Dokumentenhistorie

Aktuelle Version 2021-06-30 FAQs für Verifizierende Stellenv1	Stand: 30.06.2021
Vorherige Version Keine Vorgängerversion verfügbar	

Allgemeine Fragen und Antworten zu securPharm für Verifizierende Stellen

Die FAQs sammeln allgemeine Fragen und Antworten zu securPharm und dem securPharm-System für Verifizierende Stellen (z. B. Apotheker, Großhändler u.a.). Es ist zu beachten, dass die Verbände einzelner Nutzergruppen ihren Mitgliedern weit umfangreichere und detailliertere Information zur Verfügung stellen, die auf die spezifischen Fragestellungen der einzelnen Nutzergruppen eingehen. Es empfiehlt sich daher, die Veröffentlichungen der einzelnen Verbände zu diesen Themen vorrangig zu berücksichtigen.

Die Antworten haben keinen rechtsverbindlichen Charakter, sondern stellen die Auffassung und den Kenntnisstand von securPharm zum Datum der Erstellung dar.

Inhalt

1. Allgemeine Fragen zu securPharm und zum Fälschungsschutz

1.1: Warum brauchen wir ein Schutzsystem für Arzneimittel? Es gibt doch kaum Fälschungen in der legalen Lieferkette.

Bislang gibt es nur selten gefälschte Arzneimittel in der legalen Lieferkette. Die Verfügbarkeit gut gemachter Fälschungen erhöht aber die Gefahr. Das Schutzsystem ist deshalb präventiv eingeführt worden, um das hohe Sicherheitsniveau im legalen Arzneimittelhandel zu wahren und weiter zu verbessern.

1.2: Wer ist securPharm e.V.?

securPharm e. V. ist die deutsche Organisation für die Echtheitsprüfung von Arzneimitteln und verantwortlich für den Betrieb des Systems zur Echtheitsprüfung von Arzneimitteln. Der Verein wurde zur Umsetzung der EU-Fälschungsschutzrichtlinie 2011/62/EU und der Delegierten Verordnung (EU) Nr. 2016/161 von ABDA, BAH, BPI, PHAGRO und dem vfa gegründet. Zu den Gründungsmitgliedern zählen außerdem die Avoxa – Mediengruppe Deutscher Apotheker GmbH und die IFA – Informationsstelle für Arzneimittel GmbH. securPharm arbeitet als nicht-gewinnorientierte Organisation. securPharm ist der deutsche Baustein des EU-weiten Netzwerks EMVS gegen Arzneimittelfälschungen.

1.3: Wie können sich Verifizierende Stellen an das securPharm-System anschließen?

Verifizierende Stellen schließen sich über den Apothekenserver an das securPharm-System an. Die technische Umsetzung erfolgt über den Softwarepartner. Betreiber des Apothekenservers ist die Netzgesellschaft deutscher Apotheker mbH (NGDA), eine 100%ige Tochtergesellschaft der Avoxa. Die NGDA ist für die Legitimation und die Anbindung der Teilnehmer (Apotheker, Großhändler, Gesundheitseinrichtungen) verantwortlich.

1.4: Wer kann sich an das Apothekensystem anschließen?

An das Apothekensystem schließen sich alle Akteure an, die von der Fälschungsschutzrichtlinie betroffen und nicht pharmazeutische Unternehmen sind, insbesondere öffentliche Apotheken, Krankenhäuser und pharmazeutische Großhändler.

1.5: Welche Sicherheitsmerkmale fordert die Fälschungsschutzrichtlinie?

Die Fälschungsschutzrichtlinie schreibt seit dem 9. Februar 2019 zwei neue Sicherheitsmerkmale auf der Verpackung verschreibungspflichtiger Arzneimittel vor. Ein Erstöffnungsschutz (Anti-tampering Device), an dem erkennbar ist, ob eine Packung schon einmal geöffnet wurde, soll gewährleisten, dass der Inhalt der Packung echt ist. Ein individuelles Erkennungsmerkmal (Unique Identifier) soll jede Packung eindeutig identifizierbar machen.

1.6: Wie sieht das individuelle Erkennungsmerkmal aus?

Das individuelle Erkennungsmerkmal ist ein Data Matrix Code, in dem die individuelle Seriennummer, der Produktcode, die Chargenbezeichnung und das Verfalldatum enthalten sind. Zusätzlich stehen diese Angaben auch in Klarschrift auf der Packung.

1.7: Seit wann sind die Anbindung an das securPharm-System und die Echtheitsprüfung verpflichtend?

Verifizierungspflichtige Arzneimittel, die seit dem 9. Februar 2019 vom Hersteller für den Verkehr freigegeben werden, dürfen nur noch nach erfolgreicher Echtheitsprüfung abgegeben werden. Arzneimittel, die vor dem Stichtag für den Verkehr freigegeben worden sind, dürfen bis Ende ihres Verfalldatums ohne die Sicherheitsmerkmale und entsprechend ohne Echtheitsprüfung abgegeben werden.

1.8: Für welche Arzneimittel gelten die neuen Sicherheitsmaßnahmen?

Grundsätzlich gelten die neuen Vorgaben für alle verschreibungspflichtigen Human-Arzneimittel mit Ausnahme der auf der sogenannten White List (Anhang I zur delegierten Verordnung) aufgeführten Arzneimittel. Die White List ist eine Liste der verschreibungspflichtigen Arzneimittel und Arzneimittelkategorien, die die Sicherheitsmerkmale nicht tragen dürfen. In dieser Liste sind 14 Produktkategorien enthalten, darunter Homöopathika, Allergenextrakte, Kontrastmittel und Lösungen für die parenterale Ernährung. Nicht verschreibungspflichtige Arzneimittel dürfen die Sicherheitsmerkmale nicht tragen. Ausnahmen sind die in der Black List (Anhang II zur delegierten Verordnung) aufgeführten Arzneimittel. Die Black List ist eine Liste der nicht verschreibungspflichtigen Arzneimittel und Arzneimittelkategorien, die die Sicherheitsmerkmale tragen müssen. Enthalten ist bislang nur Omeprazol in zwei verschiedenen Stärken.

1.9: Dürfen OTC freiwillig einen Data Matrix Code tragen?

Laut EU-Kommission ist das Aufbringen eines Data Matrix Codes auf OTC-Packungen zulässig, sofern der Data Matrix Code keine Seriennummer enthält, gleichwohl können Produktcode, Verfalldatum und Chargenbezeichnung maschinenlesbar enthalten sein. Eine freiwillige Teilnahme an der Arzneimittelauthentifizierung ist nicht möglich.

1.10: Dürfen OTC freiwillig einen Erstöffnungsschutz tragen?

Mit Verlautbarung vom 11. April 2017 haben PEI und BfArM (BAnz AT 26.04.2017 B3.) klargestellt, dass OTC-Packungen auf freiwilliger Basis einen Erstöffnungsschutz tragen dürfen.

1.11: Wie funktioniert das securPharm-System zur Verifikation von Arzneimitteln?

Der pharmazeutische Hersteller versieht im Produktionsprozess jede Packung eines verifizierungspflichtigen Arzneimittels mit einer individuellen Seriennummer. Diese Seriennummer wird zusammen mit Produktcode (als PPN oder NTIN ummantelte PZN), Chargenbezeichnung und Verfalldatum im Data Matrix Code (und auch klarschriftlich) auf die Packung aufgebracht. Gleichzeitig werden diese Angaben in das Datenbanksystem der pharmazeutischen Industrie hochgeladen. Zur Echtheitsprüfung einer Packung wird der Data Matrix Code der Packung von der Verifizierenden Stelle gescannt. Dies löst eine Überprüfung von Seriennummer und Produktcode gegenüber der Datenbank der pharmazeutischen Industrie aus. Die Verifikationsanfragen werden dabei anonymisiert über den Apothekenserver weitergeleitet. Der in dieser Datenbank vermerkte Status einer Packung wird der Verifizierenden Stelle zurückgemeldet. Wird die Packung nach positiver Rückmeldung abgegeben, wird der Status auf „abgegeben“ gesetzt. Sollte nun eine zweite Packung mit identischer Serien- und Produktnummer verifiziert werden, fällt auf, dass diese bereits abgegeben wurde.

