

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Konzept Umschlüsselung für ePA 2.0

Version: 1.0.0 CC
Revision:
Stand: 30.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: [gemKPT_Umschlüsselung_ePA]

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die Erstversion des Dokumentes.

Dokumentenhistorie

| Version | Stand | Kap./ Seite | Grund der Änderung, besondere Hin- weise | Bearbeitung |
|----------|----------|----------------|---|-------------|
| 1.0.0 CC | 30.04.20 | | zur Abstimmung freigegeben | gematik |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Inhaltsverzeichnis

| | |
|---|-----------|
| Dokumentinformationen | 2 |
| Inhaltsverzeichnis | 3 |
| 1 Einordnung des Dokuments | 4 |
| 1.1 Zielsetzung..... | 4 |
| 1.2 Zielgruppe | 4 |
| 1.3 Geltungsbereich | 4 |
| 2 User Stories | 5 |
| 2.1 User Story: Schlüsselwechsel „on demand“ | 5 |
| 2.2 User Story: Schlüsselwechsel regelmäßig | 5 |
| 2.3 Akzeptanzkriterien und Rahmenbedingungen | 5 |
| 2.3.1 Performance | 5 |
| 2.3.2 Datenschutz und Datensicherheit | 5 |
| 2.3.3 Verfügbarkeit..... | 6 |
| 3 Kryptographische Schlüssel der ePA..... | 7 |
| 3.1 Verschlüsselung medizinischer Dokumente..... | 7 |
| 3.2 Verschlüsselung der Metadaten | 8 |
| 4 Umschlüsselungskonzept ePA 2.0..... | 9 |
| 4.1 Phase 1 | 9 |
| 4.2 Phase 2 | 12 |
| 4.3 Phase 3 | 13 |
| 4.4 Wechsel des betreiberspezifischen Schlüssels | 14 |
| 5 Betroffene Produkttypen | 15 |
| Anhang A – Verzeichnisse..... | 16 |
| A1 – Abkürzungen | 16 |
| A2 – Glossar | 16 |
| A3 – Abbildungsverzeichnis..... | 16 |
| A4 – Referenzierte Dokumente..... | 16 |

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 Anwendungen-des-Versicherten-Terminal beim Kostenträger (KTR-AdV-Terminal) der Krankenkassen 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.

108 Das vorliegende Konzept der Umschlüsselung gewährleistet daher weiterhin die ausschließ-
109 lich dezentrale Verarbeitung der Aktenschlüssel und die Ende-zu-Ende-Verschlüsselung der
110 medizinischen Dokumente.

111 **2.3.3 Verfügbarkeit**

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

115 Die Umschlüsselung darf daher nicht zu inkonsistenten Zuständen der elektronischen Pa-
116 tientenakte führen.

ENTWURF

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 Chiffre wird in der Komponente Autorisierung hinterlegt.

