Inhaltsverzeichnis

1. Ziel und Festlegung der Schnittstellendefinition 1
1.1 Einleitung 1
1.2 Festlegungen 2
2. Kurzbeschreibung http / https 2
2.1 Hypertext Transfer Protocol 2
2.1.1 Anwendung von http 2
2.2 HyperText Transfer Protocol Secure 3
2.2.1 Anwendung von https 3
3. Angewandte Standards und Normen 4
3.1 Sicherheitsstandards 4
3.2 Kommunikationsstandards 4
4. Verfahrensbeschreibung 5
4.1 Voraussetzungen 5
4.2 Das Übermittlungsverfahren 5
4.2.1 Übermittlungen an Annahmestellen 6
4.2.2 Rückmeldungen der Eingangsquittung 7
4.3 Weiterverarbeitung der übermittelten Dateien 8
4.3.1 Weiterverarbeitung bei den Annahmestellen 8
4.3.2 Weiterverarbeitung bei dem Empfänger der Rückmeldungen 8
5. Anhang 8
5.1 Literaturverweise: 8

1. Ziel und Festlegung der Schnittstellendefinition

1.1 Einleitung

Die rasche technische Weiterentwicklung der Systeme und stetig neue Anforderungen erfordern eine Richtlinie für die Übermittlung von Dateien mittels Hypertext-Transfer-Protokoll im Gesundheits- und Sozialwesen.

Die folgende Definition einer Schnittstelle ist als festgeschriebene, jedoch offengelegte Schnittstelle für das Gesundheits- und Sozialwesen ausgelegt.

Ziel dieser Definitionen ist es, im Gesundheits- und Sozialwesen eine gesicherte digitale Kommunikation unabhängig von der Art der jeweiligen Systeme zu gewährleisten.

1.2 Festlegungen

Die Definition der Schnittstelle beschreibt die zulässigen Protokolle und das grundlegende Verfahrensmanagement für die automatisierten Verarbeitungsprozesse, um eine einheitliche Abwicklung zur Übermittlung von Dateien im Gesundheits- und Sozialwesen zu gewährleisten.

Unter Berücksichtigung neuer Kommunikationsverfahren, wie z. B. dem eXTra-Standard, werden in dieser Spezifikation ausschließlich die Rahmenbedingungen zur Nutzung der Protokolle im Gesundheits- und Sozialwesen definiert; Die technischen Details und Verfahrensbeschreibungen sind in den jeweils gültigen Rechs und angewandten Standards aufgeführt.

2. Kurzbeschreibung http / https

2.1 Hypertext Transfer Protocol

Das Hypertext Transfer Protocol (HTTP, dt. Hypertext-Übertragungsprotokoll) ist ein Protokoll zur Übertragung von Daten über ein Netzwerk. Es wird hauptsächlich eingesetzt, um Webseiten aus dem World Wide Web (WWW) in einen Webbrowser zu laden.

HTTP gehört der sogenannten Anwendungsschicht etablierter Netzwerkmodelle an. Die Anwendungsschicht wird von den Anwendungsprogrammen angesprochen, im Fall des HTTP ist dies meistens ein Webbrowser. Im ISO/OSI-Schichtenmodell entspricht die Anwendungsschicht den Schichten 5–7.

HTTP ist ein zustandsloses Protokoll. Ein zuverlässiges Mitführen von Sitzungsdaten kann erst auf der Anwendungsschicht durch eine Sitzung über eine Session-ID implementiert werden.

Durch Erweiterung seiner Anfragemethoden, Header-Informationen und Statuscodes ist das HTTP nicht auf Hypertext beschränkt, sondern wird zunehmend zum Austausch beliebiger Daten verwendet. Zur Kommunikation ist HTTP auf ein zuverlässiges Transportprotokoll angewiesen. In nahezu allen Fällen wird hierfür TCP verwendet.

2.1.1 Anwendung von http

Die Kommunikationseinheiten im HTTP zwischen Client und Server werden als Nachrichten bezeichnet, von denen es zwei unterschiedliche Arten gibt: die Anfrage (engl. Request) vom Client an den Server und die Antwort (engl. Response) als Reaktion darauf vom Server zum Client.

Jede Nachricht besteht dabei aus zwei Teilen, dem Nachrichtenkopf (engl. Message Header, kurz: Header oder auch HTTP-Header genannt) und dem Nachrichtenkörper (engl. Message Body, kurz: Body). Der Nachrichtenkopf enthält wichtige Informationen über den Nachrichtenkörper wie etwa verwendete Kodierungen oder den Inhaltstyp, damit dieser vom Empfänger korrekt interpretiert werden kann. Der Nachrichtenkörper enthält schließlich die Nutzdaten.

