DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Spezifikation der XML-basierten Übermittlung der Unique Identifier von Arzneimittelpackungen für die warenbegleitende Datenlieferung im Krankenhausbereich

Version 1.0 – Stand 26.11.2018

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Inhalt

1 Einleitung

Die vorliegende Spezifikation der elektronischen Datenübermittlung stellt einen zentralen Baustein des Verfahrens der warenbegleitenden Datenlieferung zur Anbindung von Krankenhausapotheken an securPharm (1) dar. Das Verfahren der warenbegleitenden Datenlieferung ist bei Direktbelieferung von pharmazeutischen Unternehmen an Krankenhausapotheken anwendbar. Diese Spezifikation beschreibt, wie die Dateninhalte der Data Matrix Codes - also die Beschreibungen der Unique Identifier (UIs) - von verifikationsspflichtigen Packungen einer Warenlieferung von einem pharmazeutische Unternehmen an eine Krankenhausapotheke elektronisch übertragen werden.

Zurzeit empfängt ein nicht zu vernachlässigender Teil der Krankenhausapotheken noch keinerlei elektronische Informationen wie beispielsweise Rechnungen oder Lieferscheine vom Hersteller. Auch von Herstellerseite werden elektronische Verfahren nur teilweise unterstützt. Aus diesem Grunde wurde für die Übermittlung der Inhalte der Data Matrix Codes ein praktikables, aber dennoch sicheres Verfahren gewählt, welches auf Basistechnologien wie XML, E-Mail und ZIP beruht, die sowohl beim Hersteller als auch in der Krankenhausapotheke entweder schon vorhanden sind oder dort leicht eingerichtet werden können.

Durch die Nutzung des E-Mail-Verfahrens kann auf die Einrichtung oder Nutzung zusätzlicher Server für die Kommunikation zwischen pharmazeutischem Unternehmen und Krankenhausapotheke verzichtet werden. Die Verarbeitung von E-Mails, also Erstellung, Empfang, Versand und Weiterverarbeitung kann sowohl manuell als auch *automatisiert* erfolgen. E-Mail-basierte Übertragungsverfahren sind deshalb nach wie vor praxisrelevant. Beispielsweise wird ein e-mail-basiertes Verfahren für den Versand von DICOM-Daten im Rahmen von Teleradiologieanwendungen genutzt (2). Im IHE-Profil XDM ist der e-mail-basierte Versand von ZIP-Dateien zum sicheren Austausch von Patientendaten vorgesehen (3).

Die Übermittlung der UIs für eine Warenlieferung erfolgt in einer lieferungsbegleitenden E-Mail, wobei die XML-Beschreibungen der UI-Inhalte der Data Matrix Codes von serialisierten Packungen aus einer Lieferung in einer verschlüsselten ZIP-Datei im Anhang der E-Mail enthalten sind. Diese ZIP-Datei wird vom Hersteller für eine Lieferung erstellt, verschlüsselt und an die lieferungsbegleitende E-Mail angehängt. Nach dem Empfang der E-Mail durch die Krankenhausapotheke und dem Entschlüsseln und Entpacken der ZIP-Datei können die XML-Beschreibungen der UIs für die Verifikation und das Ausbuchen am securPharm-System genutzt werden.

Die folgenden Themen sind *nicht* Gegenstand der Spezifikation:

- Das Verfahren zur Erzeugung der XML-Beschreibung der UI-Inhalte der Data Matrix Codes der verifikationspflichtigen Packungen einer Lieferung als Voraussetzung für die Erstellung der ZIP-Datei und der E-Mail.

- Die Weiterverarbeitung der ZIP-Datei nach dem E-Mail-Empfang durch die Krankenhausapotheke (Entschlüsseln, Stichprobenverfahren, Verifizieren oder

Ausbuchen der mitgelieferten Seriennummern etc.). Die Weiterverarbeitung der UIs muss durch eine Software erfolgen, welche das in dieser Spezifikation beschriebene XML-Format einlesen und verarbeiten kann.

