Inhaltsverzeichnis

Abbildungsverzeichnis

1. Synchroner Dialog

1.1 Kommunikationsteilnehmer

Die Teilnehmer des synchronen Dialogs sind im Folgenden aufgeführt:

- Kommunikationspartner: Bei diesem Teilnehmer handelt es sich beispielsweise um Arbeitgeber (AG), Leistungserbringer (LE) oder Sozialversicherungsträger bzw. den Initiator einer Kommunikation.
- Sozialversicherungsträger: Bei diesem Teilnehmer handelt es sich um den Sozialversicherungsträger (im Folgenden als „SV-Träger“ bezeichnet), mit dem der synchrone Dialog durchgeführt werden soll.

1.2 Rolle des Kommunikationspartners

Der Kommunikationspartner übernimmt die im Folgenden aufgelisteten Funktionalitäten:

- Übertragung von verschlüsselten Meldungen (inkl. https Clientzertifikat) an den SV-Träger inklusive Prüfung des Serverzertifikats.
- Empfangen von fachlichen, verschlüsselten Rückmeldungen der SV-Träger.
- Empfangen von Fehlermeldungen der SV-Träger.

1.3 Rolle der Sozialversicherungsträger

Der SV-Träger übernimmt die folgenden Funktionalitäten:

- Empfang der Meldung vom Kommunikationspartner
- Prüfung https-Clientzertifikat
- Entschlüsselung und Signaturprüfung
- Durchführung struktureller und fachlicher Prüfungen, falls diese im Fachverfahren definiert sind
- Verarbeitung und Aufbereitung der fachlichen Rückmeldung (verschlüsselter und signierter Inhalt) / Fehlermeldung
- Übertragung an den Kommunikationspartner

1.4 Prozess des synchronen Dialogs

Der synchrone Dialog besteht aus dem folgendem Prozess:

Ein Kommunikationspartner sendet eine verschlüsselte Meldung an den SV-Träger.
Der SV-Träger verarbeitet diese Meldung und sendet das Verarbeitungsergebnis mit fachlicher Rückmeldung an den Kommunikationspartner.

1.4.1 Request/Response

Die Abbildung 1 verdeutlicht die Kommunikationswege zwischen dem Kommunikationspartner und dem SV-Träger. Des Weiteren werden die Verarbeitungsschritte des Kommunikationspartners und des SV-Trägers aufgezeigt.

