Elektronische Gesundheitskarte und Telematikinfrastruktur

Konzept Umschlüsselung für ePA 2.0

Version:	1.0.1
Revision:	
Stand:	06.07.2020
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemKPT_Umschlüsselung_ePA]

Dokumentinformationen

Hinweis zur Verbindlichkeit der Umschlüsselungsvorgaben

Das Konzept für die Umschlüsselung der ePA wird mit Release 4.0.0 als rein informatives Dokument veröffentlicht, das einen Ausblick auf die weitere Umsetzung in Release 4.0.1 gibt, ohne einen Vorgriff auf die Lösung darzustellen.

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	30.06.20		initiale Erstellung des Dokuments	gematik
1.0.1	06.07.20		Hinweis zur Verbindlichkeit der Umschlüsselungsvorgaben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokuments

1.1 Zielsetzung

Dieses Dokument beschreibt das Konzept zum Wechsel der ePA-spezifischen kryptographischen Schlüssel für die elektronische Patientenakte Stufe 2.0. Es gibt in diesem Zusammenhang einen Überblick über die geplanten Abläufe und betroffenen Komponenten.

1.2 Zielgruppe

Dieses Konzept richtet sich an Gesellschafter der gematik, das BSI und BfDI, sowie die Fachöffentlichkeit.

1.3 Geltungsbereich

Wichtiger Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

2 User Stories

Im Konzept sollen die folgenden zwei User Stories umgesetzt werden.

2.1 User Story: Schlüsselwechsel „on demand"

Der Versicherte möchte zu jedem Zeitpunkt die Umschlüsselung seiner elektronischen Patientenakte (ePA) veranlassen können, damit bei Verdacht oder tatsächlicher Kompromittierung von Schlüsselmaterial missbräuchliche Zugriffe verhindert werden (analog einem Passwortwechsel).

Der Versicherte soll den Schlüsselwechsel über sein ePA-Frontend des Versicherten oder über ein KTR-AdV-Terminal veranlassen können.

2.2 User Story: Schlüsselwechsel regelmäßig

Der Versicherte möchte, dass seine elektronische Patientenakte ohne seine explizite Veranlassung regelmäßig (z.B. alle fünf Jahre) oder anlassbezogen umgeschlüsselt wird, damit die Möglichkeiten einer Kompromittierung verringert und die aktuellen kryptographischen Vorgaben eingehalten werden.

2.3 Akzeptanzkriterien und Rahmenbedingungen

Die folgenden Aspekte sind sowohl beim Schlüsselwechsel „on demand" als auch beim regelmäßigen Schlüsselwechsel zu berücksichtigen.

2.3.1 Performance

Die Umschlüsselung muss mit den Endgeräten und Bandbreiten der Nutzer erfolgen können, ohne dass für sie lange Wartezeiten entstehen.

Bei einer elektronischen Patientenakte mit vielen Dokumenten erscheint es i.d.R. nicht praktikabel, zu einem Zeitpunkt alle Dokumente der ePA auf das Endgerät des Nutzers zu laden, dort jedes Dokument umzuschlüsseln und anschließend wieder in der ePA zu speichern. Dieses Vorgehen stellt hohe Ansprüche an Endgeräte (z.B. Smartphones der Versicherten) sowie Bandbreiten. Die dabei zu erwartenden Wartezeiten sind insbesondere nicht praktikabel, wenn der Versicherte dies an einem KTR-AdV-Terminal ausführen sollte.

2.3.2 Datenschutz und Datensicherheit

Die Sicherheit darf durch die Umschlüsselung nicht sinken, damit die ePA weiterhin nur für die vom Versicherten bestimmten Zwecke und nur von den Berechtigten genutzt werden kann.

Die Übertragung von neuen Aktenschlüsseln in die vertrauenswürdige Ausführungsumgebung (VAU) der ePA würde zwar eine performante zentrale Umschlüsselung erlauben, würde jedoch das bisherige Prinzip der ausschließlich dezentralen Verarbeitung der Aktenschlüssel (d.h. Ende-zu-Ende-Verschlüsselung der medizinischen Dokumente) durchbrechen. Der Aktenschlüssel würde beim Betreiber des ePA-Aktensystems verarbeitet werden. Das vorliegende Konzept der Umschlüsselung gewährleistet daher weiterhin die ausschließlich dezentrale Verarbeitung der Aktenschlüssel und die Ende-zu-Ende-Verschlüsselung der medizinischen Dokumente.

2.3.3 Verfügbarkeit

Auch nach der Umschlüsselung möchten der Versicherte und alle Berechtigten auf alle Dokumente der ePA wie zuvor zugreifen können, damit die Dokumente für die medizinische Behandlung des Versicherten weiterhin genutzt werden können.