1.12: Warum gibt es zwei Teilsysteme?

Die deutschen Stakeholder haben sich für ein System entschieden, welches aus verteilten Datenbanken für Apotheken und pharmazeutische Unternehmer besteht. Mit der Ausgestaltung eines Zwei-Server-Modells wird ein besonderer Schutz sensibler Daten gewährleistet, denn Daten für die Prüfprozesse (Verifikation und Statusänderung) werden nur anonymisiert ausgetauscht. Die Teilsysteme werden außerdem von unterschiedlichen Gesellschaften betrieben. Das Datenbanksystem für pharmazeutische Unternehmer wird von ACS PharmaProtect GmbH, einer Gesellschaft der Pharmaverbände, betrieben. An das Datenbanksystem der pharmazeutischen Industrie werden alle pharmazeutischen Unternehmer angeschlossen, deren Produkte der Verifizierungspflicht unterliegen. Der Apothekenserver wird von der Netzgesellschaft Deutscher Apotheker mbH (NGDA) betrieben.

1.13: Warum wird dieses System auch „Ende-zu-Ende-System" genannt?

Der pharmazeutische Unternehmer erzeugt an einem Ende der Lieferkette – beim Verpacken des Medikaments – ein Sicherheitsmerkmal, während am anderen Ende der Kette – vor Abgabe an den Patienten in der Apotheke – dieses Sicherheitsmerkmal verifiziert und die Seriennummer ausgebucht wird.

1.14: Warum wird für dieses System der Data Matrix Code verwendet?

Zweidimensionale Barcodes können viele Daten aufnehmen (z.B. zu Produktcode inkl. PZN noch die Seriennummer, die Chargenbezeichnung und das Verfalldatum) und diese mit sehr geringem Platzbedarf abbilden.

1.15: Tragen Parallelimporte deutsche oder ausländische Codierung?

Parallelimporte tragen im deutschen Markt eine deutsche Codierung. Parallelimporteure müssen das individuelle Erkennungsmerkmal des Produktes, das sie unter eigenem Namen in Verkehr bringen, aus dem System des ursprünglichen Marktes prüfen und ausbuchen. Sie nehmen dann die Position als pharmazeutischer Unternehmer ein und erzeugen ein neues individuelles Erkennungsmerkmal, das sie in das securPharm-System hochladen.

1.16: Wie ist der Umgang mit ausländischen Packungen (Individualimporten)?

Mit ausländischen Packungen ist wie mit deutschen Packungen umzugehen. Der Scan des Data Matrix Codes löst eine Verifizierungsanfrage aus, die über den europäischen Hub an das jeweilige nationale System weitergeleitet wird, in dem die Packungsdaten gespeichert sind. Man bezeichnet den Vorgang auch als IMT (Intermarket Transaktion). Verifizieren Sie beispielsweise ins spanische System hochgeladenen Packungsdaten, wird die Verifizierungsanfrage über den europäischen Hub an das spanische nationale Verifikationssystem weitergeleitet. Individualimporte aus einem europäischen Land, in dem das Medikament nicht verifizierungspflichtig ist, fallen auch in Deutschland nicht unter die Verifizierungspflicht.

1.17: Welche Daten werden bei Benutzung des securPharm-Systems durch die Endnutzer erzeugt?

Bei der Verifikation oder Ausbuchung einer Packung, wird eine Anfrage an das Apothekensystem (AP-System) gesendet. Dabei werden N-ID (also die pseudonymisierte Benutzerkennung/APO-Nummer), der Zeitstempel, die Aktion/ der Vorgang und die im Data Matrix Code enthaltenden Packungsdaten (PC, SN, LOT, EXP) übermittelt. Auf diese Daten hat nur die NGDA Zugriff. Aus dem

APS wird die Anfrage an die Datenbank der pharmazeutischen Industrie (PU-System) weitergeleitet. Die Identität einer Verifizierenden Stelle bleibt dem PU-System jedoch verborgen, denn alle Anfragen werden anonymisiert unter einer speziellen NGDA-Nutzer-ID weitergeleitet. Persönliche Daten werden nicht an das PU-System übermittelt. Die Abfrage dient ausschließlich dem Abgleich zwischen der ausgelesenen Information (Sicherheitsmerkmale der Packung) und der im System hinterlegten Daten für die jeweilige Packung. Durch den Datenaustausch kann die Echtheit des Arzneimittels überprüft werden.

Jede Anfrage an die Datenbanken wird gespeichert. Dies ermöglicht es den zuständigen Aufsichtsbehörden, einen Fälschungsverdachtsfall und die Einhaltung der Delegierten Verordnung zu untersuchen.

1.18: Was ist der europäische Hub?

Der europäische Hub wird benötigt, um grenzüberschreitende Warenströme zu ermöglichen. Er vernetzt die Verifikationssysteme der einzelnen Mitgliedsstaaten miteinander, so dass jede mit den Sicherheitsmerkmalen versehene Arzneimittelpackung in jeder Apotheke in Europa überprüft werden kann. Außerdem laden pharmazeutischen Unternehmen über den europäischen Hub (EU-Hub) die Packungsdaten in das jeweilige nationale System. Betreiber des EU-Hubs ist die EMVO, die European Medicines Verification Organisation. Mehr zur EMVO unter https://emvo-medicines.eu/

1.19: Welche Länder sind an den europäischen Hub angeschlossen?

An den europäischen Hub angeschlossen sind die Systeme zur Echtheitsprüfung der EU-Mitgliedstaaten sowie von Island, Liechtenstein, Norwegen, Nordirland und die Schweiz. Die Systeme von Italien und Griechenland kommen erst 2025 hinzu. Diese haben vom Gesetzgeber eine Übergangsfrist eingeräumt bekommen, weil in diesen Ländern vor Inkrafttreten der Delegierten Verordnung bereits System zur Überprüfung von Arzneimitteln existierten, die an die europäischen Vorgaben angepasst werden müssen.

1.20: Wer ist die EMVO?

Die European Medicines Verification Organisation (EMVO) betreibt den EU-Hub, über den die einzelnen Ländersysteme die Packungsdaten austauschen. Zwischen EMVO und securPharm wurde eine entsprechende Vereinbarung geschlossen, um das securPharm-System mit dem EU Hub zu verbinden und so in das europäische Fälschungsschutzsystem zu integrieren.

1.21: Was ist das EMVS?

Das European Medicines Verification System (EMVS) ist das europaweite Fälschungsschutzsystem. Es besteht aus zwei Komponenten. Eine Komponente bilden die nationalen Organisationen zur Umsetzung der Delegierten Verordnung (NMVOs) mit den entsprechenden nationalen Systemen (NMVS).

Die zweite Komponente des EMVS wird durch den europäischen Hub gebildet. Dieser Hub gewährleistet als Router (Verbindungsstelle) den Austausch der Daten aus den nationalen Datenspeichern und wird außerdem zum Upload von Packungsdaten durch die pharmazeutischen Unternehmer genutzt.

1.22: Wie sollen die Sicherheitsmerkmale die Fälschungssicherheit erhöhen?

Mit dem neuen Fälschungsschutz aus individuellem Erkennungsmerkmal und Erstöffnungsschutz werden Fälschungen leichter erkennbar. Das individuelle Erkennungsmerkmal macht jede Packung zum Unikat, so dass Fälschungen unattraktiver werden und das Entdeckungsrisiko hoch ist.