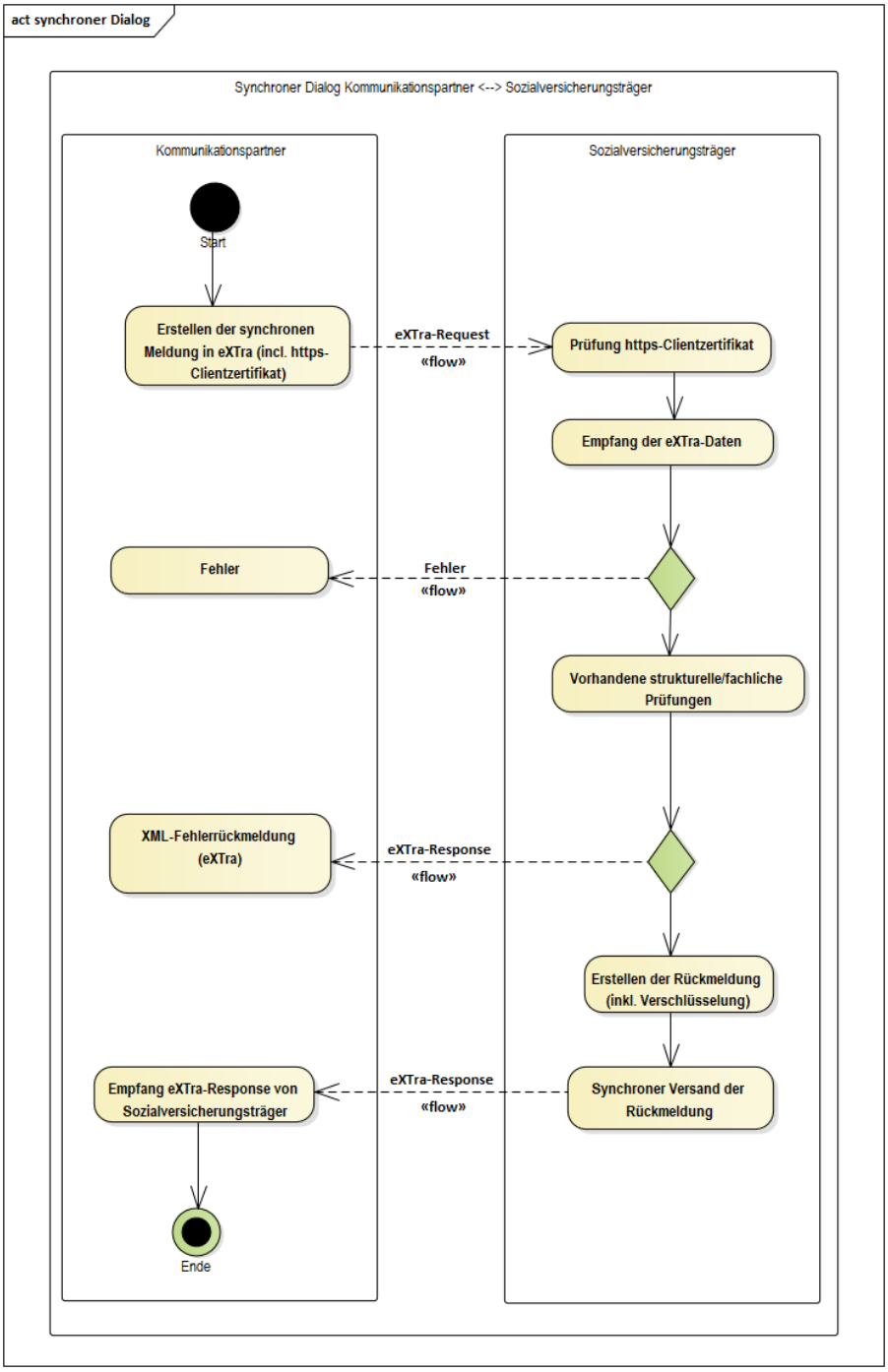

Abbildung 1 Diagramm zum Verarbeitungsablauf der synchronen Meldungen zum SV-Träger

Die Übertragung der in Abbildung 1 aufgeführten eXTra-Requests und eXTra-Responses erfolgt mittels MTOM (siehe 3.2.1). Im SOAP-Envelope-Body sind die Requests und Responses gemäß des eXTra-Strandards aufgebaut (siehe 2.2).

In dem für den synchronen Dialog profilierten eXTra-Standard bestehen die eXTra-Daten im generellen aus der Transport- und Packageebene (siehe folgende exemplarische Abbildung 2). Generell ist auf der Packageebene genau ein „Package“ zu platzieren! Die Regulierung der Messages (Datensatzanzahl) innerhalb eines Packages obliegt der inhaltlichen Ausgestaltung im jeweiligen Fachverfahren. Hierbei sollen einerseits die fachlichen Anforderungen und müssen andererseits die technisch prozessual leistbaren Kapazitätsgrenzen zur Aufrechterhaltung einer synchronen Kommunikation Berücksichtigung finden.

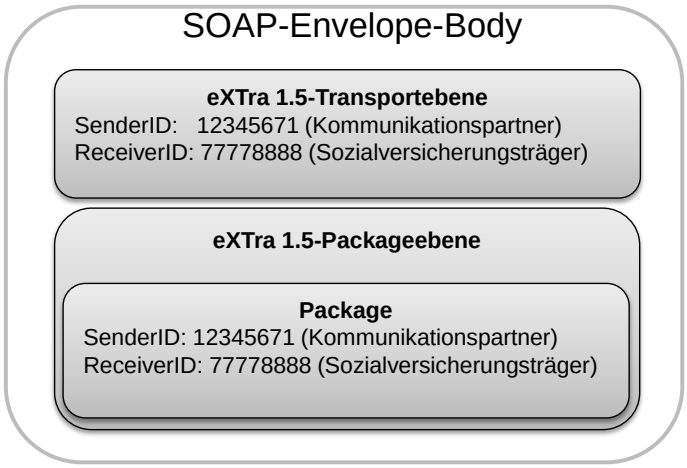

Abbildung 2 Gliederung eXTra-Nachricht

1.4.2 Request Kommunikationspartner → SV-Träger

Im Folgenden werden die eXTra-Adressierungsdaten innerhalb des SOAP-Envelope-Body im Request veranschaulicht.