Die Umschlüsselung darf daher nicht zu inkonsistenten Zuständen der elektronischen Patientenakte führen.

3 Kryptographische Schlüssel der ePA

3.1 Verschlüsselung medizinischer Dokumente

Dieser Abschnitt gibt einen Überblick über die in der ePA genutzten kryptographischen Schlüssel zum Schutz der Daten der Versicherten.

Für die Verschlüsselung medizinischer Dokumente gilt Folgendes (vgl. Abbildung 1: Kryptographische Schlüssel der ePA):

- Jedes medizinische Dokument (MDO) wird mit einem dokumentenindividuellen Dokumentenschlüssel symmetrisch verschlüsselt.
- Jeder Dokumentenschlüssel wird mit dem Aktenschlüssel des Versicherten symmetrisch verschlüsselt. Der Aktenschlüssel wird nur dezentral verarbeitet, d.h., der Aktenschlüssel wird niemals im Klartext im ePA-Aktensystem verarbeitet.
- Der Betreiber eines ePA-Aktensystems verschlüsselt die verschlüsselten medizinischen Dokumente sowie die verschlüsselten Dokumentenschlüssel nochmals mit einem aus dem betreiberspezifischen Schlüssel abgeleiteten aktenspezifischen Schlüssel (vgl. Abschnitt 3.15.3 in [gemSpec_Krypt]). Der betreiberspezifische Schlüssel kann nur über die VAU genutzt werden kann, sodass der Anbieter und der Betreiber keinen Zugriff auf den betreiberspezifischen Schlüssel haben.
- Der Aktenschlüssel wird für jeden berechtigten Nutzer mit den nutzerspezifischen Schlüsseln des Schlüsselgenerierungsdienstes 1 und 2 (SGD1 und SGD2) symmetrisch verschlüsselt. Das dabei entstehende Chiffrat wird in der Komponente Autorisierung hinterlegt.

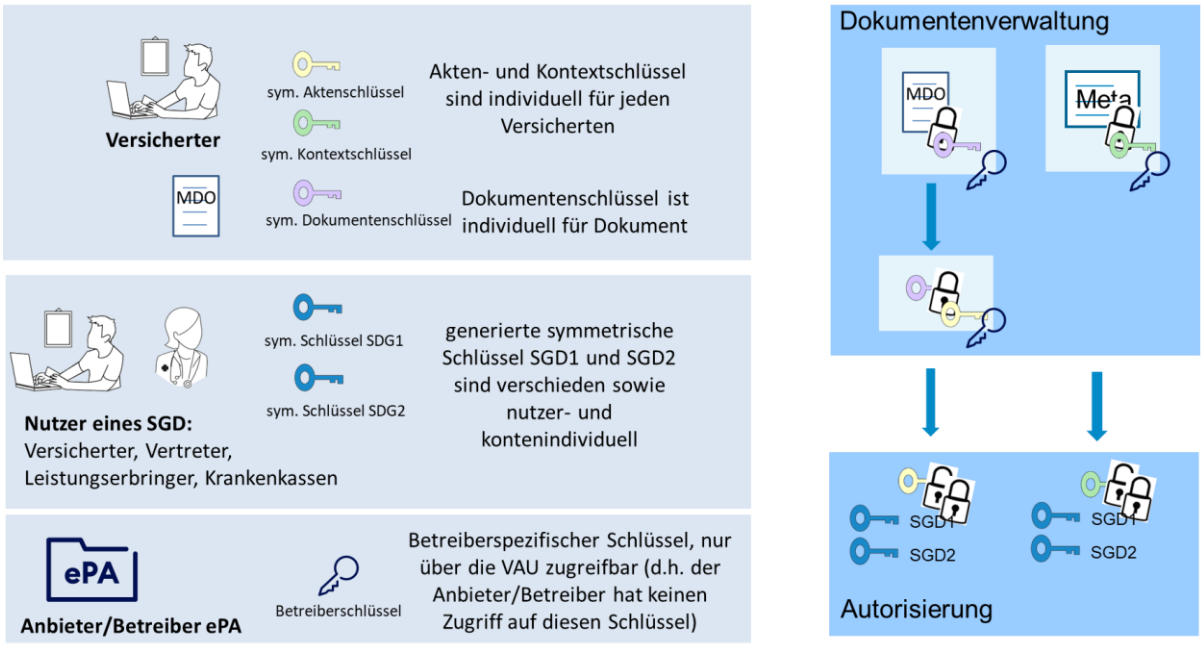

Abbildung 1: Kryptographische Schlüssel der ePA

3.2 Verschlüsselung der Metadaten

Für die Verschlüsselung von Metadaten gilt Folgendes (vgl. Abbildung 1: Kryptographische Schlüssel der ePA):

