

Inhaltsverzeichnis

1	GRUNDLAGEN DES GKV-KOMMUNIKATIONSSERVERS	2
1.1	ALLGEMEINES	2
1.2	SERVERADRESSEN	3
1.3	KOMMUNIKATIONSART	4
1.4	KOMMUNIKATIONSSTANDARD	4
1.5	VERSCHLÜSSELUNG UND ZERTIFIKATE	4
1.5.1	<i>Verschlüsselung der Melde – und Rückmeldedaten</i>	4
1.5.2	<i>Transportverschlüsselung und Authentifizierung über https</i>	5
1.6	SCHEMAPRÜFUNGEN DES GKV-KOMMUNIKATIONSSERVER	6
1.7	KODIERUNG	7
2	KOMMUNIKATIONSPROZESSE ZWISCHEN AG UND GKV-KOMMUNIKATIONSSERVER	8
2.1	MELDEWEG	8
2.1.1	<i>Meldungen</i>	8
2.2	RÜCKMELDEWEG	10
2.2.1	<i>Statusanfrage und Rückmeldungen</i>	10
2.2.1.1	<i>Aufbau einer Statusanfrage für die Übertragung</i>	12
2.2.1.2	<i>Technische Fehlerrückmeldungen</i>	12
2.2.2	<i>Empfangsquittung</i>	13
3	ERGÄNZENDE INFORMATIONEN	15
3.1	FACHLICHE RAHMENBEDINGUNGEN	15
3.1.1	<i>Absender/Ersteller und Zertifikat</i>	15
3.1.2	<i>Adressierung der Meldung</i>	15
3.2	TECHNISCHE RAHMENBEDINGUNGEN	16
3.2.1	<i>Schemadateien</i>	16
3.2.2	<i>WebService Schnittstelle</i>	17
3.2.2.1	<i>WebService-WSDL</i>	17
3.2.2.2	<i>Datenformat</i>	17
3.2.3	<i>Geschäftsfall Meldungen</i>	18
3.2.4	<i>Geschäftsfall Rückmeldungen</i>	18
3.2.5	<i>Verbindungen über TLS mit TLS Clientzertifikat</i>	18
3.2.6	<i>Verwendung des neuesten Arbeitgeber-Zertifikats</i>	18
3.2.7	<i>Quittierung von Rückmeldungen</i>	18
3.2.8	<i>Auswertung der Fehler- bzw. Rückgabeinformation</i>	19
3.2.9	<i>Zusammenfassung von mehreren Meldungen in einer Meldungsliste</i>	19
3.2.10	<i>Verwendung von *-Anfragen und Besonderheiten beim eAU Verfahren</i>	19
3.2.11	<i>Verfügbarkeitsanzeige</i>	20
ANHANG A	XML-SCHEMA- UND BEISPIELDATEIEN.....	21
ANHANG B	STATUSCODES DES GKV-KOMMUNIKATIONSSERVERS	21
ANHANG C	GLOSSAR	22

Abbildungsverzeichnis

Abbildung 1: Der GKV-Kommunikationsserver als Makler zwischen AG und Sozialversicherungsträgern	2
Abbildung 2: Verschlüsselung und Authentifizierung	5
Abbildung 3: Übersicht der Kommunikationsprozesse zwischen AG und GKV-Kommunikationsserver	8
Abbildung 4: Flussdiagramm zum Verarbeitungsablauf der Meldungen des AG	9
Abbildung 5: Flussdiagramm zum Verarbeitungsablauf der Statusanfrage und Rückmeldung.....	11
Abbildung 6: Flussdiagramm zum Verarbeitungsablauf der Empfangsquittungen.....	14

1 Grundlagen des GKV-Kommunikationsservers

1.1 Allgemeines

Der GKV-Kommunikationsserver dient als zentrale Stelle für den Melde- und Rückmeldeweg und somit als „Tor“ zu den **Datenaustauschverfahren**. Arbeitgeber und sonstige Meldepflichtige (im Folgenden als „AG“ bezeichnet) sind 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 zuständigen Datenannahmestellen (im Folgenden als „DAVn“ bezeichnet) ist Aufgabe des GKV-Kommunikationsservers.