Beim Aufbau der Adressierungsdaten vom Kommunikationspartner → SV-Träger ist auf der Transportebene als Empfänger (ReceiverID) der SV-Träger einzutragen und als Sender (SenderID) der Kommunikationspartner.
Innerhalb der Packageebene sind ebenfalls als Sender (SenderID) der Kommunikationspartner und als Receiver (ReceiverID) der SV-Träger einzutragen. Die SenderID auf der Transportebene und Packageebene sind somit immer identisch. Die ReceiverID der Transportebene kann sich jedoch von der in der Packageebene unterscheiden. Dies ist der Fall, wenn keine direkte Kommunikation zwischen Kommunikationspartner und SV-Träger erfolgt, sondern ein Intermediär (z. B. Kopfstelle oder Kommunikationsserver) zwischengeschaltet ist. In diesem Fall wird als Empfänger auf der Transportebene der Kommunikationsserver und auf der Packageebene der SV-Träger eingetragen.

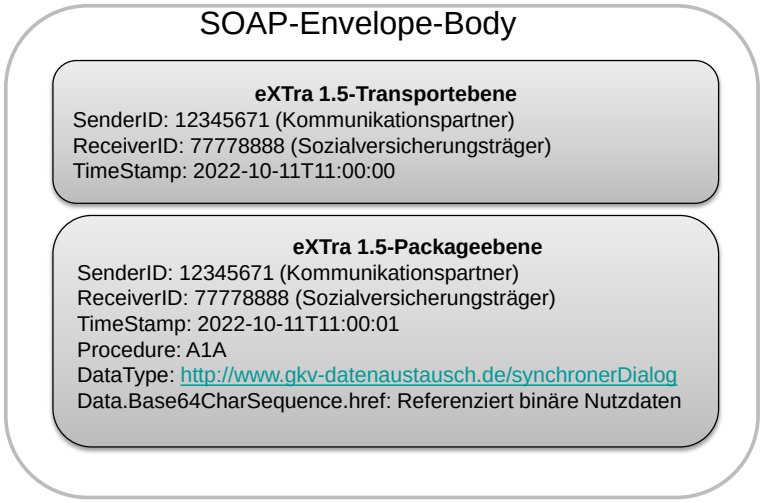

Abbildung 3 eXTra Request

1.4.3 Response SV-Träger → Kommunikationspartner

Im Folgenden werden die eXTra-Adressierungsdaten innerhalb des SOAP-Envelopes in der Response veranschaulicht. Hierbei ist zu beachten, dass die SenderID und ReceiverID auf Transportebene, als auch auf der Packageebene 1:1 dem erhaltenen Request entspricht.

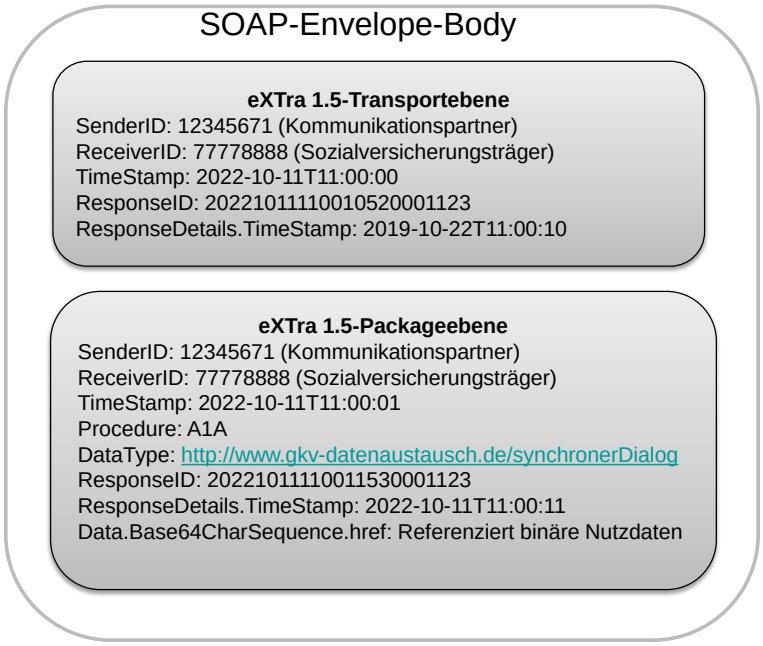

Abbildung 4 eXTra Response

Als Antwort erhält der Kommunikationspartner vom SV-Träger oder einem Intermediär eine der folgenden Responsearten:

Der MIME-Multipart-Boundary Part muss aus der Antwort entfernt werden damit es zu einer XML-Datei wird.