1.23: Wo erfahre ich, welche Fälschungen durch das securPharm-System aufgedeckt wurden? Existiert eine Liste zu aufgedeckten Fälschungen?

securPharm unterstützt die zuständigen Aufsichtsbehörden bei der Aufklärung von Fälschungsverdachtsfällen, in dem es Berichte aus dem securPharm-System, die sogenannten Prüfpfade einzelner Packungen, zur Verfügung stellt. Über die Ermittlungen der Behörden erhält securPharm in der Regel keine Informationen. Informationen zu Fälschungen sind daher bei den zuständigen Aufsichtsbehörden zu erfragen.

2. Fragen zur Anbindung an das securPharm-System

2.1: Was sind die Voraussetzungen für die Nutzung des securPharm-Systems?

Für die Nutzung des securPharm-Systems wird neben den technischen Voraussetzungen (Hard- und Software, Internetverbindung) ein Zugang zum Apothekenserver des securPharm-Systems in Form eines elektronischen Zertifikats (N-ID) benötigt. Um eine unberechtigte Nutzung des Systems zu verhindern, durchläuft ein Nutzer vor dem Systemzugang einen Legitimationsprozess. Die Legitimation wird in regelmäßigen Abständen überprüft und der Nutzer erneut legitimiert. Dies geschieht für Verifizierende Stelle über das NGDA-Portal.

2.2: Was ist das NGDA Portal?

Das NGDA Portal stellt Zugänge für verschiedene Zielgruppen zur Verfügung. Verantwortliche einer Betriebsstätte können über das NGDA Portal u.a. die Zertifikate einer oder mehrerer Betriebsstätten verwalten. Jede Betriebsstätte erhält im N-Ident-Verfahren eine eigene N-ID. Die Kontaktdaten der jeweiligen Betriebsstätte sollten (u.a. E-Mail-Adresse) stets aktuell gehalten werden. Bei der Registrierung im NGDA Portal werden Benutzername und Passwort festgelegt. Das Portal ist erreichbar unter www.ngda.de.

2.3: Was ist die N-ID?

Die N-ID ist die im Rahmen des N-Ident-Prozesses geprüfte elektronische Identität einer einzelnen Betriebsstätte. Sie dient dem Zugang zu digitalen Diensten und Systemen ohne zusätzliche Registrierung und ist zwingende Voraussetzung zur Teilnahme am securPharm-System. Hinter der N-ID steht ein Zertifikat, welches eine Laufzeit von 24 Monaten hat.

Bei der Registrierung und Legitimation einer Betriebsstätte im NGDA Portal kann ein N-ID Zertifikat erwerben werden. Mit dem Zertifikat erhält ein Nutzer eine Kombination aus Benutzername, die N-ID und Passwort. Wurde das Zertifikat für die einzelne Betriebsstätte erneuert, wird ein neues Passwort für das Zertifikat erteilt, der Benutzername (N-ID) für die Betriebsstätte bleibt jedoch gleich.

2.4: Was lässt sich tun, wenn Schwierigkeiten bei der Anmeldung im NGDA Portal auftreten?

Für den Fall, dass das Passwort vergessen sein sollte, erhält man auf der Seite der NGDA ein neues Passwort. Dazu muss der Benutzername und die hinterlegte E-Mail-Adresse angegeben werden. Hilfestellungen dazu gibt es unter www.ngda.de.

2.5: Was lässt sich tun bei Schwierigkeiten mit der Anmeldung in der securPharm-GUI?

Für die Anmeldung in der securPharm GUI wird die N-ID und das Passwort aus dem ersten PIN-Brief benötigt, welcher per Post zugegangen ist. Bei einer Zertifikatsverlängerung erhalten Nutzer ein neues Passwort, das Passwort aus dem ersten PIN-Brief dient aber weiterhin als Zugang in der GUI.

Für den Fall, dass das Passwort vergessen sein sollte, erhält man auf der Seite der NGDA ein neues Passwort. Dazu muss der Benutzername und die hinterlegte E-Mail-Adresse angegeben werden.

Das Passwort wird an die im NGDA Portal für diese Betriebsstätte hinterlegte E-Mail-Adresse gesandt. Daher ist es wichtig, die im NGDA Portal hinterlegte E-Mail-Adresse aktuell zu halten.

Die securPharm-GUI ist zu erreichen unter: https://securpharm-gui.ngda.de/ .

2.6: Wer trägt die Verantwortung für den Anschluss an das System?

Die Verantwortung für die Umsetzung der gesetzlichen Vorgaben aus Fälschungsschutzrichtlinie und Delegierter Verordnung, zu der auch die Anbindung an securPharm über den Apothekenserver gehört, trägt die Verifizierende Stelle.

2.7: Was kostet der Anschluss an das securPharm-System?

Die Kosten sind bei der NGDA zu erfragen.

2.8: Wie wird eine N-ID erstmalig beantragt?

Das N-Ident-Anmeldeverfahren unterteilt sich in drei Stufen. Zunächst muss ein Account auf https://ngda.de/ angelegt werden. Anschließend muss jede Betriebsstätte, für die eine N-ID benötigt wird, im Account angelegt werden. Zuletzt bedarf es einer Prüfung der Zugangsberechtigung. Dafür müssen die entsprechenden Unterlagen der NGDA zur Prüfung vorgelegt werden, indem die geforderten Dokumente hochgeladen werden. Sind die Dokumente erfolgreich geprüft worden, so kann die N-ID für die Betriebsstätte erworben werden. Nach Zahlungseingang wird das Zertifikat erstellt. Die PIN für den Download wird per Post an die Betriebsstätte geschickt. Anschließend lässt sich das Zertifikat herunterladen und einbinden.

Die NGDA empfiehlt, für den oben beschriebenen Prozess der Legitimation einen Zeitraum von 4 Wochen vor der Eröffnung einer Betriebsstätte einzuplanen.

2.9: Wann muss ich meine Filiale relegitimieren?

Die Relegitimation ist im Zusammenhang mit der Zertifikatserneuerung alle 24 Monate erforderlich, um die weiter bestehende Berechtigung zur Nutzung der digitalen Dienste nachzuweisen. Für weitere Infos, etwa welche Dokumente für die Relegitimation benötigt werden, bitte an die NGDA wenden.

2.10: Habe ich Nachteile, wenn ich bereits vor Ablauf der Zertifikatslaufzeit ein neues Zertifikat bestelle?

Das Zertifikat hat eine Laufzeit von 24 Monaten, welche mit dem ersten Download beginnt. Da der Prozess der Relegitimation und Zertifikatserneuerung etwas Zeit in Anspruch nimmt, empfiehlt die NGDA die Zertifikatserneuerung frühzeitig anzustoßen. Das Zertifikat kann bis zu drei Monate im Voraus angefordert und aktiviert werden (Herunterladen und einbinden), ohne dass der Verifizierenden Stelle Nachteile entstehen.

Erst nach dem ersten Herunterladen wird das Zertifikat auch als aktiv im NGDA Portal angezeigt.

2.11: Woher weiß ich, wann eine N-ID-Zertifikatserneuerung ansteht?

Die NGDA informiert rechtzeitig vor Ablauf der Gültigkeit des Zertifikates per E-Mail, sodass der Bestellprozess frühzeitig angestoßen werden kann. Um eine Erinnerung zu erhalten, müssen die Kontaktdaten im NGDA Portal für die jeweilige Betriebsstätte aktuell gehalten werden.

2.12: Was muss ich beim N-Ident Verfahren beachten, wenn ich mehrere Betriebstätten habe?

Für Inhaber mehrerer Betriebsstätten (z.B. Filialen oder Niederlassungen) ist eine einmalige Anmeldung im NGDA Portal ausreichend. Jede Betriebsstätte muss legitimiert werden und benötigt ein eigenes elektronisches Zertifikat. Achten Sie bitte darauf, die mit der jeweiligen Betriebsstätte verbundenen Kontaktdaten (u.a. E-Mail-Adresse) stets aktuell zu halten.