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

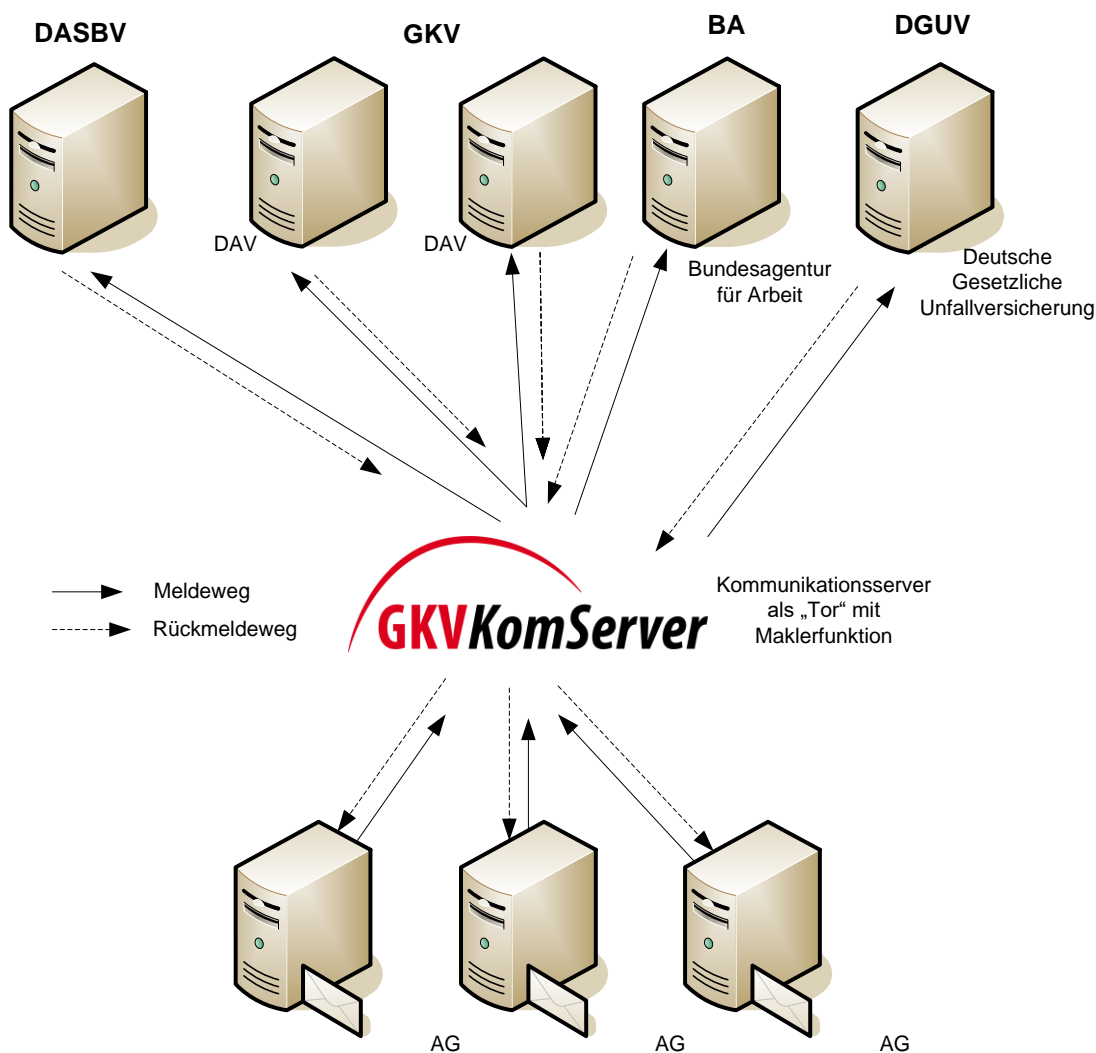


Abbildung 1: Der GKV-Kommunikationsserver als Makler zwischen AG und Sozialversicherungsträgern

1.2 Serveradressen

Um eine Vermischung von Test – und Produktionssystemen zu vermeiden, existieren physikalisch getrennte Systeme. Die URLs des Produktivsystems sind die folgenden:

- **Abgabe von Meldungen:**

<https://verarbeitung.gkv-kommunikationsserver.de/meldung/extra14.meldung>

<https://verarbeitung.gkv-kommunikationsserver.de/meldung/extra15.meldung>

- **Anfrage von Rückmeldungen:**

<https://verarbeitung.gkv-kommunikationsserver.de/anfrage/extra14.anfrage>

<https://verarbeitung.gkv-kommunikationsserver.de/anfrage/extra15.anfrage>

- **Abgabe von Empfangsquittungen:**

<https://verarbeitung.gkv-kommunikationsserver.de/quittung/extra14.quittung>

<https://verarbeitung.gkv-kommunikationsserver.de/quittung/extra15.quittung>

Alternativ zu den oben genannten URLs kann folgende URL für alle Geschäftsfälle und eXTra Versionen verwendet werden:

- <https://verarbeitung.gkv-kommunikationsserver.de/extra>

Ein Zugriff auf das Qualitätssicherungs-System kann nur nach bilateraler Abstimmung erfolgen.

Für den Fall, dass lediglich ein Verbindungstest zum GKV-Kommunikationsserver erfolgen soll, ist hierfür ausschließlich folgende URL zu verwenden:

<https://verarbeitung.gkv-kommunikationsserver.de/verbindungstest.aspx>

Als Response auf die Testanfrage erhält der Sender einen Plain-Text („Verbindungstest zum GKV-Kommunikationsserver erfolgreich“) unter Angabe der empfangenen Nutzdaten in Bytes und des verwendeten TLS Clientzertifikats.



In diesem Fall erfolgt jedoch keine Verarbeitung oder fachliche Prüfung. Diese URL ist nur für Testzwecke gedacht, wie z.Bsp. Test der Erreichbarkeit des Systems oder des TLS-Handshakes mit dem Clientzertifikat.

1.3 Kommunikationsart

Die Kommunikation mit den Diensten des GKV-Kommunikationsservers ist über einen SOAP-Webservice möglich.

Dazu ist ein Client-Zertifikat erforderlich und es gelten die identischen unter Kapitel 1.2 genannten URLs.

1.4 Kommunikationsstandard

Der auf dem Kommunikationsserver betriebene Dienst verwendet den eXTra-Standard. Es werden folgende Versionen unterstützt:

- eXTra-Transport Version 1.4 in der registrierten Version vom 17.06.2019
- eXTra-Transport Version 1.5 gemäß der gemeinsamen Profilierung von GKV und DSRV

Die folgende Tabelle gibt eine Übersicht, zu welchen Zeiträumen welche Versionen des eXTra-Standards verwendet werden können:

	REST-Schnittstelle mit Base64	SOAP-Schnittstelle mit MTOM
eXTra-Version 1.4	zum 01.04.2022 abgekündigt, auf Antrag einzelner Softwareersteller verlängert bis 31.03.2026.	Betrieb bis 31.03.2026
eXTra-Version 1.5	wird nicht unterstützt	Betrieb ab 01.07.2022

Tabelle 1: Übersicht Einsatztermine eXTra-Versionen

1.5 Verschlüsselung und Zertifikate

1.5.1 Verschlüsselung der Melde – und Rückmeldedaten

Bei der Verschlüsselung und den Zertifikaten kommen die in „Anlage 16 („Security Schnittstelle“)“ beschriebenen Verfahren zum Einsatz.