- Die Metadaten werden mit dem Kontextschlüssel des Versicherten verschlüsselt. Der Kontextschlüssel wird in der VAU im Klartext verarbeitet.
- Der Betreiber des ePA-Aktensystems verschlüsselt die verschlüsselten Metadaten nochmals mit dem aus dem betreiberspezifischen Schlüssel abgeleiteten aktenspezifischen Schlüssel, der nur über die VAU genutzt werden kann. Der Anbieter und der Betreiber haben keinen Zugriff auf den betreiberspezifischen Schlüssel.
- Der Kontextschlüssel wird für jeden berechtigten Nutzer mit den nutzerspezifischen Schlüsseln des Schlüsselgenerierungsdienstes 1 und 2 (SGD1 und SGD2) symmetrisch verschlüsselt. Das entstandene Chiffrat wird in der Komponente Autorisierung hinterlegt.

4 Umschlüsselungskonzept ePA 2.0

Wird die Umschlüsselung ausgelöst – explizit durch den Versicherten oder automatisch durch das Aktensystem – werden

- Akten- und Kontextschlüssel des Versicherten,
- Dokumentenschlüssel sowie
- die SGD1- und SGD2-Schlüssel aller berechtigten Nutzer gewechselt.

Das Konzept zur Umschlüsselung dieser Schlüssel gliedert sich in drei Phasen:

- Phase 1: Neuen Akten- und Kontextschlüssel erzeugen und kryptographische Berechtigungen in der Komponente Autorisierung mit neuen SGD-Schlüsseln aktualisieren.
- Phase 2: Umschlüsselung der Dokumentenschlüssel und der Dokumente.
- Phase 3: Entfernen nicht mehr benötigter Aktenschlüssel aus der Komponente Autorisierung.

Der Wechsel des betreiberspezifischen Schlüssels erfolgt unabhängig davon regelmäßig durch den Betreiber der Akte (siehe Abschnitt 4.4).

4.1 Phase 1

Die Umschlüsselung kann entweder

- explizit durch den Versicherten über sein Frontend des Versicherten (FdV) oder ein KTR-AdV-Terminal (ggf. auch organisatorisch über den Kostenträger) ausgelöst werden oder
- regelmäßig bzw. anlassbezogen auf Hinweis des ePA-Aktensystems, wenn sich der Versicherte über sein FdV, ein KTR-AdV-Terminal oder bei einer Ad-hoc-Berechtigung über den Konnektor am ePA-Aktensystem angemeldet hat.

Die Nutzung des Konnektors (Fachmodul ePA) in Phase 1 beim regelmäßigen/anlassbezogenen Schlüsselwechsel gewährleistet, dass ein Schlüsselwechsel auch für Versicherte erfolgen kann, die kein FdV oder kein KTR-AdV-Terminal nutzen (wollen). Für diese Betroffenengruppe würden die Schlüssel ansonsten nie gewechselt werden. Eine Interaktion mit dem Leistungserbringer ist dabei nicht erforderlich.

Um einen regelmäßigen Schlüsselwechsel durch das Aktensystem initiieren zu können, wird bei Erzeugung eines neuen Akten- und Kontextschlüssels in der Komponente Autorisierung hinterlegt, wann der nächste Schlüsselwechsel zu erfolgen hat. Die konkrete Zeitspanne für den regelmäßigen Schlüsselwechsel ist in den Spezifikationen festzulegen (z.B. fünf Jahre analog zur Gültigkeitsdauer asymmetrischen Schlüsselmaterials). Beim Anmelden des Versicherten prüft das Aktensystem, ob der Zeitpunkt für die Umschlüsselung erreicht wurde und teilt dies dem Client mit. Falls ein Schlüsselwechsel erfolgen soll, startet der Client diesen.

Für einen anlassbezogenen Schlüsselwechsel kann ein regelmäßiger Schlüsselwechsel zeitlich vorgezogen werden. Hierfür vermerkt der Betreiber im Aktensystem, dass beim nächsten Anmelden des Versicherten (am FdV, KTR-AdV-Terminal oder bei einer adhoc-Berech-

tigung in der LE-Umgebung) eine Umschlüsselung erfolgen muss. Der Versicherte ist darauf hinzuweisen, dass er sich an seiner Akte anmelden sollte, um den Schlüsselwechsel zu starten. Der Betreiber darf den Zeitpunkt des Schlüsselwechsels zeitlich vorziehen, jedoch niemals verzögern.