HTTP ist ein Kommunikationsschema, um Webseiten (oder Bilder oder prinzipiell jede andere beliebige Datei) von einem entfernten Computer auf den eigenen zu übertragen. Wenn auf einer Webseite der Link zur URL http://www.example.net/infotext.html aktiviert wird, so wird an den Computer mit dem Hostnamen www.example.net die Anfrage gerichtet, die Ressource /infotext.html zurückzusenden.

Der Name www.example.net wird dabei zuerst über das DNS-Protokoll in eine IP-Adresse umgesetzt. Zur Übertragung wird über TCP auf den Standard-Port 80 des HTTP-Servers eine HTTP-GET-Anforderung gesendet.

2.2 HyperText Transfer Protocol Secure

HTTPS steht für HyperText Transfer Protocol Secure (dt. sicheres Hypertext-Übertragungsprotokoll) und ist ein Verfahren, um Daten im World Wide Web abhörsicher zu übertragen. Technisch definiert es als URI-Schema eine zusätzliche Schicht zwischen HTTP und TCP.

2.2.1 Anwendung von https

Das HTTPS Protokoll wird zur Verschlüsselung, zur Authentifizierung der Kommunikation zwischen Webserver und Browser im World Wide Web verwendet.

Ohne Verschlüsselung sind Web-Daten für jeden, der Zugang zum entsprechenden Netz hat, als Klartext lesbar. Mit der zunehmenden Verbreitung von Funkverbindungen, die etwa an WLAN-Hotspots häufig unverschlüsselt ablaufen, nimmt die Bedeutung von HTTPS zu, da hiermit die Inhalte unabhängig vom Netz verschlüsselt werden. Es stellt dabei das einzige Verschlüsselungsverfahren dar, das ohne gesonderte Softwareinstallation auf allen Internet-fähigen Computern unterstützt wird.

Die Authentifizierung dient dazu, dass sich jede Seite der Identität des Verbindungspartners vergewissern kann – ein Problem, das durch Phishing-Angriffe zunehmend Bedeutung bekommt.

Syntaktisch ist HTTPS identisch mit dem Schema für HTTP, die zusätzliche Verschlüsselung der Daten geschieht mittels SSL/TLS:

Unter Verwendung des SSL-Handshake-Protokolls findet zunächst eine geschützte Identifikation und Authentifizierung der Kommunikationspartner statt. Anschließend wird mit Hilfe asymmetri-

scher Verschlüsselung oder des Diffie-Hellman-Schlüsselaustauschs ein gemeinsamer symmetrischer Sitzungsschlüssel ausgetauscht. Dieser wird schließlich zur Verschlüsselung der Nutzdaten verwendet.

Der Standard-Port für HTTPS-Verbindungen ist 443.

Neben den Server-Zertifikaten können auch signierte Client-Zertifikate nach X.509.3 erstellt werden. Dies ermöglicht eine Authentifizierung der Clients gegenüber dem Server, wird jedoch selten eingesetzt.

Siehe dazu auch das Kapitel „Sichere Transportebene mit TLS (SSL)“ in der Security Schnittstelle für den Datenaustausch im Gesundheits- und Sozialwesen.

3. Angewandte Standards und Normen

Das Verfahren basiert auf den bereits im Gesundheits- und Sozialwesen angewandten Richtlinien und zum anderen auf den Standards des Internets, die einfach umzusetzen sind.

3.1 Sicherheitsstandards

Im Gesundheits- und Sozialwesen werden zum Datenaustausch mit Arbeitgebern und Leistungserbringern kryptographische Verfahren eingesetzt. Diese sind in der jeweils aktuellen Security Schnittstelle für das Gesundheits- und Sozialwesen definiert.

Die dort definierten Standards sind im Gesundheits- und Sozialwesen etabliert. Es sind Trust Center-Strukturen vorhanden und die Annahmestellen sind mit der entsprechenden Software ausgestattet. Eine Vielzahl von Arbeitgebern bzw. Leistungserbringern arbeiten bereits mit diesen Lösungen.

Die Annahmestellen sind berechtigt, zum Schutz des eigenen Netzes gegen Missbrauch nur bestimmte IP-Adressen/-Adressbereiche (z.B. statische IP-Adressen) zum HTTP-Verfahren zuzulassen. Die obligatorische Benutzeranmeldung kann von den Annahmestellen in eigenem Ermessen fakultativ mit einem Passwort gesichert werden.