1.5.2 Transportverschlüsselung und Authentifizierung über https

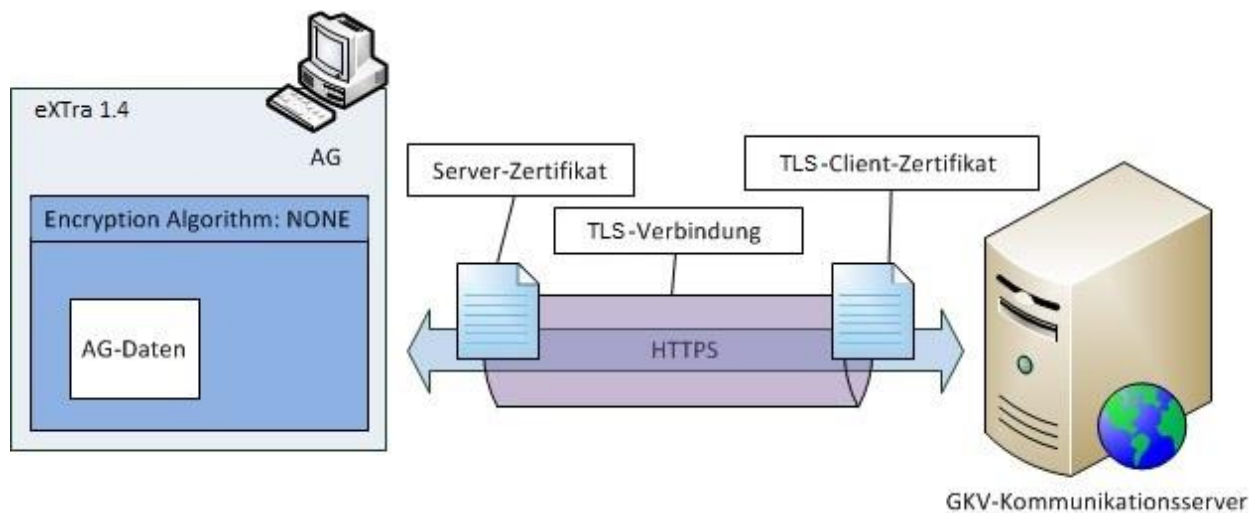


Abbildung 2: Verschlüsselung und Authentifizierung

Das https-Protokoll besitzt mit dem TLS Handshake Protocol einen Mechanismus, mit dem ein sicherer Kommunikationskanal aufgebaut wird, 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 wird in vier Phasen unterteilt:

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 inklusive einer mit dem zugehörigen privaten Schlüssel signierten Nachricht an den Client übermittelt. Außerdem fordert der Server den Client dazu auf, 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. Anschließend signiert der Client eine Nachricht mit seinem privaten Schlüssel und übermittelt sein Clientzertifikat, das vom Server verifiziert werden muss. Schlägt die Prüfung fehl, wird die Verbindung mit einem Fehler abgebrochen. **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 TLS-Client-Zertifikats für den Aufbau einer TLS-Verbindung zum GKV-Kommunikationsserver ist zwingend erforderlich!

Implementierungshinweise:

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

Der AG muss beim Aufbau der https-Verbindung und der damit verbundenen TLS-Client-Authentifizierung das von einem registrierten Trustcenter zum Datenaustausch mit der Sozialversicherung auf dessen Betriebsnummer ausgestellte Zertifikat als „TLS-Client-Zertifikat“ an den GKV-Kommunikationsserver 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 GKV-Kommunikationsserver übermittelte Serverzertifikat prüfen und 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.



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

1.6 Schemaprüfungen des GKV-Kommunikationsserver

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“ die entsprechende Fehlermeldung beinhaltet. Hier werden lediglich die mit der Kommunikation verbundenen Fehler zurückgemeldet (z.B. „DAV nicht bekannt“). Die entsprechenden Fehlercodes sind dem Anhang B zu entnehmen.

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.

1.7 Kodierung

Die Daten werden mit dem Zeichensatz ISO-8859-1 verarbeitet.

2 Kommunikationsprozesse GKV-Kommunikationsserver

zwischen

AG

und

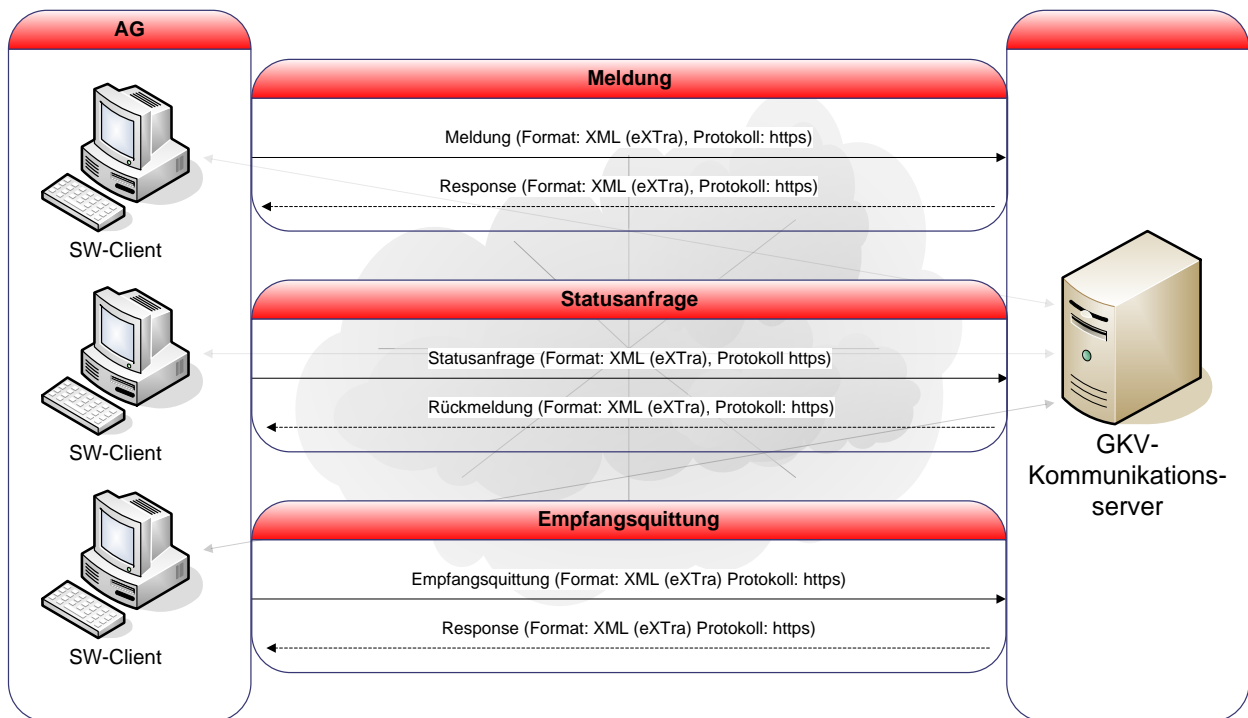


Abbildung 3: Übersicht der Kommunikationsprozesse zwischen AG und GKV-Kommunikationsserver

2.1 Meldeweg

Der Meldeweg beschreibt den Prozess des Sendens der Meldedaten eines AG zum GKV-Kommunikationsserver.