Für Versicherte, die kein FdV oder kein KTR-AdV-Terminal nutzen wollen und somit hierüber keinen Schlüsselwechsel explizit auslösen können, bestünde die Möglichkeit, einen expliziten Schlüsselwechsel über organisatorische Prozesse bei ihrem Kostenträger auslösen zu lassen. Der Kostenträger würde in diesem Falle den Betreiber anweisen, den Wunsch des Versicherten nach einem Schlüsselwechsel im Aktensystem zu vermerken, so dass beim nächsten Anmelden des Versicherten ein Schlüsselwechsel gestartet wird.

Phase 1 des Schlüsselwechsels besteht aus folgenden Schritten (vgl. Abbildung 2 und Abbildung 3).

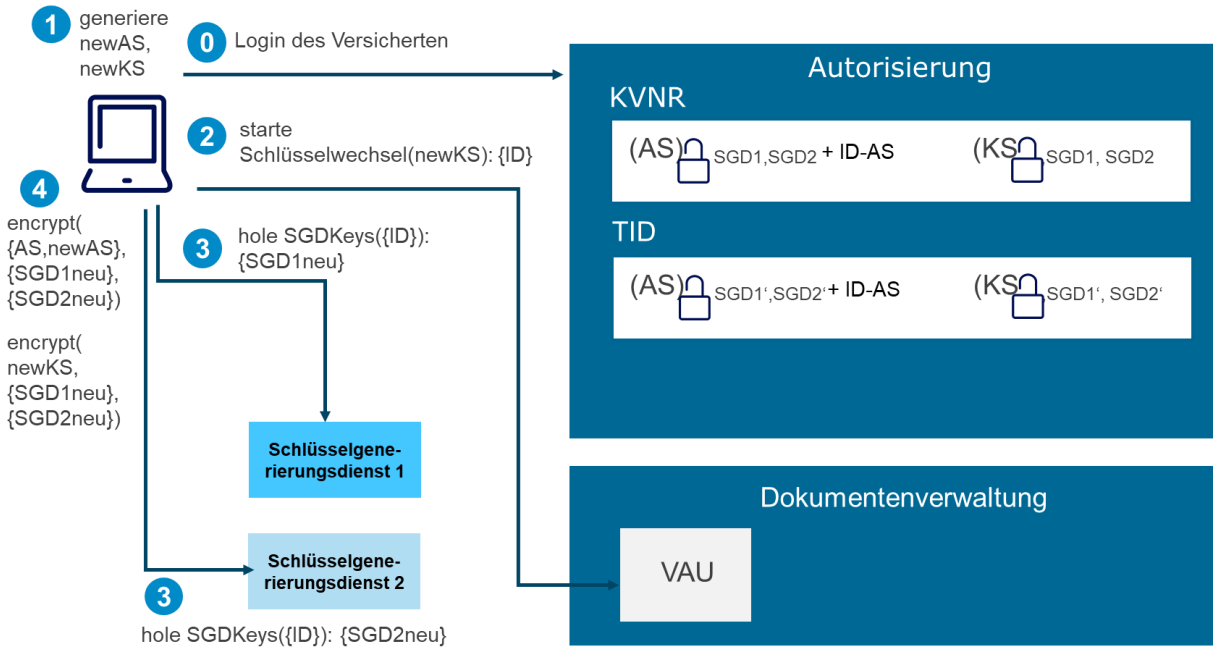

Abbildung 2: Phase 1 (Schritte 1 bis 4)

(0) Voraussetzung für den Schlüsselwechsel ist, dass der Versicherte sich in seiner Akte angemeldet hat. Zudem darf sich die Akte zum Zeitpunkt des Schlüsselwechsels nicht im Prozess des Anbieterwechsels befinden, da für den Transport der Akten-Daten zum neuen Anbieter die Daten mit dem Kontetxtschlüssel gesichert werden. Während des Logins des Versicherten werden alle für den Versicherten in der Komponente Autorisierung gespeicherten verschlüsselten Akten- und Kontextschlüssel an den Client übermittelt. Die Akten- und Kontextschlüssel können vom Client mit Hilfe von SGD1 und SGD2 entschlüsselt werden. Die VAU des Versicherten wird gestartet.
Um einen konsistenten Zustand der Akte sicherzustellen, dürfen in Phase 1 keine weiteren Nutzer an der Akte des Versicherten angemeldet sein. Sollten daher zum Zeitpunkt, zu dem der Versicherte die Umschlüsselung auslöst, weitere Nutzer an der Akte angemeldet sein, wird der Versicherte darüber informiert. Er kann dann entscheiden, ob die angemeldeten Nutzer informiert und von der Akte abgemeldet werden oder ob er die Umschlüsselung verschiebt. Das Anmelden von Nutzern während der Phase 1 wird vom Aktensystem abgelehnt.