3.2 Kommunikationsstandards

Folgende Protokollvarianten der HTTP-Protokollfamilie zur Übermittlung von Dateien werden im Gesundheits- und Sozialwesen generell mit den Standardports unterstützt:

- HTTP 1.0 (Hypertext Transfer Protocol) gemäß RFC 1945 über den Port 80
- HTTP 1.1 (Hypertext Transfer Protocol) gemäß RFC 2616 über den Port 80
- HTTPS (Hypertext Transfer Protocol Secure) gemäß RFC 2818 über den Port 443

Bei HTTPS ist für den unsymmetrischen Sitzungsaufbau ein digitales Server-Zertifikat für SSL notwendig und auf dem Client, aber es wird kein HTTP-Cookie im Browser gesetzt. Bei erfolgreichem Sitzungsaufbau erfolgt die Übermittlung der Dateien in einem symmetrischen SSL-Tunnel.

Das für https verwendete digitale SSL Zertifikat muss von einer – selbst wiederum zertifizierten – Zertifizierungsstelle ausgestellt sein, das den Server und die Domain eindeutig identifiziert. Bei der Beantragung werden dazu etwa die Adressdaten und die Firmierung des Antragstellers geprüft.

Selbst-signierte Zertifikate (self-signed certificate), die ohne Beteiligung einer gesonderten Instanz erstellt wurden, sollen nicht verwendet werden, da diese zwar die Verschlüsselung, nicht aber die Authentifizierung ermöglichen. Solche Verbindungen sind damit verwundbar für einen man-in-the-middle-Angriff.

4. Verfahrensbeschreibung

4.1 Voraussetzungen

Es wird ein Verfahren zur Kommunikation über das Internet vorgeschlagen. Die bisherige elektronische Kommunikation zwischen Arbeitgebern, Leistungserbringern und Annahmestellen ist dateiorientiert. Es werden eine Nutzdaten-Datei mit den eigentlichen Nachrichten und ein Auftragssatz mit Routinginformationen gebildet. Dieses Verfahren wird beibehalten. Daneben kann auch der eXTra Standard zur Übermittlung von Daten mit http/https genutzt werden. Beide Verfahren werden in den Gemeinsamen Grundsätzen Technik definiert und werden als KKS (Krankenkassen-Kommunikations-System) bzw. eXTra (einheitliches XML-basiertes Transportverfahren) bezeichnet.

Um zu verhindern, dass Meldungen verfälscht oder von Unberechtigten gelesen werden, werden sie verschlüsselt. Hier werden im Gesundheits- und Sozialwesen etablierte Verfahren verwendet, die jeweils gültige Security Schnittstelle ist bindend.

Die Kommunikation setzt voraus, dass der Absender bereits über ein gültiges Zertifikat verfügt und somit die Möglichkeit der Verschlüsselung nutzen kann.

4.2 Das Übermittlungsverfahren

Das Übermittlungsverfahren über HTTP kommt sowohl bei Übermittlungen an die Annahmestellen als auch bei Rückmeldungen an die Teilnehmer zur Anwendung. Die Übermittlungen und Rückmeldungen erfolgen separat, da die Rückmeldungen nur auf eine Anfrage eines Teilnehmers von die Annahmestellen bereitgestellt werden.

4.2.1 Übermittlungen an Annahmestellen

Gemäß Security Schnittstelle verschlüsselt der Absender die Datei für den Empfänger, erstellt den dazugehörigen Auftragssatz und überträgt die Dateien mittels HTTP-Upload zu einem Server des Empfängers im Internet.