Die vorliegende Spezifikation macht keinerlei Vorgaben oder zusätzliche Annahmen im Hinblick auf die Codierung von Arzneimitteln, sondern setzt eine Codierung gemäß der jeweils gültigen securPharm-Codierrichtlinien voraus (4).

2 Voraussetzungen für die elektronische Datenübermittlung

Vor der Übermittlung von warenbegleitenden Datenlieferungen müssen Arzneimittelhersteller und Krankenhausapotheke **Absender- und Empfängeradressen** für den E-Mail-Austausch einrichten und vereinbaren. Neben den Adressen müssen Hersteller und Krankenhaus ein **Passwort für die symmetrische Ver- und Entschlüsselung der ZIP-Dateien** vereinbaren, welche die Dateninhalte der Data Matrix Codes, also der UIs der warenbegleitenden Datenlieferung, enthalten. Es müssen die im folgenden Abschnitt beschriebenen Vorgaben eingehalten werden.

2.1 Vereinbarung von E-Mail-Adressen und Passwort

Für die Vereinbarung der E-Mail-Adressen sowie die Vereinbarung des von Absender und Empfänger zu nutzenden Passworts sind die Vorgaben und Empfehlungen des BSI zu beachten (5; 6; 7; 8).

Besonders kritisch ist die Wahl und Vereinbarung des Passworts zwischen Absender und Empfänger. Für die Wahl des Passworts sind die folgenden Vorgaben zu beachten (5):

- Das Passwort darf nicht leicht zu erraten sein. Namen, Kfz-Kennzeichen, Geburtsdatum usw. dürfen deshalb nicht als Passwörter gewählt werden. Eine zufällige Generierung des Passwortes ist empfehlenswert.

- Ein Passwort sollte aus Großbuchstaben, Kleinbuchstaben, Sonderzeichen und Zahlen bestehen. Es sollten möglichst alle Zeichenarten verwendet werden.

- Das Passwort sollte mindestens 20 Zeichen lang sein. Die Spezifikation folgt hier einer Empfehlung des BSI für WLAN-Passwörter (6) mit dem Ziel, sogenannte Offline-Attacken zu vereiteln.

Es ist ein regelmäßiger Wechsel des Passworts nach den Vorgaben des BSI vorzusehen (5).

Durch den großen Zeichenvorrat ist bei Verwendung von zufällig generierten Passwörtern durch die gewählte Passwortlänge der Erfolg eines Brute-Force-Angriffs sehr unwahrscheinlich.

Die sichere Vereinbarung des Passworts kann beispielsweise erfolgen, indem der Hersteller der Krankenhausapotheke das Passwort in einem verschlossenen Umschlag mit einer persönlichen Empfangsadresse auf dem Postweg zukommen lässt. Die Vereinbarung von Absender- und Empfängeradresse (E-Mail und Post) kann telefonisch erfolgen.

Um einen ausreichenden Schutz der Unique Identifier zu gewährleisten, müssen Hersteller und Krankenhausapotheke die Vorgaben des BSI für den Umgang mit Passwörtern einhalten, die in der IT-Grundschutz-Maßnahme *M 2.11 Regelung des Passwortgebrauchs* definiert sind (5).

Für die verschlüsselte Datenübermittlung dürfen nur ZIP-Programme verwendet werden, deren symmetrisches Verschlüsselungsverfahren ausreichend sicher ist - vgl. Beispiel 2 in *M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte* (7). Das BSI nennt 7-Zip als Beispiel für ein softwarebasiertes Verschlüsselungsverfahren.

Sender und Empfänger müssen kompatible ZIP-Programme und Konfigurationen verwenden. Die Kompatibilität der Programme ist vor Beginn der datenbegleitenden Datenlieferungen durch den Versand von Testdaten sicherzustellen.