2.1.1 Meldungen

Die Meldungen des AG werden entsprechend dem folgenden Verarbeitungs- und Kommunikationsweg an den GKV-Kommunikationsserver übermittelt:

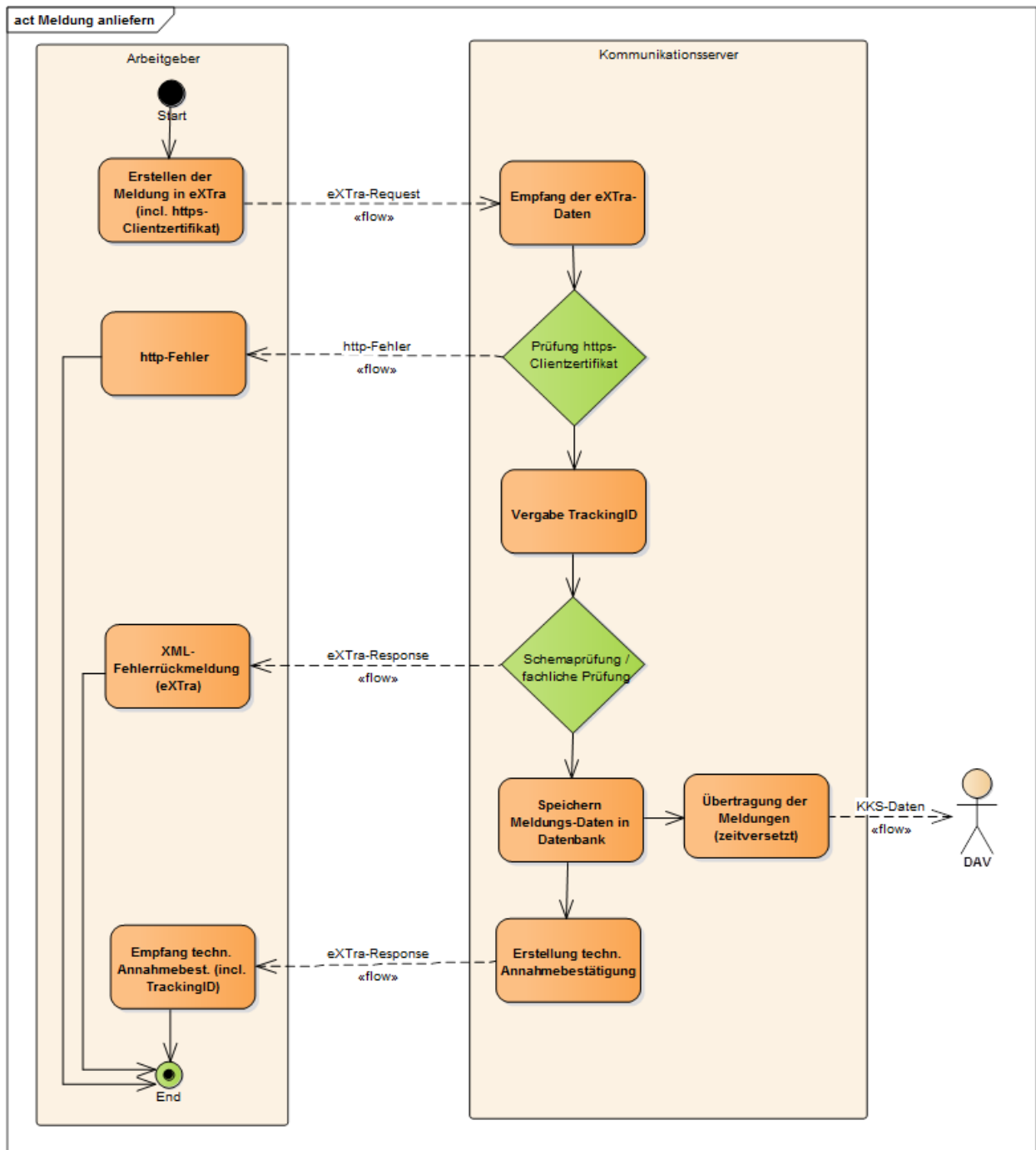


Abbildung 4: Flussdiagramm zum Verarbeitungsablauf der Meldungen des AG

Der GKV-Kommunikationsserver erstellt für jede Nutzdatendatei eine eindeutige 23-stellige TrackingID (ResponseID auf Paketebene). Diese kann genutzt werden, um den Status bei der DAV-Hotline abzufragen.

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 sie mit einem zugelassenen Zertifikat signiert wurden. Ist einer der vorgenannten Schritte nicht möglich, wird von der DAV asynchron eine technische Fehlerrückmeldung zurückgeliefert (siehe auch Kapitel 2.2.1.2). Im Element „ResponseID“ wird auf Paketebene die vom GKV-Kommunikationsserver vergebene TrackingID an den AG zurückgemeldet. Zusätzlich vergibt der GKV-Kommunikationsserver eine TrackingID (ResponseID) für die Transportebene. Die Anzahl der Meldungen an den GKV-Kommunikationsserver ist auf max. 2400 Packages begrenzt.

2.2 Rückmeldeweg

Der Rückmeldeweg beschreibt den Prozess der Statusanfrage, der Rückmeldungen und der Quittierung von Rückmeldungen.

2.2.1 Statusanfrage und Rückmeldungen

Als „Statusanfrage“ wird eine Anfrage (Request) des AG an den GKV-Kommunikationsserver bezeichnet, welche prüft, ob 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. Beim Aufbau der https-Verbindung wird der sendende AG auf Basis des TLS Handshakes authentisiert. Ist der AG identifiziert und berechtigt, werden die entsprechenden Rückmeldungen der DAVn an den AG übermittelt.