(1) Ein neuer Akten- und ein neuer Kontextschlüssel (newAS, newKS) werden auf dem Client generiert. Jeder Aktenschlüssel besitzt eine eindeutige ID, um Aktenschlüssel eindeutig identifizieren zu können. Für den neuen Aktenschlüssel wird daher eine eindeutige ID generiert (ID-newAS).

(2) Der neue Kontextschlüssel (newKS) wird in die laufende VAU des Versicherten übermittelt, um damit beim Schließen der VAU die Metadaten zu verschlüsseln. Der alte Kontextschlüssel wird dann nicht mehr benötigt.
Die Identifier {ID} (=KVNRs und Telematik-IDs (TID)) der auf die Akte berechtigten Nutzer werden dem Client aus der VAU übermittelt. Die berechtigten Nutzer und deren IDs können in der VAU aus der dort verarbeiteten Policy entnommen werden. Die Liste wird dem Client aus der VAU übergeben und nicht aus der Komponente Autorisierung (wo die Information ebenfalls vorhanden ist), damit der Anbieter des ePA-Aktensystems nicht unberechtigt weitere Identitäten hinzufügen kann.

(3) Für jeden berechtigten Nutzer aus Schritt (2) (d.h. jede ID in {ID}) werden vom Versicherten nutzerindividuelle SGD-Schlüssel (SGD1 und SGD2) von den SGDs abgerufen. Die Regeln an den SGDs erlauben die Generierung der benötigten SGD-Schlüssel für alle berechtigten Nutzer im Allgemeinen nur dem Kontoinhaber, jedoch nicht berechtigten Leistungserbringerinstitutionen oder Vertretern. Daher kann Phase 1 nur nach Anmeldung des Versicherten selbst durchgeführt werden. In diesem Schritt wechseln auch die nutzerindividuellen SGD-Schlüssel.

(4) Der Client verschlüsselt für jeden berechtigten Nutzer aus Schritt (2) jeden Aktenschlüssel (die alten Aktenschlüssel aus Schritt (0) und den neuen Aktenschlüssel aus Schritt (1)) sowie den neuen Kontextschlüssel mit den vom SGD1 und SGD2 generierten nutzerindividuellen Schlüsseln aus Schritt (3).

(5) Der Client übermittelt für jeden berechtigten Nutzer aus Schritt (2) die mit den neuen SGD-Schlüsseln verschlüsselten alten Aktenschlüssel sowie den mit den neuen SGD-Schlüsseln verschlüsselten neuen Akten- und Kontextschlüssel an die Komponente Autorisierung (siehe Abbildung 3). Diese ersetzen die dort bisher hinterlegten Akten- und Kontextschlüssel. In der Komponente Autorisierung werden so für jeden Berechtigen Nutzer mehrere Aktenschlüssel gespeichert, die jeweils über ihre ID eindeutig identifizierbar sind. Während die Aktenschlüssel selbst verschlüsselt sind, ist die Aktenschlüssel-ID für den Betreiber lesbar.

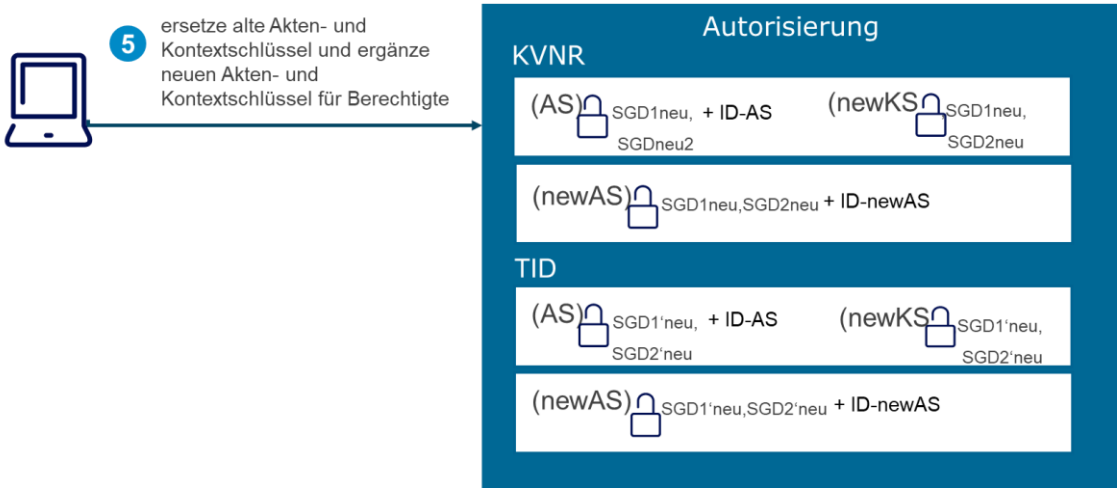

Abbildung 3: Phase 1 (Schritt 5)