Hersteller und Krankenhausapotheke sollen die Vorgaben des BSI-Bausteins *B 5.3 Groupware* (8) für die Nutzung von E-Mails einhalten. Insbesondere müssen die E-Mail-Konten der warenbegleitenden Datenlieferung sowie die zugehörigen ZIP-Dateien und deren Inhalte so gesichert sein, dass ein Zugriff nur durch berechtigte Personen erfolgen kann.

Kann der Empfänger die ZIP-Datei mit demjenigen Passwort erfolgreich entschlüsseln, dass dem Absender zugeordnet ist, so bietet dies eine implizite Gewähr für die Authentizität der empfangenen Informationen, da eine sinnvoll zu entschlüsselnde E-Mail nur von demjenigen erzeugt werden konnte, der im Besitz des Schlüssels ist.

Die Sicherung der Übertragung erfolgt durch die symmetrische Verschlüsselung des übertragenen Datenpakets sowie durch die Nutzung der Transportverschlüsselung SSL/TLS (9; 10) für Teile des Übertragungsweges. Im unwahrscheinlichen Fall, dass die UIs einer Lieferung durch einen Angreifer abgegriffen und entschlüsselt werden können, verbleibt für die Nutzung dieser UIs zum Verpacken und Inverkehrbringen gefälschter Ware nur das Zeitfenster zwischen der Erstellung der Lieferungs-Mail und dem Ausbuchen durch die Krankenhausapotheke bei Wareneingang, d. h. in der Regel nur 1 – 2 Tage. Der Betrugsversuch würde in diesem Fall beim Verifizieren bzw. Ausbuchen entweder beim Empfänger der Originalware oder beim Empfänger der Fälschungen auffallen - das Ausbuchen sollte deshalb möglichst gleich beim Wareneingang erfolgen. In der Gesamtbetrachtung erscheint es nicht wahrscheinlich, dass über einen Angriff auf die elektronische Datenübermittlung gefälschte Ware erfolgreich in Verkehr gebracht werden kann.

Zum Schutz vor Manipulationen der Warenlieferung kommt ein Stichprobenverfahren zum Einsatz, welches in der Umsetzungsempfehlung der DKG zur warenbegleitenden Datenlieferung separat beschrieben wird.

3 Aufbau der elektronischen Datenübermittlung

Die warenbegleitende Datenlieferung beinhaltet den Aufbau, Versand und Empfang einer E-Mail, die genau eine verschlüsselte ZIP-Datei als Anhang besitzt, welche die XML-Beschreibungen der UI-Dateninhalte der Data Matrix Codes von verifikationspflichtigen Packungen der Lieferung in einer oder mehreren XML-Dateien enthält. Die Inhalte der XML-Beschreibungen (also die UIs) werden in einem späteren Schritt zum Verifizieren und Ausbuchen am securPharm-System genutzt. In den folgenden Abschnitten werden die einzelnen Bausteine der elektronischen Datenübermittlung dargestellt.

3.1 XML-Darstellung der warenbegleitenden Datenlieferung

3.1.1 XML-Darstellung der Lieferungsdatei

Für alle Packungen einer Lieferung kann eine *gemeinsame* XML-Datei erstellt werden, die den Namen

```
universal_identifiers_[LNR].xml
```

erhält, wobei `[LNR]` durch die Lieferungsnummer zu ersetzen ist.

Das Top-Level-Element `Shipment` der XML-Datei beinhaltet die XML-Darstellungen der UIs. Das Pflichtattribut `snr` muss zur Angabe der Lieferungsnummer genutzt werden. Es ergibt sich so die folgende schematische Darstellung:

```
<Shipment snr="[LNR]">
    Content-Element der Packung 1
    Content-Element der Packung 2
    …
    Content-Element der Packung N
</Shipment>
```

`[LNR]` ist auch hier durch die konkrete Lieferungsnummer zu ersetzen.

Die Lieferungsnummer LNR darf die Sonderzeichen \, /, :, *, ?, ", <, >, | nicht enthalten. Von der Verwendung von Leerzeichen und anderen Sonderzeichen wird abgeraten.