Mit der Übertragung der Rückmeldungen an den AG wird spätestens nach 30 Sekunden durch den GKV-Kommunikationsserver begonnen. Die Daten werden als XML-Datei nach dem eXTra-Standard über die durch den AG offen zu haltende https-Verbindung (Gesamt-Timeout 180 Sek.) übertragen.

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

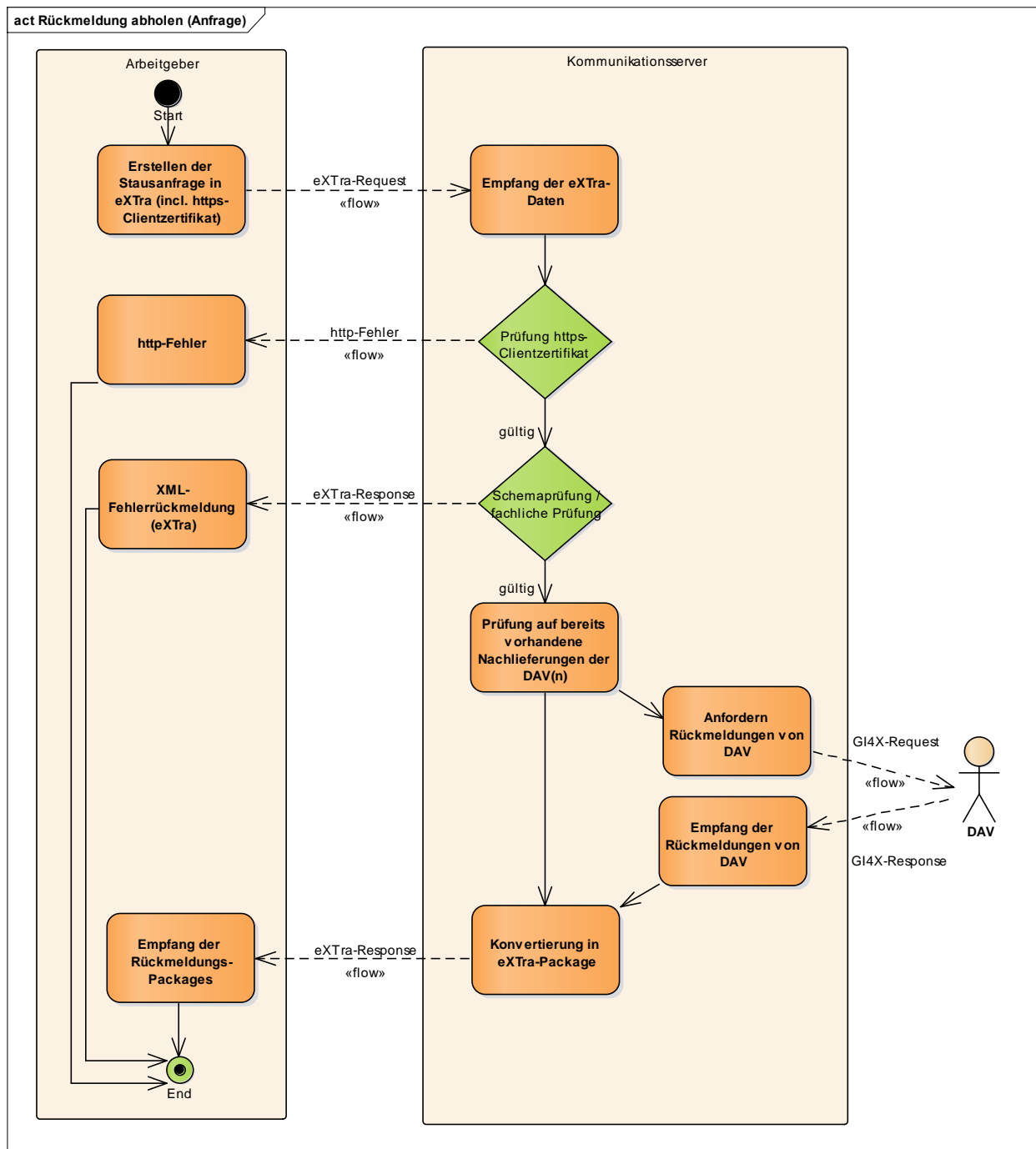


Abbildung 5: Flussdiagramm zum Verarbeitungsablauf der Stausanfrage und Rückmeldung.



Eine Stausanfrage ist pro DAV und pro Verfahren bei der Datenart „Echt“ nur einmal innerhalb von 15 Minuten möglich. Weitere Anfragen innerhalb von 15 Minuten werden mit einer Informationsnachricht vom GKV-Kommunikationsserver beantwortet. Bei der Datenart „Test“ kann dies jede Minute einmal erfolgen.

2.2.1.1 Aufbau einer Statusanfrage für die Übertragung

Die Nachricht wird via MTOM 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.

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 Rückantworten ist in den jeweiligen Fachverfahren definiert. Jede Rückantwort einer DAV stellt innerhalb der eXTra-Antwort ein eigenes Paket dar.

Der Inhalt der Pakete ist nach den Vorgaben der SECON (Anlage 16 der Gemeinsamen Grundsätze Technik) zu signieren und für den Empfänger zu verschlüsseln. Bei technischen Fehlerrückmeldungen sind keine Nutzdaten vorhanden.

Jede weitere Anfrage an den GKV-Kommunikationsserver darf erst nach 15min erfolgen, ansonsten wird ein entsprechender Fehlercode (I004) zurückgeliefert.

Es werden pro Statusanfrage maximal 2400 Nutzdatendateien oder 20 MB Gesamtnutzdaten-größe von allen DAVn als Rückantwort an den GKV-Kommunikationsserver zurückgesendet. Diese werden nach Datum sortiert und die Ältesten als Erste an den AG geliefert. Falls mehr Daten 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 (I003), 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. In diesem Fall kann die nächste Statusanfrage direkt ohne Wartezeit (15min) erfolgen.

2.2.1.2 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 (z.B. Entschlüsselungsfehler oder Fehler in der Nutzdatenstruktur).