Die VAU kann nun geschlossen und nochmals mit dem neuen Kontextschlüssel gestartet werden, um zu überprüfen, dass das Speichern der Metadaten mit dem neuen Kontextschlüssel erfolgreich war. War dies der Fall, kann der alte Kontextschlüssel aus der Komponente Autorisierung endgültig entfernt werden.

Tritt in Phase 1 ein Fehler auf, ist der Zustand des Aktensystems, insbesondere der Komponente Autorisierung, wieder auf den konsistenten Zustand zurückzusetzen, der beim Start von Phase 1 bestand. Hierzu ist der konsistente Zustand nachzuhalten, bis Phase 1 erfolgreich abgeschlossen wurde.

Am Ende von Phase 1 sind die Metadaten mit dem neuen Kontextschlüssel verschlüsselt in der Dokumentenverwaltung gespeichert und Akten- und Kontextschlüssel sowie die SGD-Schlüssel aller Berechtigten sind gewechselt.

In Phase 1 erfolgt noch keine Umschlüsselung von Dokumentenschlüsseln oder Dokumenten. Auch bei kompromittierten Akten- und/oder Kontextschlüsseln sind diese jedoch durch den betreiberspezifischen Schlüssel geschützt, mit dessen Hilfe alle verschlüsselten Dokumentenschlüssel und alle verschlüsselten Dokumente zusätzlich verschlüsselt sind. Da der betreiberspezifische Schlüssel nur über eine VAU zugreifbar ist, ist der Zugriff des Betreibers (oder von sonst irgendjemand, der im Besitz der verschlüsselten Daten und des Akten- bzw. Kontextschlüssels ist) auf die Daten nicht möglich. Der betreiberspezifische Schlüssel ist regelmäßig zu wechseln, um kontinuierlich ein Sicherheitsniveau gemäß den Vorgaben aus [gemSpec_Krypt] aufrechtzuerhalten (siehe Abschnitt 4.4).

4.2 Phase 2

In Phase 2 werden die Dokumentenschlüssel und die Dokumente umgeschlüsselt. Die Umschlüsselung erfolgt zu dem Zeitpunkt, zu dem ein berechtigter Nutzer zugreift, unabhängig davon, um welchen berechtigten Nutzer es sich dabei handelt (der Versicherte, eine berechtigte Leistungserbringerinstitution oder ein Vertreter). Der Nutzer muss lediglich ein Lese- und Schreibrecht besitzen (daher können zum Beispiel berechtigte Kostenträger nicht umschlüsseln, da sie nur in der ePA bereitstellen dürfen).

Bei einem Zugriff auf ein Dokument in Phase 2 werden folgende Schritte ausgeführt (vgl. Abbildung 4 und Abbildung 5):

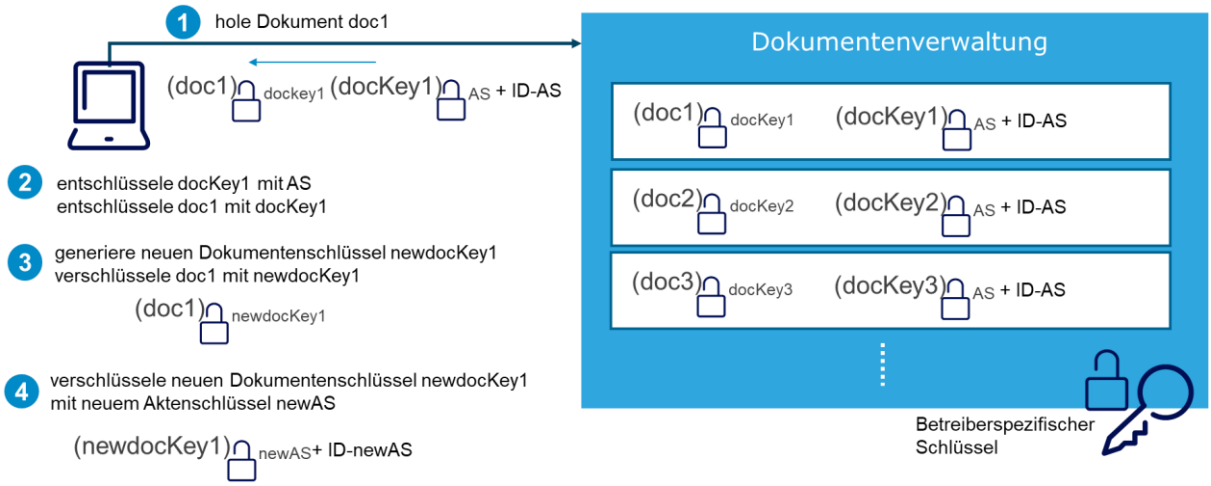

Abbildung 4: Phase 2 (Schritt 1 bis 4)