- Eine XML-Datei, die valide gegenüber SynchronerDialog\xsd_mtom\SynDialog-response-envelope-1.0.0.xsd ist und eine fachliche Antwort beinhaltet
- Eine XML-Datei, die valide gegenüber SynchronerDialog\xsd_mtom\SynDialog-response-envelope-1.0.0.xsd ist und im Element „Report“ die entsprechende Fehlermeldung beinhaltet (hierbei handelt es sich zum Beispiel um Fehler, die Wertebereiche verletzen)
- Eine XML-Datei, die valide gegenüber SynchronerDialog\xsd_mtom\extra-error-envelope-1.0.0.xsd ist (dies ist z.B. der Fall, wenn der Empfänger aus dem erhaltenen fehlerhaften Request nicht in der Lage ist eine Response wie in den ersten beiden Aufzählungspunkten beschrieben zu erzeugen).

2. Grundlagen der Kommunikation

2.1 Kommunikationsart

Die Kommunikation zwischen den Kommunikationspartnern für den synchronen Dialog ist über folgende Art möglich:

- Über die WebService-Schnittstelle mittels SOAP/MTOM als https POST-Request

Hierfür ist ein Client-Zertifikat erforderlich.

2.2 Kommunikationsstandard

Für den synchronen Dialog ist der eXTra-Standard in der Version 1.5 zu verwenden. Die Profilierung und Spezifikation der Verfahren werden durch die AWV (www.extra-standard.de) geprüft und freigegeben. Nach der Freigabe werden die Verfahren öffentlich auf der Seite der AWV als „Registrierte Verfahren“ mit entsprechenden Dokumenten zur Verfügung gestellt. In diesen sind auch die jeweiligen Steuerinformationen für die eXTra-Nachrichten und die Endpunkte der jeweiligen Dienste beschrieben. Die profilierten eXTra-Dateien für den synchronen Dialog sind über den Anhang dieses Dokumentes erhältlich.

2.3 Verschlüsselung und Zertifikate

2.3.1 Verschlüsselung der Melde – und Rückmeldedaten

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

2.3.2 Transportverschlüsselung und Authentifizierung über https

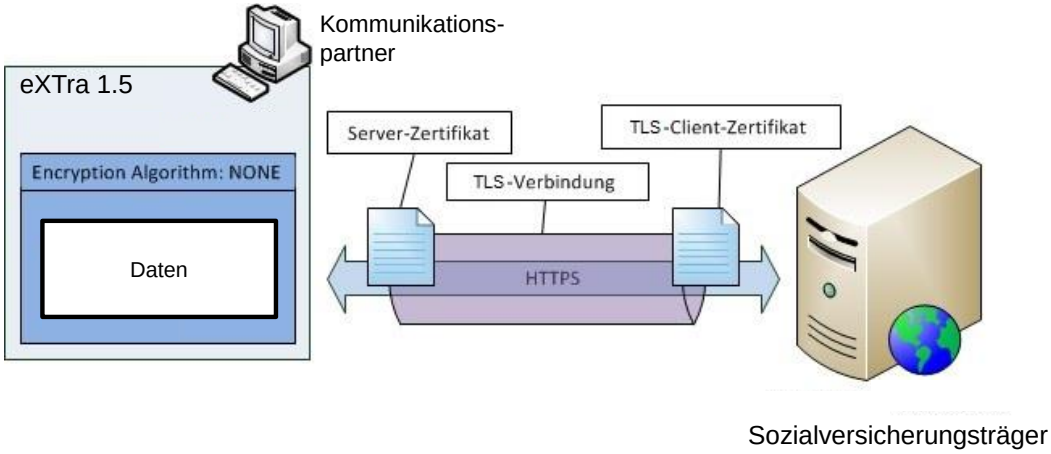

Abbildung 5 Verschlüsselung und Authentifizierung

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 Rahmen des Authentifizierungsprozesses wird ein eindeutiger Schlüssel (Session Key) erstellt, der anschließend für die Verschlüsselung der Nachricht(en) verwendet wird. Der Handshake erfolgt bei TLS Version 1.2 gemäß den in RFC 5246 (Abschnitt 7.4) sowie für TLS Version 1.3 gemäß den in RFC 8446 (Abschnitt 4) detailliert beschriebenen Bestimmungen.

Die Verwendung des TLS-Client-Zertifikats für den Aufbau einer TLS-Verbindung zum SV-Träger 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 Kommunikationspartner 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 Absendernummer/Institutionskennzeichen ausgestellte Zertifikat als „TLS-Client-Zertifikat“ an den SV-Träger übermitteln. Hierbei gilt zu beachten, dass diese Art der Kommunikation ggf. vorerst in der internen Firewall des Kommunikationspartners durch die dortige IT Abteilung freizuschalten ist. Der Kommunikationspartner muss im Gegenzug das vom SV-Träger 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.