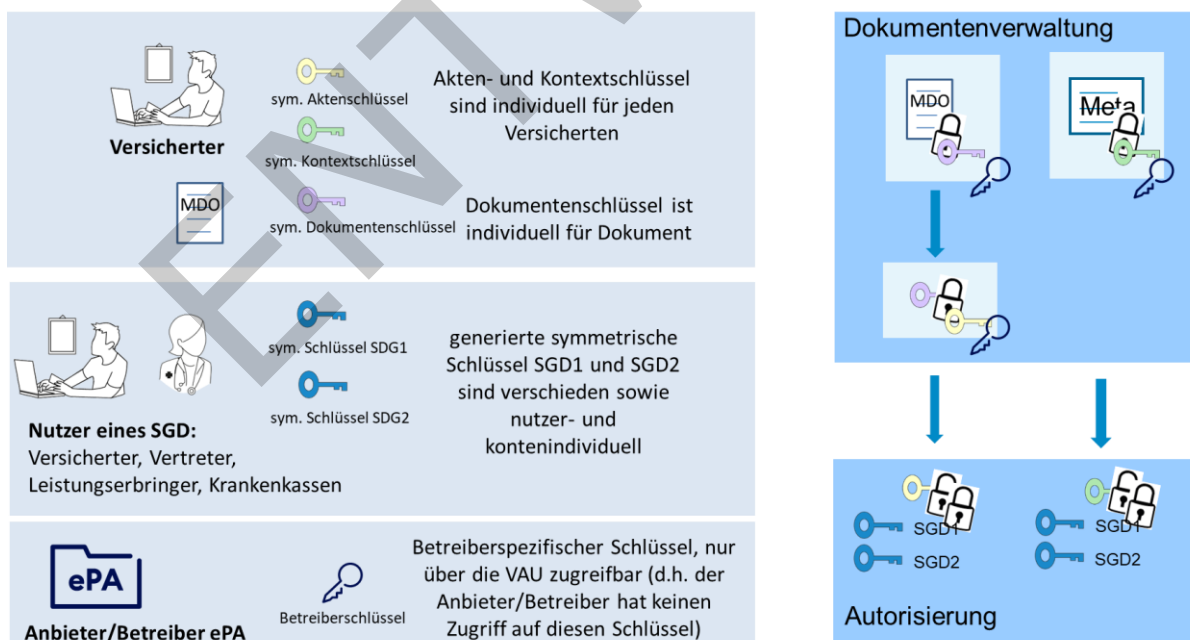


Abbildung 1: Kryptographische Schlüssel der ePA

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 Chiffre 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 Betroffengruppe 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).

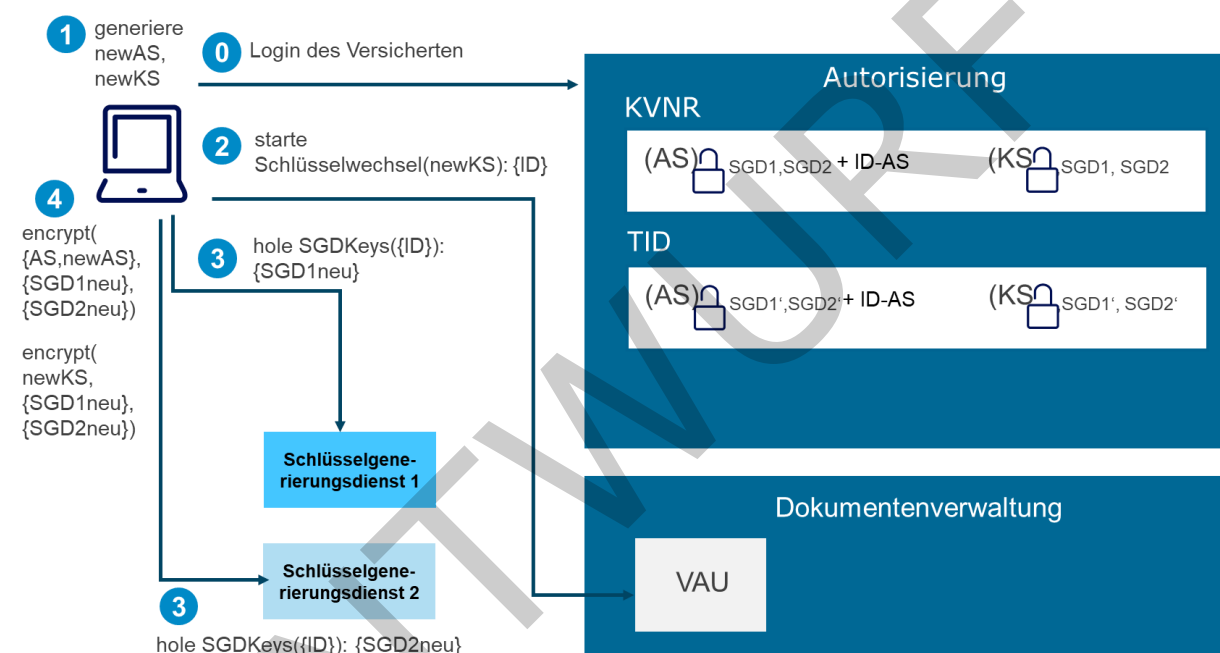


Abbildung 2: Phase 1 (Schritte 1 bis 4)

(0) Voraussetzung für den Schlüsselwechsel ist, dass der Versicherte sich in seiner Akte angemeldet hat. 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, werden diese informiert und von der Akte abgemeldet und 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 Berechtigten 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.