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

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

2.2.2 Empfangsquittung

Die „Empfangsquittung“ bezeichnet die Bestätigung des AG, dass er die Rückmeldung (fachliche Rückmeldung, Verarbeitungsbestätigung, fachliche und technische Fehlerrückmeldung) der DAV über den GKV-Kommunikationsserver erhalten hat. 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.

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. Die Datei wird nach der erfolgreichen Quittierung gelöscht. Nach 30 Tagen werden auch die nicht quittierten Rückmeldungen gelöscht und können durch den AG nicht mehr elektronisch abgerufen werden (§96 SGB IV).

Eine Quittierung erfolgt immer auf der Basis einer erhaltenen TrackingID. Hierbei können mehrere Quittungen zur einer Quittungsliste vom AG zusammengeführt werden.

Die Antwort (Response) des GKV-Kommunikationsservers ist an dieser Stelle nur eine technische Annahmestätigung. Im Fehlerfall werden entsprechende Fehlercodes gemäß „Anhang B Statuscodes des GKV-Kommunikationsservers“ zurück gemeldet.

Hinweis:

Die Wirksamkeit der Quittung tritt prozessbedingt verzögert ein, aus diesem Grund sollte eine darauffolgende Statusanfrage verzögert ausgeführt werden.

Es sind alle vom GKV-Kommunikationsserver erhaltenen Rückmeldedaten (Rückmeldungen, Verarbeitungsbestätigungen, technische und fachliche Fehlerrückmeldungen) zu quittieren.

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

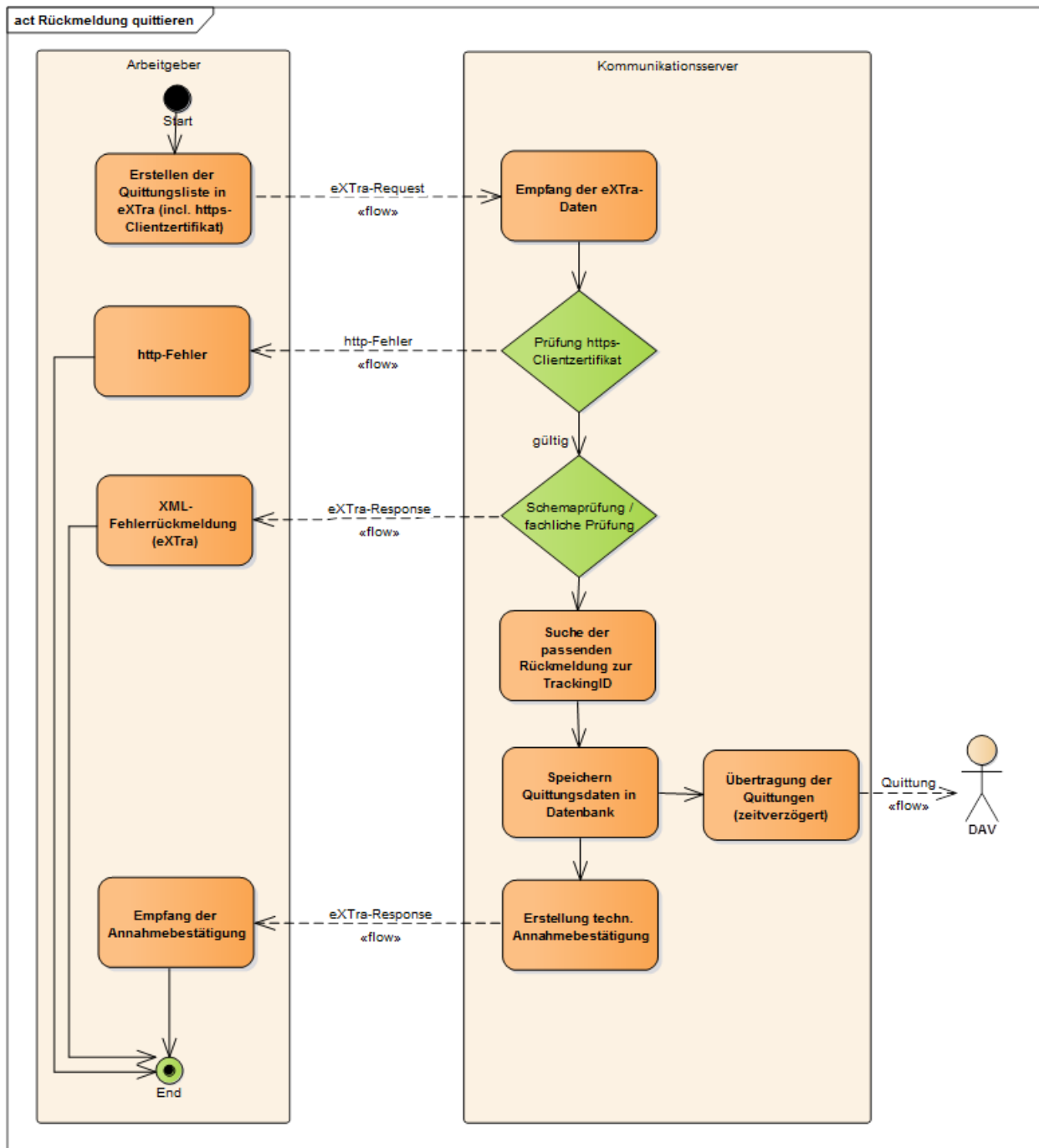


Abbildung 6: Flussdiagramm zum Verarbeitungsablauf der Empfangsquittungen

3 Ergänzende Informationen

3.1 Fachliche Rahmenbedingungen

3.1.1 Absender/Ersteller und Zertifikat

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.

Jeder AG muss sich eindeutig über ein Zertifikat authentifizieren, das eindeutig einer Absendernummer zugeordnet ist. Es ist immer nur das jüngste Zertifikat zu einer Absendernummer gültig. Die Absendernummer des Absenders wird somit als Abrufkriterium für den GKV-Kommunikationsserver zur Zuordnung der richtigen Rückmeldungen genutzt.

3.1.2 Adressierung der Meldung

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“ zuständige DAV und muss auch vom AG für diese DAV verschlüsselt werden. Die Zuordnung der Krankenkassen zu den DAVn kann der Beitragssatzdatei entnommen werden, die von der ITSG unter <https://beitragssatz.itsg.de> veröffentlicht wird.