2.13: Was muss ich beachten, wenn ich meine Betriebsstätte abgebe oder schließe?

Der aktuelle Inhaber kündigt das Zertifikat der Betriebsstätte unter Angabe des Kündigungstermins. Die Kündigung erfolgt über eine E-Mail an kuendigung@ngda.de unter Angabe der Betriebsstättennummer, der vollständigen Anschrift und des Kündigungszeitpunktes. Beachten Sie, dass die E-Mail nach Möglichkeit von der gleichen Adresse gesendet wird wie die E-Mail-Adresse des N-Ident Accountinhabers. Ein Mitarbeitender der NGDA wird nach Eingang der Kündigung diese noch einmal prüfen und dann alle notwendigen Schritte in die Wege leiten.

2.14: Ich habe eine Betriebsstätte übernommen, kann ich auch die N-ID übernehmen?

Das existierende N-ID-Zertifikat kann nicht übernommen werden. Die Registrierung für eine bestehende Betriebsstätte kann auf zwei Arten stattfinden:

» Der neue Inhaber hat noch keine Betriebsstätte bei der NGDA angemeldet.

In diesem Fall ist die Registrierung eines N-Ident Accounts inklusive Anlage der Betriebsstätte notwendig.

» Der neue Inhaber hat bereits eine oder mehrere Betriebsstätten.

In diesem Fall muss innerhalb des NGDA Portals eine neue Betriebsstätte angelegt werden.

2.15: Warum erhalte ich einen PIN-Brief?

Für den Erwerb des N-ID Zertifikates erhält die Verifizierende Stelle einen Brief mit einem Passwort (PIN). Gemeinsam mit der entsprechenden N-ID (z.B. APOxxxxxxx) wird diese PIN zum Herunterladen und Entpacken des Zertifikates benötigt. Erst nach dem ersten Herunterladen wird das Zertifikat auch im NGDA Portal als aktiv angezeigt.

Die Zugangsdaten sollten sicher verwahrt werden, da sie neben der Zertifikatserneuerung u.a. auch für die Weboberfläche des securPharm-Apothekenservers (www.securpharm-gui.ngda.de/) benötigt werden.

2.16: Mein Download hat nicht funktioniert, was muss ich beachten?

Die NGDA hat folgende Hinweise zum Download des N-ID-Zertifikats veröffentlicht:

» Der Download des Zertifikates ist dreimal möglich, Fehlversuche aufgrund einer Falscheingabe der N-ID (APO-Nummer) oder fehlerhafte PIN-Eingabe werden nicht gezählt. Die Schreibweise der N-ID mit Groß- oder Kleinbuchstaben ist unerheblich.

» Zertifikat-Downloads werden nicht gesperrt, wenn ein Teilnehmer dreimal die falsche PIN eingibt.

» Wenn eine PIN unklar ist (Verwechslungsmöglichkeit von „O“ und „0“ bzw. „l“ und „I“), kann die richtige PIN durch Ausprobieren ermittelt werden.

» Der NGDA sind die jeweiligen PINs unbekannt, sie kann daher leider keine Hilfestellung geben.

» Bitte beachten Sie, dass auch eine evtl. vorhandene Sicherheitsinfrastruktur – wie zum Beispiel eine Firewall – den Download verhindern kann.

3. Fragen zu securPharm im Arbeitsalltag

3.1: Woran erkenne ich ein verifizierungspflichtiges Arzneimittel?

Die IFA-Datenbank bzw. der ABDA-Artikelstamm ist um eine entsprechende Information erweitert worden. Das Warenwirtschaftssystem sollte, sofern es auf den ABDA-Artikelstamm zurückgreift, erkennen, ob es sich um ein verifizierungspflichtiges Produkt handelt.

3.2: Wenn alle von mir abgegebenen verifizierungspflichtigen Arzneimittel gescannt werden, erfährt dann die Pharmaindustrie von meinen Verkaufszahlen?

Nein, keinesfalls. securPharm basiert auf dem Prinzip der getrennten Datenbanken für pharmazeutische Unternehmer und Verifizierende Stellen. Der Apothekenserver, mit dem Ihre Software in Verbindung steht, anonymisiert jede Transaktion, so dass niemand erfährt, wo das Arzneimittel abgegeben wurde.

3.3: Ich habe eine Packung ohne Data Matrix Code vor mir. Wie gehe ich damit um?

Scannen Sie den Strichcode („Code 39“). Das Warenwirtschaftssystem wird, sofern es auf die IFA-Daten oder den ABDA-Artikelstamm zurückgreift, mitteilen, ob diese Packung einen Data Matrix Code tragen muss oder ob es sich um eine Bestandsware handelt, die vor dem 9. Februar 2019 in Verkehr gebracht wurde.

3.4: Reicht es, wenn ich statt Data Matrix Code auch den PZN-Strichcode scanne?

Nein, denn im bisherigen PZN Strichcode ist lediglich die PZN in maschinenlesbarer Form codiert. Nur im Data Matrix Code ist neben der PZN auch die Seriennummer der Packung enthalten, mit der die Verifikation/Echtheitsprüfung gegenüber der Datenbank stattfindet. Außerdem wird neben dem Produktcode, die Chargenbezeichnung und das Verfalldatum im Data Matrix Code übermittelt, sodass diese künftig elektronisch im Warenwirtschaftssystem erfasst werden können. Mit der Einführung des Data Matrix Codes besteht außerdem keine Verpflichtung mehr, den Code 39 auf der Packung aufzubringen.

3.5: Welche Merkmale müssen auf der Packung (in Klarschrift) aufgebracht sein?

Neben dem Data Matrix Code muss auf verifizierungspflichtigen Packungen neben den Elementen PZN, Chargenbezeichnung und Verfalldatum zusätzlich der Produktcode und die Seriennummer in Klarschrift aufgebracht sein. Ausgenommen von der Regelung sind besonders kleine Packungen. Nähere Informationen erhalten Sie auf der Website der IFA.

3.6: Was passiert, wenn ich den Strichcode scanne?

Wenn Sie den Strichcode scannen, prüft ihr Warenwirtschaftssystem, sofern es auf den ABDA-Artikelstamm zurückgreift, ob es sich um ein verifizierungspflichtiges Produkt handelt und weist sie in diesem Fall darauf hin, dass Sie den Data Matrix Code scannen müssen.

3.7: Welche Daten sind im Data Matrix Code enthalten?

Der Data Matrix Code enthält den Produktcode, welcher wiederum die PZN enthält, sowie eine packungsindividuelle Seriennummer, Chargenbezeichnung und Verfalldatum.

3.8: Gibt es für die Angaben in Klarschrift eine vorgeschriebene Reihenfolge?

Nein. Pharmazeutische Unternehmer können die Reihenfolge der Datenelemente frei wählen, solange die erforderlichen Datenelemente Produktcode, Seriennummer, Chargennummer und Verfalldatum enthalten sind. Wenn es die Abmessungen der Verpackung zulassen, befinden sich die vom Menschen lesbaren Datenelemente neben dem Data Matrix Code.

3.9: Woran erkenne ich, welchen Data Matrix Code ich für die Echtheitsprüfung scannen muss, wenn mehrere Data Matrix Codes auf der Packung sind?

Wenn mehrere Data Matrix Codes auf einer Packung vorhanden sind, steht neben dem Data Matrix Code für die Echtheitsprüfung die Kennzeichnung PPN.

3.10: In der Hektik passiert es doch mal, dass eine Packung irrtümlich zweimal gescannt/verifiziert wird. Habe ich damit die Abgabefähigkeit zerstört?

