datei aufgetreten.
E201	Es ist ein Fehler bei der Verarbeitung der Inhalte der eXTra-Standard-Message-XML-Datei aufgetreten.
E202	Es ist ein Fehler bei der Validierung der eXTra-XML-Datei aufgetreten.
E203	Es ist ein Fehler bei der Validierung der eXTra-Standard-Message-XML-Datei aufgetreten.
E204	Es ist ein Fehler bei der Verarbeitung der ASN.1-Datenstruktur aufgetreten.
c) Verschlüsselung und Zertifikate	

E300	Allgemeiner Krypto-Fehler aufgetreten.
E301	Die empfangenen Daten konnten nicht entschlüsselt werden.
E302	Die Signatur der Daten konnte nicht verifiziert werden.
E303	Das verwendete Zertifikat konnte im Verzeichnisserver nicht gefunden werden."
E304	Das verwendete Zertifikat ist entweder abgelaufen oder nicht gültig."
E305	Bitte für Statusanfragen jeweils das zuletzt ausgestellte und gültige Zertifikat verwenden.
E306	Verschlüsselungsmethode und Übertragungsprotokoll stimmen nicht überein
d) Technische Fehlerrückmeldungen der DAVn	
E410	Die Datei konnte nicht entschlüsselt werden
E411	Die Datei wurde nicht für diesen Empfänger verschlüsselt
E412	Die Datei war nicht verschlüsselt
E413	Die Datei war nicht signiert
E414	Signaturprüfung fehlgeschlagen
E415	Das verwendete Zertifikat ist abgelaufen
E416	Das verwendete Zertifikat wurde gesperrt
E417	Das verwendete Zertifikat wurde von einer unbekannten Zertifizierungsstelle ausgestellt
E420	Zum Komprimierungsverfahren ist keine Dekomprimierung möglich
E430	BBNR Abs.-Eigner eXtra-Header** ungleich BBNR-ABSENDER Vorlaufsatz*
E431	BBNR Abs.-Eigner der Datei aus eXTra-Header** nicht identisch mit Zertifikatsinhalt*
E432	Zeichensatz der Nutzdaten ungleich Angaben im eXTra-Header**
E433	Dateistruktur nicht erkennbar oder entspricht nicht den Vorgaben
E434	Die Datei entspricht nicht den Angaben im eXTra-Header**

Anhang D Glossar

Abkürzung	Beschreibung
AAG	Verfahrenskennung für Erstattungsanträge nach dem Aufwendungsausgleichgesetz (Meldung)
AAK	Verfahrenskennung für Erstattungsanträge nach dem Aufwendungsausgleichgesetz (Rückmeldung)
ALG	Arbeitsbescheinigungen für Zwecke des über- und zwischenstaatlichen Rechts sowie Nebeneinkommen
ASCII	„American Standard Code for Information Interchange“, eine Zeichenkodierung
AG	Arbeitgeber oder andere Meldepflichtige
BBNR	Bundeseinheitliche Betriebsnummer
BEA	Verfahrenskennung Beitragserhebungen der berufsständischen Versorgungseinrichtungen
BNA	Verfahrenskennung Beitragsnachweise der Arbeitgeber
BNZ	Verfahrenskennung Beitragsnachweise der Zahlstellen
Datenlieferungen	Elektronische Meldungen im Arbeitgeberverfahren (z.B. Sozialversicherungsmeldungen und Beitragsnachweise)
DAV	Datenannahme- und –verteilstellen der gesetzlichen Krankenversicherung
DEÜV	Datenerfassungs- und –übermittlungsverordnung
DSKO	Datensatz Kommunikation
DUA	Verfahrenskennung Sozialversicherungsmeldungen nach DEÜV
EEK	Verfahrenskennung Entgeltersatzleistungen (Rückmeldung)
EEL	Verfahrenskennung Entgeltersatzleistungen (Meldung)
eXTra	eXTra („einheitliches XML-basiertes Transportverfahren“) ist offener, frei verfügbarer Standard für den Datenaustausch, der unter Federführung der AWV von Wirtschaft und Verwaltung gemeinsam auf der Basis bestehender Verfahren entwickelt wurde.
GKV	Gesetzliche Krankenversicherung
http	Hypertext Transfer Protocol
https	HTTP secure. SSL/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.
ID	Identifikationsnummer
LDAP	Lightweight Directory Access Protocol
PKCS#7	„Public Key Cryptography Standards“, ein Verschlüsselungs-Standard gemäß RFC 2315
Replay-Attacken	Eine Replay-Attacke ist eine kryptoanalytische Angriffsform auf die Authentizität von Daten in einem Kommunikationsprotokoll. Hierbei sendet der Angreifer zuvor aufgezeichnete Daten, um etwa eine fremde Identität vorzutäuschen.

SAG	Verfahrenskennung Krankenkassenmeldungen zum Sozialausgleich
TrackingID	Eindeutige Sendungsnummer, mit der die Beteiligten den Status einer Sendung nachverfolgen können
URL	„Uniform Resource Locator“, URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise http oder ftp) und den Ort (engl. location) der Ressource in Computernetzwerken.
VSA	Verfahrenskennung Rückmeldung der Versichertennummer
XML	Extensible Markup Language
ZAK	Verfahrenskennung Rückmeldung an Zahlstellen
ZAV	Verfahrenskennung Meldungen der Zahlstellen