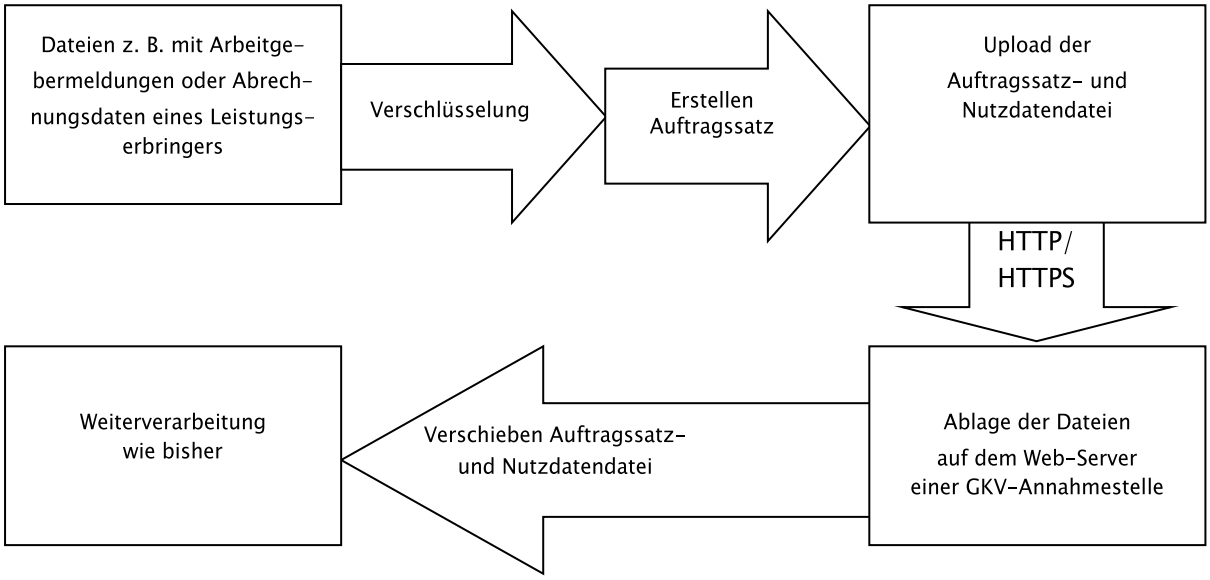
Bei http (außer bei der Nutzung von eXTra) identifiziert sich der Absender auf dem Web-Server durch Anmeldung mit Usernamen und Kennwort (z.B. mit seiner Betriebsnummer bzw. seinem Institutionskennzeichen). Die Anmeldung erfolgt case-sensitive, d. h. es ist die Groß-/Kleinschreibung zu beachten (z.B.: „BN12345678“ bzw. „IK123456789“).

Die Übermittlung selbst kann über zwei Verfahren, je nach Anwendungsfall, durchgeführt werden:

1. Manueller Upload: Ein Benutzer authentifiziert sich mit Usernamen und Kennwort auf einer Webseite und lädt beide Dateien manuell auf den Webserver
2. Automatischer Upload: Eine Anwendung des Senders authentifiziert sich via http(S) -Post bei dem Webserver der Annahmestelle.

In einer Session müssen die Dateilieferungen immer paarweise (eine Nutzdaten- und eine Auftragssatzdatei) übertragen werden. Vor Versand muss die Eindeutigkeit des verwendeten Dateinamens durch den Absender sichergestellt werden. Die Nutzdaten-Datei und die Auftragsdatei werden immer gemeinsam versendet.

Nach dem Ende des Upload-Prozesses ist der jeweilige Return-Code vom Absender (Uploader) auszuwerten. Eine erfolgreiche Beendigung des Transfers wird durch einen HTTP-Statuscode gemäß RFC vom empfangenden System bestätigt. Bei Übertragungsfehlern während der Übermittlung der Dateien ist das Dateipaar erneut zu übermitteln.
Die Übermittlung an eine GKV-Annahmestelle erfolgt gemäß nachfolgender Abbildung:



Nach erfolgter Übertragung eines Nutzdaten-, Auftragsatz-Dateipaares wird automatisch eine Antwort aus dem angewandten Verfahren erstellt. Auf Protokollebene erfolgt die Bestätigung der Übermittlung durch HTTP-Statuscodes.