Nein. Der Data Matrix Code einer Packung kann beliebig oft durch einen Scan verifiziert werden. Wichtig ist dabei allerdings, dass Sie die Packung nur verifizieren und nicht aus dem System ausbuchen, d.h. das individuelle Erkennungsmerkmal deaktivieren. Sollte Ihnen dieser Fehler jedoch trotzdem unterlaufen, können Sie ihn innerhalb von 10 Tagen beheben. Die Delegierte Verordnung sieht vor, dass Packungen, deren Status auf „abgegeben“ gesetzt wurde und die den Kontrollbereich der Apotheke nicht verlassen haben, innerhalb von 10 Tagen in derselben Betriebsstätte wieder zurückgebucht werden dürfen.

3.11: Dürfen die Packungsdaten in weißer Schrift auf schwarzem Grund (invers) gedruckt sein?

Ja, das Aufbringen des Data Matrix Codes sowie der Klarschriftinformation in weißer Schrift auf schwarzem Grund ist zulässig. Ein geeigneter und richtig eingestellter Scanner ist in der Lage, alle zugelassenen Darstellungsformen zu lesen.

3.12: Eine Packung hat ihr Verfalldatum erreicht. Muss diese bei Vernichtung ausgebucht werden?

Nein, die Packung darf nicht ausgebucht werden, da dies systemseitig automatisch zum Zeitpunkt des Verfalls geschieht. Ansonsten wird ein Alarm generiert. Wird eine verifizierungspflichtige Packung vor Ablauf des Verfalldatums vernichtet, so ist diese auszubuchen.

3.13: Wie ist der Umgang mit codierter Bestandsware, die zu Testzwecken vor dem Pflichtbetrieb hochgeladen wurde?

Bestandsware bezeichnet Ware, die schon vor dem 9. Februar 2019 vom Hersteller für den Verkehr freigegeben worden ist, aber Sicherheitsmerkmale trägt, die zu Testzwecken aufgebracht worden sind. Diese können unter Umständen Fehlalarme im System hervorrufen. Der Anteil an codierter Bestandsware ist bereits deutlich gesunken, sodass das Problem seltener auftreten dürfte. Gemäß delegierter Verordnung ist diese Ware grundsätzlich abgabefähig, sofern keine anderen Gründe dagegen sprechen.

3.14: Darf securPharm e. V. Protokolle mit Packungsdaten aus dem securPharm-System an Verifizierende Stellen geben, z. B. wenn diese wissen wollen, ob sie eine Packung schon überprüft und ausgebucht haben oder nicht?

Nein. Nach Vorgaben aus der Delegierten Verordnung darf securPharm e. V. Protokolle mit Packungsdaten aus dem securPharm-System nur an Behörden herausgegeben.

3.15: Was ist der Unterschied zwischen Verifizierung und Ausbuchung einer Packung?

Die Verifizierung dient der Überprüfung des Packungsstatus, dabei werden die ausgelesenen oder manuell eingegebenen Packungsdaten mit den im System hinterlegten Packungsdaten abgeglichen. Eine Anzeige spiegelt den Status der Packung wider. Eine Packung kann beliebig oft verifiziert werden.

Die Ausbuchung (Abgabe) beschreibt die Statusänderung eines individuellen Erkennungsmerkmals von „abgabefähig" bzw. „aktiv" auf „abgegeben" bzw. „inaktiv". Die Ausbuchung deaktiviert somit das individuelle Erkennungsmerkmal.

3.16: Woher weiß ich, ob mein Scanner geeignet ist und auch richtig funktioniert?

Die NGDA hat einen Scannertest entwickelt, mithilfe dessen die Einstellung aller Scanner geprüft werden sollte. Die Konfiguration der Scanner ist wichtig, da nur so die Daten beim Scannen korrekt ausgelesen und übermittelt werden.

Bei falsch konfigurierten Scannern beobachtet man häufig, dass die Spracheinstellung Alarme auslöst. Oftmals ist beispielsweise eine englische Spracheinstellung voreingestellt, sodass beim Auslesen Y und Z vertauscht wird. Daneben können durch nicht korrekt eingestellte Scanner Fehler bei der Übermittlung von Groß- und Kleinschreibung entstehen. Falsch ausgelesene inverse Codes (weiß auf dunklem Grund) stellen ebenfalls eine häufige Fehlerquelle dar, die durch die Konfiguration des Scanners vermieden werden kann.

Um sicherzustellen, dass die Scanner in Ihrer Betriebsstätte den Data Matrix Code korrekt auslesen können, testen Sie bitte alle Scanner (u.a. Wareneingang und HV). Stellen Sie Auffälligkeiten fest oder haben Sie Fragen zur Konfiguration des Scanners, können die Hersteller oder Lieferanten der Scanner Hilfestellung geben.

Den Scannertest erhalten Sie unter: www.securPharm.de, www.ngda.de oder in der securPharm-GUI.

3.17: Wie lange muss ich warten, bis ich nach einem Scan eine System-Rückmeldung erhalte?

Die Delegierte Verordnung legt fest, dass die Antwortzeit des Systems bei mindestens 95 % der Abfragen unter 300 Millisekunden liegen muss.

Die Leistung des Datenspeichers muss es Verifizierenden Stellen ermöglichen, ihre Tätigkeit ohne wesentliche Zeitverzögerung auszuführen. Die Antwortzeit aus Sicht der Verifizierenden Stelle wird jedoch auch von der Internetverbindung zwischen einer verifizierenden Stelle und dem Apothekensystem sowie der internen Infrastruktur in der verifizierenden Stelle beeinflusst, so dass die Gesamtdauer der Anfrage die 300 Millisekunden überschreiten kann

Dauert eine Rückmeldung unverhältnismäßig lange, kann e die Verfügbarkeit des securPharm-Systems auf www.securpharm-status.de/ überprüft werden.

3.18: Wie wird die 10-Tage Rückbuchungsfrist berechnet?

Die Rückbuchungsfrist beginnt mit dem Zeitpunkt der Ausbuchung und endet exakt nach 10 Kalendertagen zur selben Uhrzeit.

3.19: Welche Aspekte müssen bei einer Rückbuchung beachtet werden?

Eine Rückbuchung muss innerhalb der 10-Tage Rückbuchungsfrist erfolgen und darf auch nur dann durchgeführt werden, wenn die Packung den Kontrollbereich der Verifizierenden Stelle nicht verlassen hat. Ist der Status der Packung einmal auf „gestohlen“ oder „zerstört“ gesetzt, ist eine Rückbuchung nicht mehr möglich. Die NGDA hat keinen Einfluss auf die Rückbuchung und kann die Packung nicht reaktivieren oder den Zeitraum zum Fristablauf verlängern.

3.20: Kann der Status „zerstört“ oder „gestohlen“ wieder rückgängig gemacht werden?

Nein, der Status „zerstört“ oder „gestohlen“ kann nicht zurückgesetzt werden. Die Packung darf nicht mehr in den Verkaufsbestand aufgenommen werden.

3.21: Wie gehe ich mit Rückrufen um?

Deaktivieren Sie die Packung nicht, wenn Sie sie zur Entsorgung an den pharmazeutischen Großhändler oder Unternehmer zurückgeben, es sei denn Sie werden explizit dazu aufgefordert. Setzen Sie den Status einer Packung nur auf „Zerstört“, wenn Sie sie selbst entsorgen.

3.22: Was mache ich bei Packungen, die das Verfalldatum überschritten haben?

Ist das Verfalldatum erreicht, darf vor der Entsorgung keine Ausbuchung erfolgen. Wird die Packung dennoch vor der Entsorgung ausgebucht, entsteht ein Alarm. Eine Verifikation zur Überprüfung des Status ist weiterhin gefahrlos möglich. Das securPharm-System antwortet dann mit dem Hinweis, dass das Verfalldatum überschritten ist und die Packung nicht abgegeben werden darf.

3.23: Was muss ich bei der Entsorgung einer beschädigten Packung beachten?

Wenn die Packung in der Verifizierenden Stelle so beschädigt wurde, dass sie nicht mehr abgegeben werden kann, muss der Code vor der Entsorgung aus dem System ausgebucht werden.