Der Inhalt der Meldedatei ist in den jeweiligen Fachverfahren definiert.

3.2 Technische Rahmenbedingen

3.2.1 Schemadateien

Profilierte Schemata auf Basis von eXTra 1.4

Geschäftsfall am GKV-Kommunikationsserver	Prüfung im GKV-Kommunikationsserver gegen folgende XSD-Schemadatei
Meldung-Request	xsd_KomServer_1_request_senden_datenlieferungen_mtom.xsd
Meldung-Response	xsd_KomServer_2_response_senden_datenlieferungen_mtom.xsd
Statusanfrage-Request	xsd_KomServer_3_request_anfordern_rueckmeldungen_mtom.xsd
Statusanfrage-Response	xsd_KomServer_4_response_abholen_rueckmeldungen_mtom.xsd
Quittung-Request	xsd_KomServer_5_request_senden_empfangsquittungen_mtom.xsd
Quittung-Response	xsd_KomServer_6_response_senden_empfangsquittungen_mtom.xsd
Fehler-Response	xsd_KomServer_0_error_mtom.xsd

Profilierte Schemata auf Basis von Version eXTra 1.5

Geschäftsfall am GKV-Kommunikationsserver	Prüfung im GKV-Kommunikationsserver gegen folgende XSD-Schemadatei
Meldung-Request	Senden-request-envelope-1.0.0.xsd
Meldung-Response	Senden-response-envelope-1.0.0.xsd
Statusanfrage-Request	Statusanfrage-request-envelope-1.0.0.xsd
Statusanfrage-Response	Statusanfrage-response-envelope-1.0.0.xsd
Quittung-Request	Empfangsquittung-request-envelope-1.0.0.xsd
Quittung-Response	Empfangsquittung-response-envelope-1.0.0.xsd
Fehler-Response	extra-error-envelope-1.0.0.xsd

Hinweis:

Die Responses des GKV-Kommunikationsserver sind grau hinterlegt, eine etwaige Fehlerantwort ist dunkelgrau hinterlegt.

3.2.2 Webservice Schnittstelle

Der GKV-Kommunikationsserver stellt eine entsprechende SOAP-Schnittstelle bereit. MTOM (SOAP Message Transmission Optimization Mechanism) dient der Übertragung binärer Daten in Webservices. Durch den Entfall des Base64 wird die zu übertragende Datenmenge um ca. 33 % verringert.

3.2.2.1 Webservice-WSDL

Die WSDL Datei ist in der Schemabeschreibung enthalten.

Da die Webservice-URLs nur mit Client-Zertifikat-Authentifizierung erreichbar ist, wird auf die sonst übliche Bereitstellung der WSDL-Datei mit Hilfe einer http-GET-Anforderung und abschließender ?wsdl-Abfragezeichenfolge verzichtet. Die folgende Beispiel-URL ist somit **NICHT** gültig: <https://verarbeitung.gkv-kommunikationsserver.de/extra?wsdl>

3.2.2.2 Datenformat

Die Kommunikation mit dem GKV-Kommunikationsserver findet in einer profilierten (speziell für den GKV-Kommunikationsserver eingeschränkten) Variante des eXTra-Datenformats statt.

Das eXTra-Datenformat ist ein offener, frei verfügbarer Bundesstandard für den Datenaustausch.

Unterstützt werden die in Abschnitt 1.4 Kommunikationsstandard aufgeführten Versionen:

Für die Verwendung von MTOM müssen die folgenden Punkte eingehalten werden:

1. Header: Der http-Header „Content-Type“ des http-Requests muss den Wert „multipart/related; boundary=MIME-Multipart-Boundary“ besitzen (für https-POST lautet der Wert „application/xml“)
2. Datenformat: Die eXTra-XML-Dateien müssen in einen SOAP-Envelope eingebettet werden
3. Datenformat: Der üblicherweise BASE64-kodierte Inhalt muss als SOAP with Attachments unter Verwendung von MIME versendet werden

3.2.3 Geschäftsfall Meldungen

Der GKV-Kommunikationsserver ist in der Lage, Meldungen bis zu einer Gesamtgröße von 20 MB (brutto) bei https POST-Request und 60 MB (brutto) bei SOAP/MTOM als https POST-Request zu verarbeiten und den Kommunikationskanal bis zu 178 Sekunden für die Datenübertragung offen zu halten.

3.2.4 Geschäftsfall Rückmeldungen

Im Falle der zu übertragenden Rückmeldungen an den AG, erfolgt seitens des GKV-Kommunikationsserver eine Begrenzung auf max. 2400 Packages oder 20MB (netto). Sind weitere Daten vorhanden so erhält der AG eine entsprechende Info-Meldung (lxxx). In Einzelfällen kann die Grenze von 20 MB überschritten werden. Siehe hierzu auch Anhang B - Statuscodes des GKV-Kommunikationsservers.

3.2.5 Verbindungen über TLS mit TLS Clientzertifikat

- Alle http-Request zum GKV-Kommunikationsserver müssen über TLS gemäß den Vorgaben aus den Anlagen 8 und 16 der gemeinsamen Grundsätze Technik gesendet werden.
- Auch wenn das „TLS-Clientzertifikat“ vom Protokoll her optional ist, so gilt dieses jedoch bei Verbindungen zum GKV-Kommunikationsserver als verpflichtend und muss immer verwendet werden
- Als TLS-Clientzertifikat ist das Arbeitgeber-Zertifikat zu verwenden welches von einem Trustcenter gemäß der Security Schnittstelle (Anlage 16) bezogen wurde
- Das erhaltene TLS-Serverzertifikat des GKV-Kommunikationsservers ist auf Gültigkeit und die Domäne „gkv-kommunikationsserver.de“ zu überprüfen

3.2.6 Verwendung des neuesten Arbeitgeber-Zertifikats

- Da mit der Ausstellung eines neuen AG-Zertifikats (für dieselbe Betriebsnummer, Absendernummer oder Zahlstellennummer) alle bisherigen Zertifikate ihre Gültigkeit verlieren, ist immer das neueste Zertifikat zu verwenden