Vor dem `Shipment`-Element muss wie üblich eine passende XML-Deklaration eingefügt werden, z. B.

```
<?xml version="1.0" encoding="UTF-8"?>
```

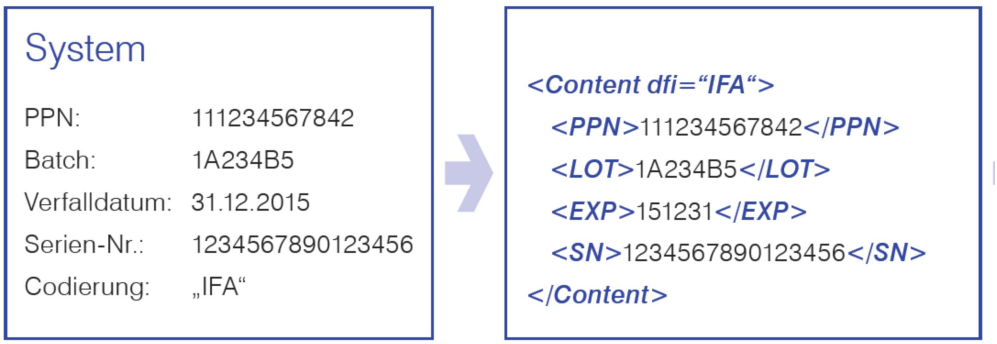
3.1.2 XML-Code einer serialisierten Packung

Für die Codierung eines verifizierungspflichtigen Arzneimittels ist die jeweils gültige Spezifikation der securPharm-Codierregeln zu verwenden (4), so dass ein problemloses Verifizieren und Ausbuchen der Arzneimittelpackungen ermöglicht wird. Die vorliegende Spezifikation macht keine eigenen Vorgaben zur Kodierung.

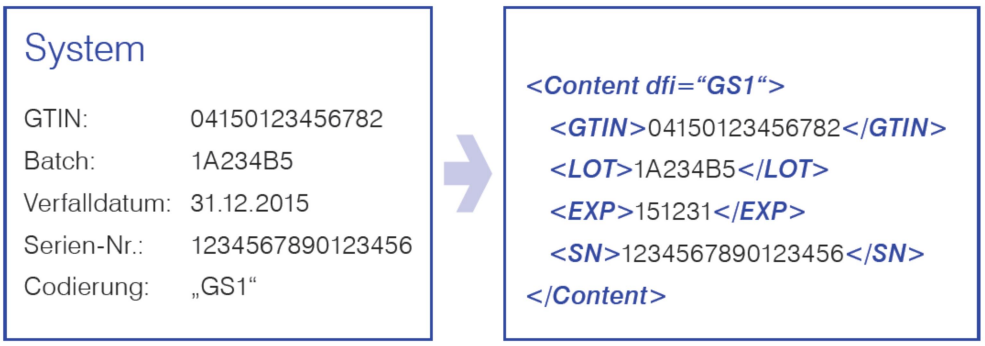
Für den elektronischen Datenaustausch muss die in Abschnitt 8 sowie in den Anhängen A und C der Codierregeln (4) definierte *XML-Beschreibung* des UI-Dateninhalts der Data Matrix Codes verwendet werden. Die XML-Beschreibung einer Packung umfasst den Produktcode, die Seriennummer, die Chargenbezeichnung sowie das Verfallsdatum, die zusammen den Unique Identifier (UI) bilden. Die grafische Darstellung des Data Matrix Codes ist nicht Teil der Datenlieferung. Besonderheiten für Multi Market Packs werden in Abschnitt 3.1.3 beschrieben.