3.24: Wo kann ich nachschauen, ob das securPharm-System erreichbar ist?

Den Betriebsstatus der securPharm-Teilsysteme lässt sich unter www.securpharm-status.de nachvollziehen.

4. Umgang mit Alarmen

4.1: Was ist ein Alarm oder ein Alert?

Ein Alarm oder ein Alert ist eine Warnmeldung. Diese Meldung informiert über eine mögliche Fälschung im System. Je nach Art des Alarmes werden unterschiedliche Akteure innerhalb des securPharm-Systems benachrichtigt. Dabei unterliegen sensible Daten einem besonderen Schutz.

Das Auftreten einer Warnmeldung sagt zunächst nichts über den Verursacher aus. Außerdem steckt nicht hinter jedem Alarm eine Fälschung – auch technische Fehler, unvollständig hochgeladene Packungsdaten, Probleme mit der Codierung, falsch eingestellte Scanner oder eigene Handhabungsfehler (z.B. eine doppelte Ausbuchung einer Packung) können ursächlich sein.

4.2: Wie entsteht ein Alarm in einer Verifizierenden Stelle?

In einer Verifizierenden Stelle kann ein Alarm sowohl beim Verifizieren als auch bei der Statusänderung einer Packung (bspw. Ausbuchen) generiert werden.

Beim Verifikations-Prozess findet ein Daten-Abgleich statt. Die Packungsdaten der Ihnen vorliegenden Packung werden mit den Daten, die im securPharm-System hinterlegt sind, auf Übereinstimmung geprüft. Eine Verifikation kann durch den Scanner oder durch die manuelle Eingabe der Packungsdaten erfolgen. Liest der Scanner die Daten nicht korrekt aus, oder ein Tippfehler schleicht sich ein, kann die Packung nicht im System gefunden werden. Dies löst einen Alarm aus, denn es wird eine verifizierungspflichtige Packung verarbeitet, deren Identität der legalen Lieferkette unbekannt ist.

Bei einer Statusänderung wird der bestehende Packungsstatus geändert, beispielsweise von „abgabefähig“ (aktiv) auf „abgegeben“ (inaktiv). Ist der gewollte Packungsstatus jedoch vor der Änderung bereits gesetzt, führt der Versuch der Änderung zu einem Alarm. In der Praxis zeigt sich dieser Alarm häufig als doppelter Ausbuchungsversuch. Ursächlich kann ein Handhabungsfehler sein, bspw. ein versehentliches Ausbuchen im Wareneingang und dann ein erneutes Ausbuchen bei Abgabe an den Patienten. Aus Systemsicht deutet ein solcher Vorgang auf eine mögliche Fälschung hin, denn es besteht die Gefahr, dass es sich um eine Kopie einer originalen Packung handelt.

4.3: Welche Rolle spielt mein Scanner?

Der Scanner ist ein wichtiges Werkzeug zur Erfassung der Packungsinformationen. Er erleichtert und beschleunigt die Bearbeitung bei der Abgabe von Packungen und verhindert Falscheingaben bei der manuellen Erfassung.

Ist der Scanner jedoch nicht richtig konfiguriert, werden die Packungsdaten falsch ausgelesen und übermittelt. Dies kann zu einem Alarm führen, weil die ausgelesenen Daten nicht mit den im System hinterlegten Daten übereinstimmen. Häufig sieht man dieses Fehlerbild, wenn die Groß- und Kleinschreibung nicht richtig ausgelesen wird oder der Scanner Y und Z vertauscht (Spracheinstellung). Ebenso entstehen in der Praxis häufig Fehler, wenn Trennzeichen überlesen werden oder ein inverser Data Matrix Code (weiß auf dunklem Grund) auf der Packung aufgebracht ist.

Um zu prüfen, ob ein Scanner richtig eingestellt ist, testen Sie bitte jeden Ihrer Scanner. Der Test ist mit dem Scannertest der NGDA möglich. Die aktuelle Version des Scannertests erhalten Sie unter: www.securPharm.de, www.ngda.de oder in der securPharm-GUI.

4.4: Was muss bei einer manuellen Eingabe beachtet werden?

Bei der manuellen Eingabe über die securPharm GUI muss ein genaues Augenmerk auf die exakte Eingabe der Packungsdaten gelegt werden. Insbesondere besteht die Gefahr der Verwechslung bei „O“ und „0“ bzw. „l“ und „I“. Eine falsche Eingabe führt unweigerlich zu einem Alarm, da die abgefragten Daten nicht im System hinterlegt sind.

4.5: Was ist ein doppelter Ausbuchungsversuch?

Wird eine bereits ausgebuchte Packung erneut ausgebucht, wird im securPharm-System ein Alarm ausgelöst. Jede Packung ist über die hinterlegten Daten (Produktcode, Seriennummer, Charge, Verfall) identifizierbar. Wird eine Packung mehrmals ausgebucht, deutet dies auf eine Fälschung hin, denn es gibt nur eine einzige Originalpackung mit dieser Datenkombination im legalen Arzneimittelmarkt.

Unsicherheit unmittelbar vor der Abgabe dahingehend, ob eine Packung schon ausgebucht worden ist oder nicht, kann leicht entstehen. In dem Fall sollte die Packung aber nicht zur Sicherheit noch einmal ausgebucht werden, denn wenn sie bereits ausgebucht war, entsteht ein Alarm. Anstelle dessen sollte der Status der Packung erst überprüft werden (Verifizierung). Bei der Verifizierung einer dem System bekannten Packung wird grundsätzlich kein Alarm ausgelöst. Generell ist zu empfehlen, die Prozesse zu überprüfen und ggfs. Anpassungen vornehmen, um das Auftreten doppelter Ausbuchungsversuche zu vermeiden.

Haben Sie versehentlich die Packung doppelt ausgebucht, können Sie diesen Vorgang unter gewissen Voraussetzungen (u.a. zeitliche Frist) heilen.

4.6: Wer wird über den Alarm informiert?

Bei jedem Verifikationsvorgang und jeder Statusänderung einer Packung findet eine Kommunikation zwischen dem Apothekenserver und der Datenbank der pharmazeutischen Industrie statt. Die Identität der Verifizierenden Stelle bleibt der Datenbank der pharmazeutischen Industrie jedoch verborgen. Dies gilt auch im Fall des Auftretens eines Alarmes. Das Datenbanksystem der pharmazeutischen Industrie und der pharmazeutische Unternehmer, zu dem die alarmauslösende Packung gehört, erhalten daher keine Information darüber, in welcher Stelle der Alarm ausgelöst wurde.

Entsteht ein Alarm, wird der zuständige pharmazeutische Unternehmer informiert. Dort kann der Alarm eingestuft werden. Je nach Bewertung erfolgt eine automatische Weiterleitung des Alarmes durch das securPharm-System an das BfArM zur weiteren Bearbeitung des Alarmes. Das BfArM agiert als Kontakt zur Gesamtheit der Aufsichtsbehörden.

4.7: Welche Informationen werden bei einem Alarm übermittelt?

Der zuständige pharmazeutische Unternehmer erhält neben den Packungsdaten (Seriennummer, Produktcode, Chargennummer, Verfalldatum), die zugeordnete Alarmbezeichnung, ein individuelles Kennzeichen des Alarmvorfalls (Alarm-ID), die Uhrzeit der Alarmentstehung und die dynamisch pseudonymisierte Kennung der Alarm auslösenden Stelle.

Kommt es zu einer automatischen oder manuellen Eskalation durch eine Verifizierende Stelle oder den pharmazeutischen Unternehmer, so werden die Daten beider Datenbanken (PU- und AP-System) in einem Bericht zusammengeführt. Die zuständige Aufsichtsbehörde hat Zugriff auf diesen Bericht, der auch Prüfpfad genannt wird.