(1) Der Client fordert ein Dokument vom ePA-Aktensystem an und erhält das mit dem Dokumentenschlüssel verschlüsselte Dokument zusammen mit dem verschlüsselten Dokumentenschlüssel. Jedem verschlüsselten Dokumentenschlüssel ist die ID des verwendeten Aktenschlüssels beigefügt.

(2) Der Client entschlüsselt den Dokumentenschlüssel mit dem angezeigten Aktenschlüssel. Den Aktenschlüssel hat der Client zuvor beim Anmelden an der Akte von der Komponente Autorisierung erhalten. Das Dokument wird mit dem Dokumentenschlüssel entschlüsselt.

(3) Es wird ein neuer Dokumentenschlüssel auf dem Client erzeugt. Das Dokument wird mit dem neuen Dokumentenschlüssel verschlüsselt.

(4) Der neue Dokumentenschlüssel wird mit dem neuen Aktenschlüssel verschlüsselt. Dem Chiffrat wird die ID des genutzten Aktenschlüssels beigefügt.

(5) Das neu verschlüsselte Dokument und der mit dem neuen Aktenschlüssel verschlüsselte neue Dokumentenschlüssel werden im Aktensystem gespeichert und ersetzen die alten Daten (vgl. Abbildung 5).

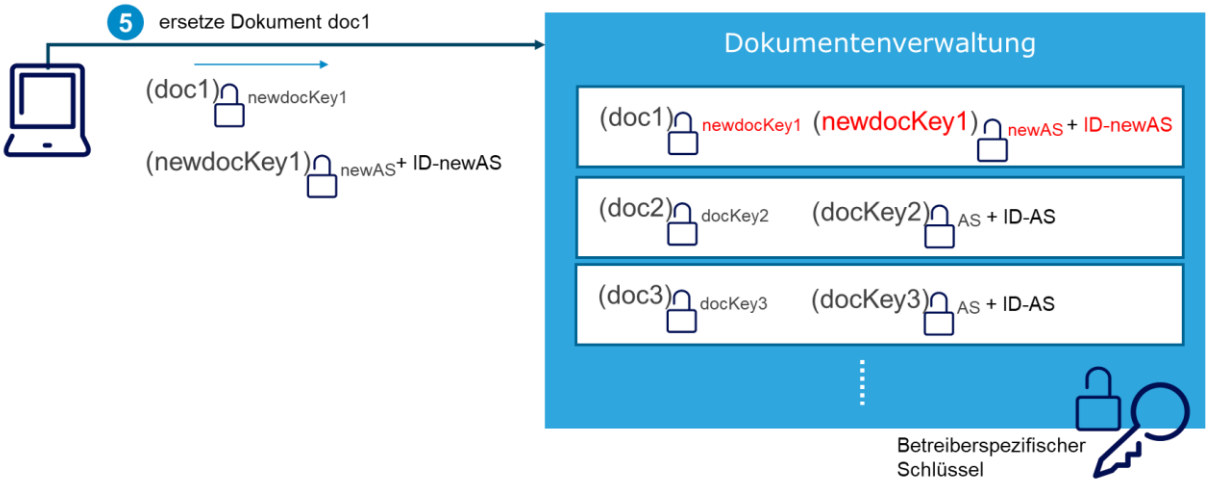

Abbildung 5: Phase 2 (Schritt 5)

Während der gesamten Phase 2 – auch wenn sie sich über einen Zeitraum verteilt – sind die Dokumente des Versicherten mit Hilfe des betreiberspezifischen Schlüssels geschützt,

mit dessen Hilfe alle verschlüsselten Dokumentenschlüssel und alle verschlüsselten Dokumente zusätzlich verschlüsselt werden. Da der betreiberspezifische Schlüssel nur über eine VAU zugreifbar ist, ist der Zugriff des Betreibers (oder von sonst irgendjemand, der im Besitz der verschlüsselten Daten und des Akten- bzw. Kontextschlüssels ist) auf die Daten nicht möglich. Der betreiberspezifische Schlüssel ist regelmäßig zu wechseln, um kontinuierlich ein Sicherheitsniveau gemäß den Vorgaben aus [gemSpec_Krypt] aufrechtzuerhalten (siehe Abschnitt 4.4).