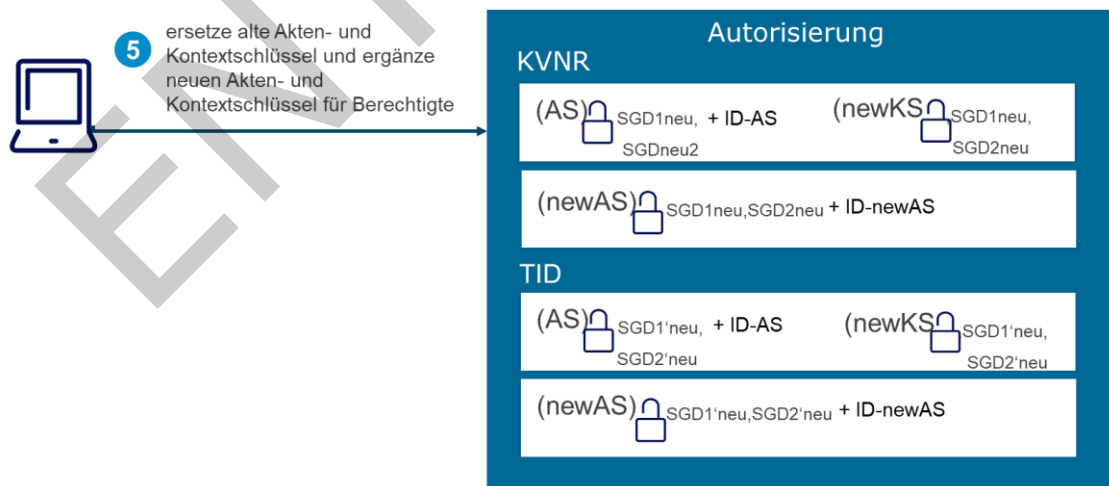


Abbildung 3: Phase 1 (Schritt 5)

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.

260 Tritt in Phase 1 ein Fehler auf, ist der Zustand des Aktensystems, insbesondere der Kom-
 261 ponente Autorisierung, wieder auf den konsistenten Zustand zurückzusetzen, der beim
 262 Start von Phase 1 bestand. Hierzu ist der konsistente Zustand nachzuhalten, bis Phase 1
 263 erfolgreich abgeschlossen wurde.

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

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

276 4.2 Phase 2

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

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

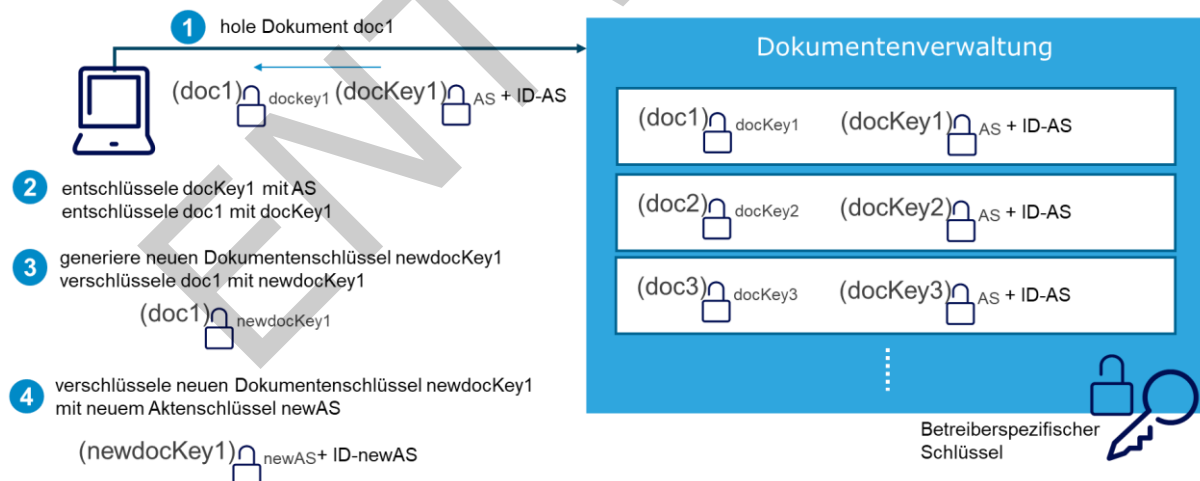


Abbildung 4: Phase 2 (Schritt 1 bis 4)

287 (1) Der Client fordert ein Dokument vom ePA-Aktensystem an und erhält das mit dem
 288 Dokumentenschlüssel verschlüsselte Dokument zusammen mit dem verschlüssel-
 289 ten Dokumentenschlüssel. Jedem verschlüsselten Dokumentenschlüssel ist die ID
 290 des verwendeten Aktenschlüssels beigelegt.

291 (2) Der Client entschlüsselt den Dokumentenschlüssel mit dem angezeigten Akten-
 292 schlüssel. Den Aktenschlüssel hat der Client zuvor beim Anmelden an der Akte von

- 293 der Komponente Autorisierung erhalten. Das Dokument wird mit dem Dokumen-
 294 tenschlüssel entschlüsselt.
- 295 (3) Es wird ein neuer Dokumentenschlüssel auf dem Client erzeugt. Das Dokument wird
 296 mit dem neuen Dokumentenschlüssel verschlüsselt.
- 297 (4) Der neue Dokumentenschlüssel wird mit dem neuen Aktenschlüssel verschlüsselt.
 298 Dem Chifftrat wird die ID des genutzten Aktenschlüssels beigefügt.
- 299 (5) Das neu verschlüsselte Dokument und der mit dem neuen Aktenschlüssel verschlüs-
 300 selte neue Dokumentenschlüssel werden im Aktensystem gespeichert und ersetzen
 301 die alten Daten (vgl. Abbildung 5).

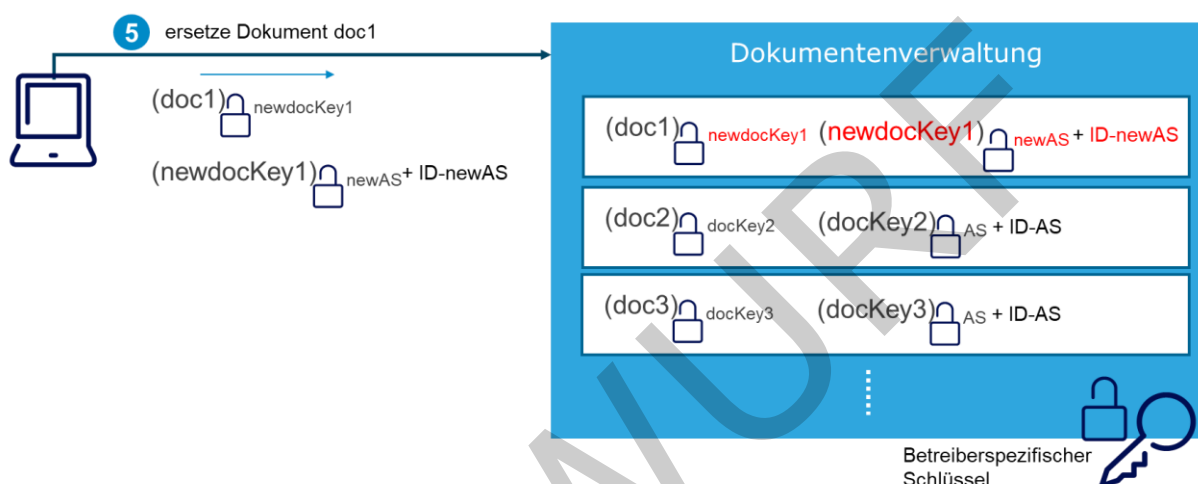


Abbildung 5: Phase 2 (Schritt 5)

304 Während der gesamten Phase 2 – auch wenn sie sich über einen Zeitraum verteilt – sind
 305 die Dokumente des Versicherten mit Hilfe des betreiberspezifischen Schlüssels geschützt,
 306 mit dessen Hilfe alle verschlüsselten Dokumentenschlüssel und alle verschlüsselten Doku-
 307 mente zusätzlich verschlüsselt werden. Da der betreiberspezifische Schlüssel nur über eine
 308 VAU zugreifbar ist, ist der Zugriff des Betreibers (oder von sonst irgendjemand, der im
 309 Besitz der verschlüsselten Daten und des Akten- bzw. Kontextschlüssels ist) auf die Daten
 310 nicht möglich. Der betreiberspezifische Schlüssel ist regelmäßig zu wechseln, um kontinu-
 311 uierlich ein Sicherheitsniveau gemäß den Vorgaben aus [gemSpec_Krypt] aufrechtzuerhal-
 312 ten (siehe Abschnitt 4.4).

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

323 4.3 Phase 3

324 Sind alle Dokumentenschlüssel und alle Dokumente umgeschlüsselt, kann der Betreiber
 325 des ePA-Aktensystems die verschlüsselten alten Aktenschlüssel aus der Komponente Au-
 326 torisierung entfernen.

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

331 In Phase 3 muss der Versicherte nicht angemeldet sein. Diese kann vom Betreiber durch-
332 geführt werden.

333 **4.4 Wechsel des betreiberspezifischen Schlüssels**

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

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

342

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

| | |
|--|----|
| Abbildung 1 - Kryptographische Schlüssel der ePA | 7 |
| Abbildung 2 - Phase 1 (Schritte 1 bis 4) | 10 |
| Abbildung 3 - Phase 1 (Schritt 5)..... | 11 |
| Abbildung 4 - Phase 2 (Schritt 1 bis 4) | 12 |
| Abbildung 5 - Phase 2 (Schritt 5)..... | 13 |

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.

376

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

377

ENTWURF