Der Prüfpfad enthält alle Informationen zu einer Packung. Das heißt, neben den Packungsdaten, alle Transaktionen (u.a. Verifikationen und Statusänderungen) und Alarminformationen, die zugehörigen Zeitpunkte sowie die entsprechenden de-pseudonymisierten Systemnutzer. Nur die Behörden erhalten die Möglichkeit, die jeweilige Verifizierende Stelle zu identifizieren.

4.8: Wie wird der Alarm in der Software/Warenwirtschaft angezeigt?

Ein Alarm wird immer direkt bei Entstehung in der Software angezeigt, das heißt bei einem fehlerhaften Verifikationsvorgang oder einer nicht gelungenen Statusänderung. Je nach Softwarehaus unterscheidet sich die Darstellung der „roten Ampel“. Oftmals wird ein Warnfenster geöffnet. Auch der Umfang der Informationsanzeige zu dem Alarm unterscheidet sich je nach Softwarehaus.

Historische Alarme können von vielen Softwareherstellern anhand eines automatisch geführten Protokolls in der Software/Warenwirtschaft angezeigt werden. Beachten Sie zudem die securPharm-GUI.

Bei Fragen zur Darstellung und dem Funktionsumfang der Softwareprodukte, wenden Sie sich bitte direkt an Ihren Softwarehersteller.

4.9: Wo erhalte ich weitere Informationen über einen Alarm?

Neben der Darstellung in der Apothekensoftware/Warenwirtschaft besteht die Möglichkeit die graphische Benutzeroberfläche des Apothekenservers (securPharm-GUI der NGDA) zu nutzen. Mit der darin enthaltenen Funktion des „Alarm-Monitorings“ erhält die jeweilige Betriebsstätte Informationen zu von ihr ausgelösten Alarmmeldungen. Über die Warenwirtschaft hinaus bietet die GUI Informationen zum Alarmstatus (Angelegt, De- und Eskaliert), die Alarm-ID, sowie einen Kommentar, den ein pharmazeutischer Unternehmer bei der Einstufung eines Alarms hinterlassen kann. Außerdem können Sie die Alarme nach unterschiedlichen Kriterien filtern. Hilfestellungen zur Benutzung der Benutzeroberfläche erhalten Sie im GUI Hilfsdokument.

Die securPharm-GUI ist unter folgendem Link verfügbar: https://securpharm-gui.ngda.de/

Beachten Sie, dass die angezeigten Fehlercodes in der Warenwirtschaft von denen in der GUI abweichen können. Eine Tabelle der Fehlercodes finden Sie im Hilfsdokument zur GUI.

4.10: Wie ist der Umgang mit Packungen, deren Echtheit nicht erfolgreich überprüft werden konnte oder eine Statusänderung nicht erfolgreich ist?

Grundsätzlich gilt, dass eine Packung, deren Verifizierung negativ ist, nicht abgegeben werden darf und separiert werden muss. Um den Verdacht einer Fälschung zu erhärten oder zu entkräften, muss eine Fehleranalyse durchgeführt werden. Daher ist es unabdingbar, dass sich Verifizierende Stellen aktiv mit den in ihrer Betriebsstätte aufgetretenen Fehlermeldungen auseinandersetzen und den Ursachen auf den Grund gehen. Parallel kann der zuständige pharmazeutische Unternehmer eine Untersuchung anstrengen.

Das Ergebnis der Analyse des pharmazeutischen Unternehmers (Alarmstatus und ggfs. Kommentar) ist über das Alarm Monitoring in der securPharm-GUI (https://securpharm-gui.ngda.de/) anhand des Alarmstatus überprüfbar. Gibt es parallel durch die Analyse in der Verifizierenden Stelle keine guten Gründe für die Annahme, dass ein technischer Fehler oder eigene Handhabungsfehler (z.B. versehentliche Ausbuchung im Wareneingang) ausschlaggebend für den Alarm ist, so ist die Packung weiterhin zu separieren und die behördlichen Meldewege sind einzuhalten.

Wird der Verdacht einer Fälschung durch die Fehleranalyse entkräftet und liegen keinerlei weitere Hinweise auf eine Fälschung vor, so kann die Packung wieder abgabefähig sein. Beachten Sie, dass nur „abgabefähige“ (aktive) Packungen ausgebucht und abgeben werden können. Vergewissern Sie sich also über den Packungsstatus, indem Sie die Packung scannen (verifizieren) und nehmen Sie erst im Anschluss die Packung wieder in den Verkaufsbestand auf.

4.11: Wie läuft die Prüfung eines Alarms beim zuständigen pharmazeutischen Unternehmer ab?

Nach dem Auftreten eines Alarms kann der Alarm innerhalb eines Zeitfensters von sieben Kalendertagen vom zuständigen pharmazeutischen Unternehmer bewertet werden. Stellt dieser innerhalb des Zeitfensters fest, dass es sich um einen Fehlalarm handelt, wird er als solcher eingestuft und damit deeskaliert. Wird kein Grund für einen Fehlalarm festgestellt, muss der Alarm als potenzieller Fälschungsverdachtsfall eingestuft und damit eskaliert werden. Erfolgt innerhalb der Frist keine Bewertung, wird der Alarm ebenfalls automatisch eskaliert.

Beachten Sie, dass der pharmazeutische Unternehmer nur bei selbstverursachten oder ihm sicher bekannten Fehlern (bspw. fehlender Datenupload, falsches Verfalldatum hochgeladen, falsch bedruckte Packung, usw.) eine Deeskalation vornehmen kann. Umso wichtiger ist es, dass Sie in der Verifizierenden Stelle auf Fehlersuche gehen, die Scanner-Einstellung überprüfen und gegebenenfalls die Prozesse anpassen.

Kommt es zu einer Eskalation wird die Alarmmeldung vom securPharm-System an das BfArM weitergeleitet. Das BfArM agiert als Kontakt zur Gesamtheit der Aufsichtsbehörden.

Bitte beachten Sie etwaige Meldepflichten, die unabhängig von der Bewertung durch den pharmazeutischen Unternehmer bestehen.

4.12: Darf eine Packung, die einen Alarm ausgelöst hat, wieder in den Verkaufsbestand genommen werden, bevor die Prüfung durch den zuständigen pharmazeutischen Unternehmer abgeschlossen ist?

Ausschlaggebend für die Wiederaufnahme in den Verkaufsbestand ist der Packungsstatus, der

Erstöffnungsschutz und die Einschätzung der Verifizierenden Stelle.

Gibt es nach erfolgter sorgfältiger Analyse gute Gründe für die Annahme, dass ein technischer Fehler oder eigene Handhabungsfehler (z.B. versehentliche Ausbuchung im Wareneingang) ausschlaggebend für den Alarm waren und keinerlei weitere Hinweise auf eine Fälschung vorliegen, so lässt sich der Verdacht einer Fälschung auch ohne die Prüfung des pharmazeutischen Unternehmers entkräften. Hierbei kann sowohl die manuelle Verifikation, die Transaktionsübersicht in der Software, als auch das Alarm-Monitoring in der securPharm-GUI hilfreich sein. (https://securpharm-gui.ngda.de/).

Neben der Fehleranalyse und der Einschätzung der Verifizierenden Stelle zum Fälschungsverdachtsfall, ist der Packungsstatus im securPharm-System für die Einschätzung der Abgabefähigkeit relevant. Nur Packungen, die den Status „abgabefähig“ innehaben, dürfen in den Verkaufsbestand aufgenommen werden.

4.13: Was ist der Unterschied zwischen Alarmstatus und Packungsstatus?

Der Status des Alarms drückt aus, ob ein Alarm auf einen tatsächlichen Fälschungsverdachtsfall hindeuten könnte, oder ob ein Fehlalarm ausgelöst wurde. Der Status der Packung bestimmt, ob die Packung „abgabefähig“ (aktiv) ist oder nicht, wobei andere Faktoren die Abgabefähigkeit trotz aktivem Status einschränken können. Packungsstatus und Alarmstatus lassen sich über die Software sowie die securPharm-GUI überprüfen.