Eine serialisierte Packung der Lieferung wird durch genau ein `Content`-Element repräsentiert, das gemäß der Codierregeln (4) definiert ist. Abhängig von der gewählten Codiervariante – ASC oder GS1 – ergeben sich zwei unterschiedliche Darstellungen:

1. Beispielhafte Darstellung im ASC-Format (4):



2. Beispielhafte Darstellung im GS1-Format (4):



Hinweis: Gemäß den Codierregeln (4) haben auch Packungen, deren Data Matrix Code auf dem GS1-Format basiert, zurzeit den Aufdruck „PPN“. Das tatsächliche Codierschema (ASC oder GS1) erschließt sich beispielsweise aus dem Format des Produktcodes (4).

Im Folgenden wird als Beispiel eine Lieferung mit der Nummer `44444444 betrachtet`, die zwei Packungen umfasst. Für die warenbegleitende Datenlieferung muss eine XML-Datei mit dem Namen „universal_identifiers_`44444444.xml`“ und dem folgenden Inhalt erzeugt werden:

```
<Shipment snr=“44444444“>
      <Content dfi=“IFA“>
            <PPN>111234567842</PPN>
            <LOT>1A234B5</LOT>
            <EXP>151231</EXP>
            <SN>1234567890123456</SN>
      </Content>
      <Content dfi=“GS1“>
            <GTIN>04150123456792</GTIN>
            <LOT>1A234B6</LOT>
            <EXP>151232</EXP>
            <SN>1234567890123457</SN>
      </Content>
<Shipment>
```

3.1.3 Multi Market Packs

Bei Multi Market Packs können im Data Matrix Code neben dem Produktcode und den anderen Angaben des UI zusätzliche Datenelemente enthalten sein (4). Dies sind eine oder mehrere sogenannte NHRN, die der landesspezifischen Produktidentifizierung dienen.

In der aktuellen Version der securPharm-Codierregeln (4) sind keine XML-Knoten definiert, mit denen NHRN in der XML-Darstellung abgebildet werden können. NHRN werden gemäß der NGDA-Schnittstellenbeschreibung (11) allerdings auch nicht zur Ausbuchung am securPharm-Server benötigt und sind insofern für die warenbegleitende Datenlieferung nicht relevant. Bei Bedarf können die entsprechenden Informationen dem Aufdruck (Data Matrix Code) der Einzelpackung entnommen werden.

Die NHRN dürfen aus den genannten Gründen beim Verfahren der warenbegleitenden Datenlieferung **nicht** in die XML-Darstellungen der UIs aufgenommen werden. Dies

betrifft auch eine möglicherweise im Data Matrix Code als NHRN neben dem Produktcode vorhandene PZN. Zum Ausbuchen wird nur der jeweilige Productcode benötigt, der in jedem Fall vorhanden ist und mitgeliefert werden muss.

3.1.4 Aufbau des ZIP-Containers für die warenbegleitenden Datenlieferung

Für den e-mail-basierten Transport wird die XML-Datei der Lieferung durch eine verschlüsselte ZIP-Datei gekapselt. Die ZIP-Datei für die warenbegleitende Datenlieferung mit der Lieferungsnummer `LNR` muss das Lieferungs-XML in einem Verzeichnis

```
universal_identifiers_[LNR]/
```

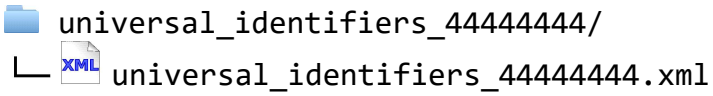
enthalten.

Die mit dem vereinbarten Passwort verschlüsselte ZIP-Datei erhält damit den Dateinamen

```
universal_identifiers_[LNR].zip
```

wobei `[LNR]` hier wieder durch die konkrete Lieferungsnummer zu ersetzen ist.