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

2.4 Schemaprüfungen

Der SV-Träger prüft die vom Kommunikationspartner 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 Kommunikationspartner erstellt, die im Element „Report“ die entsprechende Fehlermeldung beinhaltet. Hier werden lediglich die mit der Kommunikation verbundenen Fehler zurückgemeldet.

Kann der SV-Träger keine eXTra-Antwort an den Kommunikationspartner erstellen, wird als Antwort eine „Error.xml“ (siehe die dazugehörige Schema- und XML-Beispieldateien) erstellt.

2.5 Kodierung

Die Steuerungsdaten werden mit dem Zeichensatz ISO-8859-1 verarbeitet. Die Zeichensätze der Nutzdaten sind in Anlage 15 der Gemeinsamen Grundsätze Technik definiert.

2.6 Abweichungen vom synchronen Verfahren / Sonderfälle

Nicht in allen Fachverfahren kann von vornherein sichergestellt werden, dass sämtliche Anfragen synchron beantwortet werden können. Dies kann unterschiedliche Gründe haben, beispielsweise eine fachliche Weiterleitung im Rahmen der Sachbearbeitung oder eine umfangreiche Prüfung durch einen Sachbearbeiter.

Für den Fall, dass über die synchrone Schnittstelle keine fachlich qualifizierte Antwort gegeben werden kann, muss eine asynchrone Kommunikation angeschlossen werden. Diese erfolgt durch erneute Übermittlung der ursprünglichen Anfrage an das asynchrone System.

3. Ergänzende Informationen

3.1 Fachliche Rahmenbedingungen

3.1.1 Absender/Ersteller und Zertifikat

Die Erstellung und Übermittlung der Meldungen kann durch den Kommunikationspartner 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 Kommunikationspartner muss sich eindeutig über ein Zertifikat authentifizieren, das eindeutig einer Absendernummer/Institutionskennzeichen zugeordnet ist. Die Absendernummer/Institutionskennzeichen des Absenders wird somit als Abrufkriterium für den Server beim SV-Träger zur Zuordnung der richtigen Rückmeldungen genutzt.

3.2 Technische Rahmenbedingen

3.2.1 WebService Schnittstelle

MTOM (SOAP Message Transmission Optimization Mechanism) dient der Übertragung binärer Daten in Webservices. Der SV-Träger stellt eine entsprechende Schnittstelle bereit. MTOM verwendet XML-binary Optimized Packaging (XOP) für die optimierte Übermittlung binärer Daten und ersetzt die sonst übliche Übertragung von Binärdaten mittels Base64-Kodierung in eXTra-XML-Dateien. Durch den Entfall des Base64 wird die zu übertragende Datenmenge um ca. 33 % verringert.

Die SV-Träger folgen hierbei der W3C-Empfehlung für die Übertragung binärer Daten in Webservices via MTOM (SOAP Message Transmission Optimization Mechanism) und verwendet XOP (XML-binary Optimized Packaging) für die optimierte Übermittlung binärer Daten.

3.2.1.1 WSDL Zugriff

Da die WebService-URL nur über eine https-POST-Anforderung 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.

3.2.1.2 Hinweise zur Erzeugung eines WebService-Clients

Die bereitgestellte WSDL-Datei bezieht sich auf den reinen eXTra-Standard und referenziert daher intern die XSD-Schemadateien des reinen eXTra-Standards und nicht die Schemadateien der hiervon abgeleiteten Synchronen-Dialog-Profilierung.

Der reine eXTra-Standard bietet mehr Freiheitsgrade – bezogen auf die Erzeugung von XML-Dateien - als die eXTra-Profilierung für den synchronen Dialog. Letztere bildet nur eine Untermenge des umfangreicheren eXTra-Standards ab.

Bei der Erstellung eines WebService-Clients anhand der bereitgestellten WSDL-Datei müssen die hieraus generierten XML-Dateien somit nicht nur gegen die XSD-Schemadateien des reinen eXTra-Standard validieren, sondern auch gegen die für den synchronen Dialog profilierten XSD-Schemadateien.