4.14: Was ist die securPharm-GUI?

Die securPharm-GUI ist die Weboberfläche des securPharm-Apothekenservers der NGDA. GUI steht für Graphical User Interface (graphische Benutzeroberfläche). Über die GUI kann eine Verifizierende Stelle auf die folgenden Funktionen zugreifen:

a) Manuelle Verifikation und Ausbuchung von verifizierungspflichtigen Arzneimitteln

Die Option ermöglicht Ihnen die manuelle Verifikation von verifizierungspflichtigen Arzneimitteln sowie die Möglichkeit den Status der Packung zu ändern. Diese Funktion ist insbesondere bei Störungen in der Warenwirtschaft praktisch.

b) Alarm-Monitoring

Durch das Alarm-Monitoring System erhalten Sie eine Übersicht zu angefallenen Alarmen in Ihrer Betriebsstätte und Informationen zur Bewertung des Alarms. Mithilfe einer Such- und Sortierfunktion lassen sich einzelne Alarme herausfiltern. Diese Informationen können hilfreich sein, um Alarme aufzuklären, Fehlerquellen zu detektieren und zu vermeiden.

Die securPharm-GUI ist unter folgendem Link verfügbar: https://securpharm-gui.ngda.de/

Beachten Sie hierzu auch die GUI Alarm-Monitoring Dokumentation, die sie in der GUI unter dem Reiter: „Hilfe“ erhalten.

4.15: Wo kann ich alle Transaktionen (Verifikationen und Statusänderungen) meiner Betriebsstätte abrufen?

Viele Softwarehäuser bieten die Möglichkeit an, mithilfe ihrer Software die bisherigen Handlungen im Zusammenhang mit der Delegierten Verordnung (Statusüberprüfung und -änderung) nachzuvollziehen. Diese Überprüfung geschieht über ein Protokoll oder Log File. Bei Fragen hierzu kontaktieren Sie bitte Ihren Softwarehersteller.

4.16: Wann wird ein Fälschungsverdachtsfall durch das securPharm-System an die Behörden gemeldet?

Nachdem ein Alarm im System aufgetreten ist, kann dieser Alarm durch den zuständigen pharmazeutischen Unternehmer innerhalb eines Zeitfensters von sieben Kalendertagen bewertet werden. Das Ergebnis ist in der securPharm-GUI im jeweiligen Alarmstatus einsehbar. Stellt der pharmazeutische Unternehmer innerhalb dieses Zeitfensters fest, dass es sich um einen Fehlalarm handelt, wird er als solcher eingestuft und damit deeskaliert. Mit der Deeskalation entfällt die automatische Meldung durch das System. Wird kein Grund für einen Fehlalarm festgestellt, muss der Alarm als potenzieller Fälschungsverdachtsfall eingestuft und damit eskaliert werden. Erfolgt innerhalb der Frist keine Bewertung, wird der Alarm ebenfalls automatisch eskaliert.

Kommt es zu einer Eskalation wird die Alarmmeldung vom securPharm-System an das BfArM weitergeleitet. Das BfArM agiert als Kontakt zur Gesamtheit der Aufsichtsbehörden.

Beachten Sie in diesem Kontext, dass zuständige Aufsichtsbehörden ein Recht auf alle Informationen haben, die zur Prüfung der Einhaltung der Delegierten Verordnung notwendig sind. Entfällt eine Meldung durch die Verifizierende Stelle oder das securPharm-System, so können sich Aufsichtsbehörden dennoch alle Informationen (u.a. Transaktionen und Alarme) zu dieser Packung anzeigen lassen.

4.17: Wann muss ich einen Alarm an die Behörden melden?

Ein Alarm könnte immer auf eine Fälschung hinweisen. Handeln Sie deshalb unverzüglich. Untersuchen Sie die Packung und den Alarm, nutzen Sie dazu alle Ihnen zur Verfügung stehenden Informationen (u.a. Bewertung des Alarmstatus durch den zuständigen Unternehmer, manuelle Eingabe und Scannertest oder die Transaktionshistorie in der Software sofern verfügbar). Zu den Meldefristen und -wegen bitte die jeweilige Gesetzgebung konsultieren.

4.18: Auf welche Informationen hat die Behörde Zugriff?

Zuständige Aufsichtsbehörden haben ein Recht auf alle Informationen, die zur Prüfung der Einhaltung der Delegierten Verordnung notwendig sind. Dazu gehören Informationen zu Alarmen, aber auch die Transaktionshistorie einer Packung, darunter Verifizierungen und Ausbuchungen. Um die Informationen aus dem Datenspeicher zu erhalten, erfolgt durch securPharm eine De-pseudonymisierung der verursachenden Stelle gegenüber der Behörde. Die Identität der Verifizierenden Stelle bleibt gegenüber der Datenbank der pharmazeutischen Industrie weiterhin verborgen.

Bislang erfolgt der Zugriff der Aufsichtsbehörden durch die einzelne Abfrage der sogenannten Prüfpfade und der Alarm-ID über die securPharm Geschäftsstelle.

In Zukunft ist dieser Prozess automatisiert und Behörden haben unmittelbaren Zugang. Potenzielle Verstöße gegen die Fälschungsschutzrichtlinie können dadurch noch leichter und umfassender nachverfolgt werden. Die jeweiligen Verbände der Nutzergruppen werden darüber im Vorfeld informieren.

4.19: Warum sollte man sich mit den securPharm-System und den Alarmen auseinandersetzen?

Neben der Erfüllung der gesetzlichen Vorgaben, trägt jeder einzelne Nutzer dazu bei, das hohe Sicherheitsniveau im legalen Arzneimittelhandel zu wahren.

Damit das Fälschungsschutzsystem funktioniert, müssen auftretenden Alarme registriert und eingeordnet werden. Dabei ist die zentrale Frage, ob der Alarm auf eine Fälschung oder einen Fehlalarm hindeutet.

Gehen Sie also auf Ursachenforschung und machen Sie sich noch vertrauter mit dem securPharm-System: „Was bedeutet der Fehlercode, der beim Scan oder der Statusänderung der Packung erscheint?“; „Wie erkenne ich eine doppelt ausgebuchte Packung“; „Ist der Scanner korrekt eingestellt?“; „Welche Alarme deuten auf einen unvollständigen Datenupload hin?“; „Was ist die securPharm-GUI?“, „Wer hilft mir bei Problemen und Fragen?“

4.20: Meldet das securPharm-System einen Fälschungsverdachtsfall an die Aufsichtsbehörde?

Alarme werden grundsätzlich im securPharm-System gespeichert, sodass sie dort für eine Bearbeitung durch die Behörden bereit stehen. Behörden, die einen von den Marktteilnehmern gemeldeten Fälschungsverdachtsfall mit den Daten aus dem securPharm-System untersuchen möchten, müssen zurzeit noch bei securPharm anfragen, um die entsprechenden Prüfpfade zu erhalten. Nach der geplanten Anbindung der Behörden an das securPharm-System werden diese dann einen direkten Zugriff auf die Daten aus dem System haben.

Es ist außerdem geplant, dass das securPharm-System das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) automatisch informiert, sobald im System ein Alarm eskaliert wurde. Das BfArM koordiniert dann in Absprache mit dem Paul-Ehrlich-Institut (PEI) die Fälle, trägt diese in eine eigene behördliche Fälschungsdatenbank ein und informiert die für den pharmazeutischen Unternehmer zuständige Aufsichtsbehörde.

Die Meldung durch das securPharm-System ist eine zusätzliche Meldung, die nicht die bisherigen Meldepflichten der Marktakteure ersetzt. Es gelten weiterhin die bisherigen Meldepflichten bei einem begründeten Fälschungsverdacht.