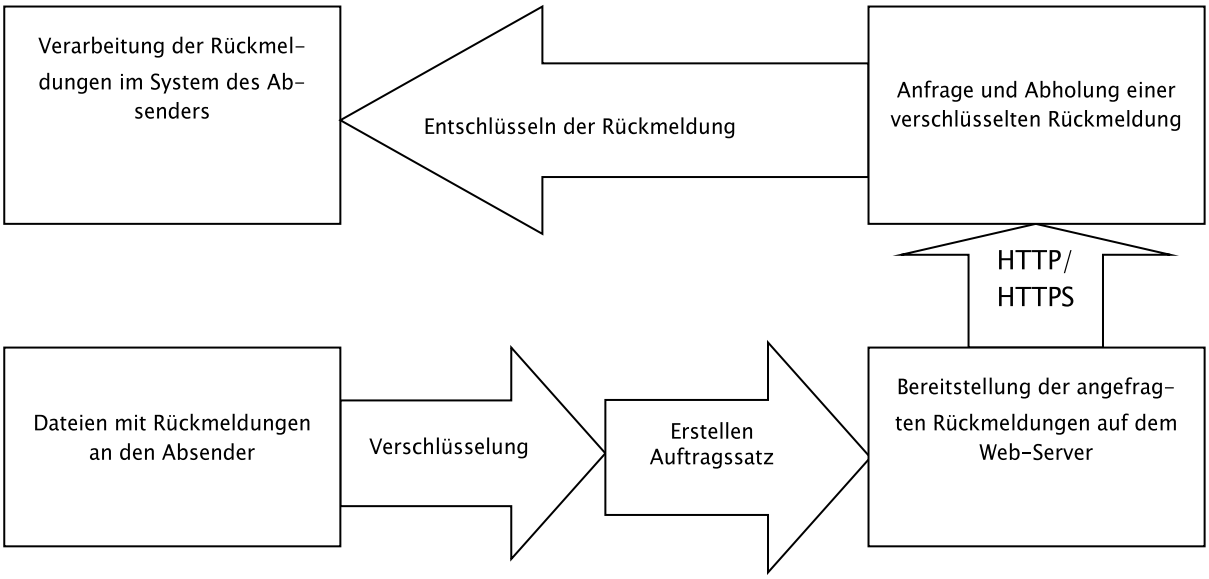
In Abhängigkeit von dem Ergebnis der Prüfungen wird das Dateipaar zur Verarbeitung weitergeleitet. Das Dateipaar ist für die Annahmestelle zur Weiterverarbeitung markiert und wird dort nach Eingangsprüfung und Verschiebevorgang automatisch weiterverarbeitet.

4.2.2 Rückmeldungen der Eingangsquittung

Die Übermittlung bzw. die Bereitstellung der Eingangsquittung ist vom gewählten Upload-Verfahren abhängig:

1. Rückmeldung nach manuellem Upload: Nach erfolgreichem Upload wird eine entsprechende Bestätigungsmeldung auf der Webseite ausgegeben.
2. Rückmeldung nach automatischem Upload: Nach dem Upload eines Teilnehmers werden von den Annahmestellen Rückmeldungen zum Download bereitgestellt. Die jeweilige Annahmestelle verschlüsselt die Rückantwort-Datei und erstellt den dazugehörigen Auftragssatz gemäß KKS für den Empfänger. Die Verschlüsselung muss den Vorgaben aus der jeweils aktuellen Security Schnittstelle für das Gesundheits- und Sozialwesen entsprechen. Die Dateien werden vom Empfänger mittels HTTP-Download vom angefragten Web-Server abgeholt. Die Anfrage und Rückmeldung erfolgen in einer Session. Auf Protokollebene erfolgt die Bestätigung der Übermittlung durch HTTP-Statuscodes.

Die Übermittlung einer Rückmeldung von einer Annahmestelle erfolgt gemäß nachfolgender Abbildung:



4.3 Weiterverarbeitung der übermittelten Dateien

4.3.1 Weiterverarbeitung bei den Annahmestellen

Die Dateien werden in das Dateisystem des Annahmeservers übertragen und auf Konsistenz geprüft. Die Dateipaare, die eindeutig benannt sind, werden per Filetransfer automatisch auf die Verarbeitungsrechner der Annahmestellen weitergeleitet und wie bisher verarbeitet, d. h. die Dateien werden entschlüsselt und die Nachrichten verarbeitet.

Der Annahmestelle (dem Betreiber des Web-Servers) obliegt die Pflicht, die Upload-Verzeichnisse regelmäßig nach abgebrochenen und fertig gestellten Transfers zu durchsuchen und zu bereinigen. Hierdurch hat der Server-Betreiber sicherzustellen, dass zu einem Upload stets ausreichend viele, freie (unbenutzte bzw. nicht-vergebene) Transfernummern zur Verfügung stehen.

4.3.2 Weiterverarbeitung bei dem Empfänger der Rückmeldungen

Die Dateien aus dem Download sind im Dateisystem des Empfängers abgelegt. Auf der Client-Seite werden die Dateien entschlüsselt und die Rückmeldungen in der jeweiligen Software verarbeitet.

5. Anhang

5.1 Literaturverweise:

[1] RFC 1945 HTTP 1.0 (Hypertext Transfer Protocol)

[2] RFC 2616 HTTP 1.1 (Hypertext Transfer Protocol)

[3] RFC 2818 HTTPS (Hypertext Transfer Protocol Secure)

[4] Wikipedia http://de.wikipedia.org/wiki/Http
http://de.wikipedia.org/wiki/Https