Für eine Beispiellieferung mit der Lieferungsnummer `44444444 ergibt sich` also die folgende Verzeichnisstruktur:



Die hieraus vom verwendeten ZIP-Programm erzeugte ZIP-Datei erhält dann den Dateinamen `universal_identifiers_44444444.zip.`

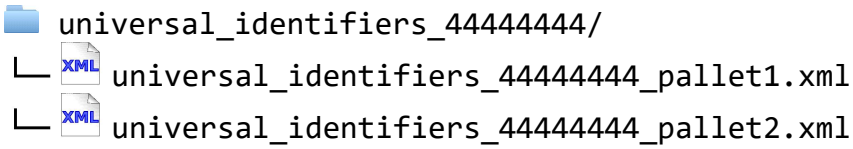
3.1.5 Berücksichtigung von Versandeinheiten

Packungen können in Versandeinheiten (z. B. Kisten oder Paletten) gruppiert sein. Die Identifikatoren der Versandeinheiten können optional in der warenbegleitenden Datenlieferung mitgegeben werden, um die Zuordnung von Packungen und Versandeinheiten zu erleichtern. Zu diesem Zweck kann eine XML-Datei pro Versandeinheit erstellt werden, so dass die zu erstellende ZIP-Datei mehrere XML-Dateien umfassen kann.

Der jeweilige Dateiname wird um die Identifikation `CID` der Versandeinheit ergänzt:

```
universal_identifiers_[LNR]_[CID].xml
```

Für eine Beispiellieferung mit der Lieferungsnummer `44444444` und zwei Paletten mit den Identifikatoren (`CIDs`) `pallet1` und `pallet2` ergibt sich beispielhaft also die folgende Verzeichnisstruktur:



Bezüglich Sonderzeichen gilt dieselbe Regelung wie für Lieferungsnummern.

Hinweis: Auch bei verschlüsselten ZIP-Dateien sind die Dateinamen innerhalb der ZIP-Datei auslesbar. Diese dürfen deshalb keine Informationen aus den UIs der Lieferungen enthalten. Einen Schutz auch der Dateinamen bietet das .7z-Format, das optional zwischen Sender und Empfänger vereinbart werden kann.

3.2 E-Mail-basierter Transport der Daten

Die Übermittlung der UIs einer Lieferung in Form einer verschlüsselten ZIP-Datei erfolgt per E-Mail.

Mit den im Abschnitt 3.1 erfolgten Festlegungen ist der Aufbau einer E-Mail für die warenbegleitende Datenlieferung wie folgt definiert:

- `From:` Absenderadresse des Herstellers,
- `To:` Empfangsadresse der Krankenhausapotheke,
- Subject: „Warenbegleitende Datenlieferung zur Lieferung [LNR]“,
- `Date:` Zeitpunkt der Erstellung.

Die E-Mail zur warenbegleitenden Datenlieferung muss die in Abschnitt 3.1.4 beschriebene Datei als einzigen Anhang enthalten. Der Body kann einen informativen Text des Herstellers enthalten, der jedoch für die Verarbeitung der Datenlieferung keine Rolle spielt und keine Informationen zu den Unique Identifiers enthalten darf.

Überschreitet die Größe der generierten E-Mail 10 MB, so muss die warenbegleitende Datenlieferung in mehreren E-Mails erfolgen. In den verwendeten Dateinamen sowie im Attribut „`snr`“ des `Shipment`-Elements ist die Lieferungsnummer dann mit einem fortlaufenden Index für die Datenteillieferung am Ende zu ergänzen.

Zur transportverschlüsselten Übertragung der E-Mail sollte möglichst SSL/TLS genutzt werden (9; 10).

Der Sender der E-Mail kann vom Empfänger eine Lesebestätigung in Form einer *Message Disposition Notification* (MDN) anfordern. Wird eine MDN angefordert, so soll der Empfänger den Empfang der E-Mail durch den Versand einer MDN an den Sender der ursprünglichen E-Mail bestätigen. Hierfür muss der E-Mail-Client ggf. geeignet konfiguriert werden.

4 Ablauf der elektronischen Datenübermittlung

Wenn eine Warenlieferung eines Herstellers an eine Krankenhausapotheke erfolgt, so muss dieser eine E-Mail zur warenbegleitenden Datenlieferung gemäß der Vorgaben in Abschnitt 3 erstellen und versenden. Es ist zulässig, dass die zugehörige ZIP-Datei nur die XML-Beschreibungen eines Teils der verifizierungsplichtigen Packungen enthält.