Die in der WSDL hinterlegten XSD-Schemadateien entsprechen dem weiter gefassten eXTra–Standard und beziehen sich – geschäftsfallunabhängig – auf einen Request bzw. eine Response:

WSDL-Message	In WSDL-Datei referenzierte XSD-Schemadatei
executeRequest	xsd_extra/ eXTra-request-1.xsd
executeResponse	xsd_extra/ eXTra-response-1.xsd
ExtraFault	xsd_extra/ eXTra-error-1.xsd

Hinweis:
Die Response des Servers beim SV-Träger ist grau hinterlegt, eine etwaige Fehlerantwort ist dunkelgrau hinterlegt.

Die von einem WebService-Client erzeugten XML-Dateien müssen jedoch vor der MTOM Umwandlung zusätzlich gegen die XSD-Schemadateien der eXTra-Profilierung für den Synchronen Dialog im Verzeichnis SynchronerDialog/xsd validieren.

Anschließend muss eine Umwandlung gemäß MTOM durchgeführt werden.

Bei den SV-Trägern erfolgt eine Validierung der Anfragen auf Basis der Schemata im Verzeichnis SynchronerDialog/xsd_mtom.

Der MIME-Multipart-Boundary Part muss aus der Anfrage entfernt werden bevor eine Validierung gegen die Schemata erfolgen kann .

Hinweis:

Die bereitgestellte WSDL Datei enthält auch XML-Beispieldateien. Diese enthalten jedoch nicht die MIME-Multipart-Boundary, um sie ohne weitere Anpassungen und mit allen gängigen XML-Tools gegen die zugehörigen Schemadateien zu validieren.

3.2.2 Verbindungen über TLS mit TLS Clientzertifikat

- Alle http-Requests müssen über TLS gemäß den Vorgaben aus den Anlagen 8 und 16 der gemeinsamen Grundsätze Technik gesendet werden.
- Die Nutzung des TLS-Clientzertifikats ist verpflichtend
- Als TLS-Clientzertifikat ist das Zertifikat zu verwenden, welches von einem Trustcenter gemäß der Security Schnittstelle (Anlage 16) bezogen wurde.
- Das erhaltene TLS-Serverzertifikat ist auf Gültigkeit und die entsprechende Domäne zu überprüfen.

3.2.3 Verwendung des neuesten Zertifikats

- Da mit der Ausstellung eines neuen Zertifikats (für dieselbe Absendernummer, Zahlstellennummer oder Institutionskennzeichen) in der Regel alle bisherigen Zertifikate ihre Gültigkeit verlieren, ist dann immer das neueste Zertifikat zu verwenden.
- In Ausnahme, insbesondere in Übergangszeiträumen für Zertifikatswechsel infolge veränderter Sicherheitsanforderungen (z. B. Wechsel des Krypto Systems oder Änderung der Schlüssellänge), gelten die Migrations-Vorgaben gemäß der jeweils gültigen Fassung der Security Schnittstelle (Anlage 16 der gemeinsamen Grundsätze Technik).

3.2.4 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!
- Return-Codes beginnend mit 0 signalisieren eine fehlerfreie Verarbeitung.

- Return-Codes beginnend mit 1 signalisieren, dass im Moment keine Verarbeitung möglich ist, so dass dieselbe Anfrage zu einem späteren Zeitpunkt erneut gestellt werden muss.
- Return-Codes beginnend mit 2 signalisieren technische Fehler, die auf Seiten der Anfrage verursacht wurden, so dass vor der erneuten Anfrage eine entsprechende Fehlerkorrektur zu erfolgen hat.
- Return-Codes beginnend mit 3 signalisieren, dass eine fachliche Beantwortung im Rahmen des synchronen Dialogs nicht möglich ist, so dass eine asynchrone Kommunikation anzustreben ist.

Anhang A XML-Schema- und Beispieldateien

Aktuelle Schema- und Beispieldateien sind unter https://www.gkv-datenaustausch.de/technische_standards_1/technische_standards.jsp als Anhang zur Anlage 21 zu finden.

Anhang B Glossar

Abkürzung	Beschreibung
AG	Arbeitgeber oder andere Meldepflichtige
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.
IK	Institutionskennzeichen
LE	Leistungserbringer
MTOM	Message Transmission Optimization Mechanism
PKCS#7	„Public Key Cryptography Standards“, ein Verschlüsselungs-Standard gemäß RFC 2315
RFC 5246	The Transport Layer Security (TLS) Protocol Version 1.2. Dierks & Rescorla. August 2008.
RFC 8446	The Transport Layer Security (TLS) Protocol Version 1.3. Rescorla & Mozilla. August 2008.
SOAP	Simple Object Access Protocol
SV-Träger	Sozialversicherungsträger
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