3.2.7 Quittierung von Rückmeldungen

- Alle Rückmeldungen (auch technische Fehlerrückmeldungen) müssen quittiert werden, da diese ansonsten erneut bereitgestellt (wiederholt) werden

- Die Quittierung sollte erfolgen, sobald die Rückmeldung clientseitig erfolgreich entschlüsselt und persistiert worden ist
- Im Falle einer Zertifikatsumstellung werden somit die noch nicht quittierten Rückmeldungen für das aktuelle Zertifikat neu verschlüsselt und gehen somit nicht verloren

3.2.8 Auswertung der Fehler- bzw. Rückgabeinformation

- Fehler- bzw. Statusrückmeldungen können sowohl auf eXTra-Transport als auch auf eXTra-Package-Ebene auftreten!
- Innerhalb eines <Report>Elements können jeweils mehrere <Flag>Elemente enthalten sein!
- Die „technischen Fehlerrückmeldungen“ (Code E4xx) sind im Rahmen der Rückmeldungen entsprechend zu quittieren

3.2.9 Zusammenfassung von mehreren Meldungen in einer Meldungsliste

- Um die Datenübertragung effizient zu gestalten, sollten möglichst viele Packages (auch für unterschiedliche DAVn/Verfahren) in einer Meldungsliste zusammengefasst werden (max. 20MB bei https POST-Request und max. 60 MB bei SOAP/MTOM als https POST-Request).

3.2.10 Verwendung von *-Anfragen und Besonderheiten beim eAU Verfahren

- Um die Datenübertragung effizient zu gestalten, sollte bei einer Anfrage kein Filter auf DAV oder Verfahren verwendet werden. Hierdurch werden vom GKV-Kommunikationsserver die Packages von allen betroffenen DAVn/Verfahren in einer Rückmeldung zusammengefasst (max. 20MB).
- Mit Aufnahme des Verfahrens für den Abruf der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) werden viele Millionen zusätzliche Datensätze pro Jahr und ein höheres Abrufverhalten der Arbeitgeber erwartet. Um der Besonderheit des einzelanlassbezogenen Verfahrens gerecht zu werden und zugleich die Belastung der Bestandssysteme zu minimieren, wird das eAU Verfahren bei einer *-Anfrage nicht berücksichtigt. Zu den Verfahrenskennungen EAA (eAU-Anfrage inkl. Verarbeitungsbestätigung oder Fehlerrückmeldung) und EAR (= fachliche Rückmeldung der Krankenkasse im eAU-Verfahren) wurde ein neues Verfahren EAS (= Verfahrensgruppe) eingeführt. Für den Abruf der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) hat der Arbeitgeber die Option, eine gebündelte

Statusanfrage mit der Verfahrenskennung EAS durchzuführen. Der GKV-Kommunikationsserver gibt als Antwort alle vorliegenden Verarbeitungsbestätigungen/Fehlerrückmeldungen (EAA) und alle vorliegenden fachlichen Rückmeldungen (EAR) aus dem eAU-Verfahren an den AG zurück. Alternativ darf der AG auch mit EAA oder EAR anfragen, dann werden die Rückmeldungen zum jeweiligen Verfahren zurückgeliefert.

3.2.11 Verfügbarkeitsanzeige

Damit die Arbeitgeber die Verfügbarkeit der Arbeitgeberschnittstelle zu jeder Zeit einsehen können, 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 „<https://status.gkv-kommunikationsserver.de>“ aufrufbar. Alternativ kann der Status auch über den Menüpunkt: „Verfügbarkeit“ auf dem Webportal des GKV-Kommunikationsservers unter „<https://www.gkv-kommunikationsserver.de>“ eingesehen werden.

Anhang A XML-Schema- und Beispieldateien

Aktuelle Schema- und Beispieldateien zu allen Geschäftsfällen sind auf folgender Seite zu finden:

- https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp

Bzgl. des Versands von Testdaten sind die entsprechenden Hinweise in den Beispieldateien und den Schemata, sowie in den Gemeinsamen Grundsätzen Technik zu beachten.

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.
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	Daten liegen vor, wobei nicht alle Kommunikationspartner erreichbar waren
I006	Keine Daten vorhanden, wobei nicht alle Kommunikationspartner erreichbar waren
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.
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
E110	Maximal zulässige HTTP-Datenmenge überschritten
E111	Es liegen keine Daten zu dieser Anfrage vor
E112	Die übermittelte "RequestID" ist nicht eindeutig
E113	Für diese Anfrage ist ein 'TestIndicator' (Echt oder Test) erforderlich
E114	Testbetriebsnummer für die Verwendung von E-Kennung nicht zulässig
E115	BBNR Abs.-Eigner aus eXtra-Header nicht identisch mit Packageinhalt
E118	Nutzdaten sind leer
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.
E205	Es ist ein Fehler bei der Verarbeitung der MIME-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**



Die Ausgabe aller Statuscodes erfolgt ausschließlich auf Header-Ebene. Im Fall der Statuscodes I005 und I006 wird empfohlen, nach 20 min den GKV-Kommunikationsserver erneut anzufragen.

Anhang C Glossar

Abkürzung	Beschreibung
ASCII	„American Standard Code for Information Interchange“, eine Zeichenkodierung
AG	Arbeitgeber oder andere Meldepflichtige
BBNR	Bundeseinheitliche Betriebsnummer

Datenlieferungen	Elektronische Meldungen im Arbeitgeberverfahren (z.B. Sozialversicherungsmeldungen und Beitragsnachweise)
DAV	Datenannahme- und -verteilstellen der gesetzlichen Krankenversicherung
DEÜV	Datenerfassungs- und -übermittlungsverordnung
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. TLS/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.
LDAP	Lightweight Directory Access Protocol
MTOM	Message Transmission Optimization Mechanism
PKCS#7	„Public Key Cryptography Standards“, ein Verschlüsselungs-Standard gemäß RFC 2315
SOAP	Simple Object Access Protocol
TLS	Transport Layer Security
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.
WSDL	Web Services Description Language
XML	Extensible Markup Language
XOP	XML-binary Optimized Packaging