Der Versand der E-Mail soll so erfolgen, dass diese das Krankenhaus spätestens mit dem Eingang der Warenlieferung erreicht, so dass ein Ausbuchen der Packungen bei oder nach Lieferungseingang möglich ist.

Die zu einer Warenlieferung gehörige E-Mail darf vom pharmazeutischen Unternehmen nur an die festgelegte und vereinbarte E-Mail-Adresse der empfangenden Krankenhausapotheke gesendet werden. Die Einbeziehung weiterer Empfänger ist nicht erlaubt.

Die Krankenhausapotheke, welche eine E-Mail eines bekannten Herstellers an die vorher festgelegte E-Mail-Adresse erhält, speichert die verschlüsselte ZIP-Datei auf der Festplatte, wo sie für die Weiterverarbeitung zur Verfügung steht. Dabei ist die Datei gesichert und mit beschränkten Zugriffsrechten abzuspeichern.

Treten Probleme beim Senden, beim Empfang oder der Verarbeitung der E-Mail und ihres Inhalts auf, so erfolgt ein Clearing zwischen Hersteller und Krankenhausapotheke. Für den sicheren Empfang der E-Mail ist ein Whitelisting der Senderadressen zu empfehlen. Zudem muss sichergestellt werden, dass der Dateianhang der E-Mail nicht durch den E-Mail-Server blockiert wird. Erreicht eine warenbegleitende Datenlieferung per E-Mail die Krankenhausapotheke dennoch nicht, so kann und muss ein packungsweises Verifizieren bzw. Ausbuchen der Ware gemäß den Vorgaben von securPharm erfolgen.

5 Quellen

1. **securPharm e.V.** *Website.* [Online] [Zitat vom: 21. 08 2018.] http://www.securpharm.de/index.html.

2. **@GIT-Initiative zur Standardisierung von Telemedizin .** DICOM-E-MAIL-Standardempfehlung. *https://www.agit.drg.de/de-DE/1228/dicom-e-mail-standardempfehlung/.* [Online] [Zitat vom: 28. 11 2018.]

3. **IHE.** Cross-enterprise Document Media Interchange. [Online] [Zitat vom: 21. 11 2018.] https://wiki.ihe.net/index.php/Cross-enterprise_Document_Media_Interchange.

4. **securPharm e.V.** Codierregeln. [Online] http://www.securpharm.de/pharma/codierregeln.html.

5. **BSI.** M 2.11 Regelung des Passwortgebrauchs. [Online] [Zitat vom: 20. 08 2018.] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html.

6. —. B 5.3 Groupware. [Online] [Zitat vom: 20. 08 2018.] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b05/b05003.html.

7. —. M 2.163 Erhebung der Einflussfaktoren für kryptographische Verfahren und Produkte. [Online] [Zitat vom: 20. 08 2018.] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02163.html.

8. —. Sichere Nutzung von WLAN (ISi-WLAN) - BSI-Leitlinie zur Internet-Sicherheit (ISi-L). [Online] [Zitat vom: 21. 11 2018.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_wlan_leitlinie.pdf?__blob=publicationFile&v=1.

9. —. M 5.177 Serverseitige Verwendung von SSL/TLS. [Online] [Zitat vom: 17. 10 2018.] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05177.html.

10. —. M 5.66 Clientseitige Verwendung von SSL/TLS . [Online] [Zitat vom: 17. 10 2018.] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05066.html.

11. **NGDA – Netzgesellschaft Deutscher Apotheker mbH.** securPharm Apothekenserver - Implementierungsleitfaden Client-Implementierungen (Version 1.11). *Partnerportal für Entwickler.* [Online] 2018. 07 13. https://securpharm.ngdalabor.de/partnerportal.

12. **GS1 Germany e.V.** [Online] [Zitat vom: 21. 08 2018.] https://www.gs1-germany.de/.