Phase 2 verteilt sich über einen Zeitraum, der durch die Nutzer bestimmt wird. Der Versicherte kann diesen Zeitraum beeinflussen. Falls der Versicherte dies wünscht, kann er zu einem durch ihn bestimmten beliebigen Zeitpunkt auf alle seine Dokumente zugreifen und so alle Dokumente seiner gesamten Akte umschlüsseln. Im FdV bzw. dem KTR-AdV-Terminal soll dem Versicherten angezeigt werden, wie viele seiner Dokumente bzw. welcher Anteil (z.B. 60% der Dokumente der Akte) bereits mit dem aktuellsten Aktenschlüssel verschlüsselt wurden bzw. wie viele noch fehlen. Er kann dann entscheiden, dass er den ganzen Rest auf einmal umschlüsseln lässt. Die Umschlüsselung der gesamten Akte zum Zeitpunkt des Auslösens der Umschlüsselung ist somit ein Spezialfall im Umschlüsselungskonzept.

Während Phase 2 müssen auch alle für die Entschlüsselung der Dokumente notwendigen kryptographischen Verfahren von den Clients unterstützt werden. Alternativ könnte man die Zeitdauer der Phase 2, bis zu der eine Umschlüsselung aller Dokumente erfolgen muss, begrenzen. In diesem Fall müssten alte kryptographische Verfahren ab einem bestimmten Zeitpunkt nicht mehr von den Clients unterstützt werden (d.h., wenn keine Dokumente in den Akten der Versicherten mehr mit diesem Verfahren verschlüsselt sind).

4.3 Phase 3

Sind alle Dokumentenschlüssel und alle Dokumente umgeschlüsselt, kann der Betreiber des ePA-Aktensystems die verschlüsselten alten Aktenschlüssel aus der Komponente Autorisierung entfernen.

Da die ID der genutzten Aktenschlüssel sowohl in der Dokumentenverwaltung an jedem verschlüsselten Dokumentenschlüssel als auch an jedem in der Autorisierung verschlüsselten Aktenschlüssel erkennbar ist, kann der Betreiber entscheiden, welche Aktenschlüssel nicht mehr zur Entschlüsselung benötigt werden.

In Phase 3 muss der Versicherte nicht angemeldet sein. Diese kann vom Betreiber durchgeführt werden.

4.4 Wechsel des betreiberspezifischen Schlüssels

Der Betreiber des ePA-Aktensystems wird verpflichtet, den betreiberspezifischen Schlüssel regelmäßig oder bei Bedarf anlassbezogen zu wechseln, damit die beim Betreiber gespeicherten verschlüsselten Daten immer zusätzlich mit einem sicheren, dem aktuellen Stand der Technik entsprechenden Schlüssel, gesichert sind.

Für den Wechsel des betreiberspezifischen Schlüssels ist keine Aktion des Versicherten notwendig. Die Umschlüsselung kann vom Betreiber durchgeführt werden. Sie muss jedoch innerhalb einer VAU erfolgen, um den Zugriff des Betreibers auf die Daten technisch auszuschließen.

5 Betroffene Produkttypen

Folgende ePA-Produkttypen müssen für das Konzept der Umschlüsselung angepasst werden:

- ePA-Aktensystem (Komponente Autorisierung, Komponente Dokumentenverwaltung),
- ePA-FdV und ePA-FdV AdV im KTR-AdV-Terminal,
- ePA-Fachmodul im Konnektor.

Folgende ePA-Produkttypen müssen für das Konzept der Umschlüsselung nicht angepasst werden:

- ePA-Fachmodul im KTR-Consumer (da sich der Versicherte am KTR nicht anmeldet und Kostenträger ein Schreib-, aber kein Leserecht besitzen),
- Schlüsselgenerierungsdienst,
- Signaturdienst.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AdV	Anwendungen des Versicherten
AS	Aktenschlüssel
ePA	elektronische Patientenakte
FdV	Frontend des Versicherten
KS	Kontextschlüssel
KTR	Kostenträger
KVNR	Krankenversichertennummer
SGD	Schlüsselgenerierungsdienst
TID	Telematik-ID
VAU	Vertrauenswürdige Ausführungsumgebung

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Referenzierte Dokumente

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer entnehmen Sie bitte der aktuellen, auf der Internetseite der gematik veröffentlichten Dokumentenlandkarte, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_Krypt]	gematik: Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur