Zum Gutachten der TU Graz zur Sicherheitsanalyse der Kernkomponenten der elektronische Patientenakte (ePA)

Berlin, Oktober 2020 – Die Telematikinfrastruktur ist eine kritische Infrastruktur und bedeutsam für das Gesundheitswesen in Deutschland. Denn nur ein zuverlässiges, leistungsfähiges digitales System unterstützt die moderne flächendeckende Gesundheitsversorgung.

Gefahren im Cyber-Raum unterliegen einem stetigen Wandel, ebenso wie geeignete Maßnahmen zur präventiven und reaktiven Absicherung. Bei diesem Kopf-an-Kopf-Rennen kann nur effektiv mithalten, wer neben einer ganzheitlichen Betrachtungsweise auch die Sicherheit von Komponenten und Anwendungen fortwährend kritisch prüft und dabei bestehende Lösungen hinterfragt. Dies gelingt nur in einem offenen und transparenten Austausch mit den Fachexperten und der Öffentlichkeit.

Zu diesem Zweck hat die gematik das vorliegende Gutachten der TU Graz zur Sicherheitsanalyse der Kernkomponenten zur elektronischen Patientenakte (ePA) beauftragt.

Die elektronische Patientenakte wird einen wesentlichen Beitrag für eine verbesserte Gesundheitsversorgung leisten. Mit der elektronischen Patientenakte erhalten Versicherte einen transparenten Überblick über ihre Gesundheitsdaten. Dabei entscheidet der Versicherte selbst, welche medizinische Dokumente in seine Patientenakte eingestellt und wer die Daten lesen darf. Damit können künftig Doppeluntersuchungen und Wartezeiten auf zusätzliche Untersuchungstermine vermieden werden. Das spart, mitunter lebenswichtige, Zeit bei der Diagnosestellung oder Therapieentscheidung.

Das Gutachten bescheinigt dem ePA-Aktensystem eine solide Grundstruktur, die einen wirksamen Schutz gegen Bedrohungen bildet. Die Grundstruktur des ePA-Aktensystems ist eine „effektive Festung" bei starken Gefahren, beispielsweise über einen kompromittierten Betreiber eines ePA-Servers, heißt es im Gutachten.

Dabei bildet die gewählte Architektur mit verteilten kryptografischen Vertrauensankern die zentrale Maßnahme zur Absicherung der ePA.

Die Gutachter haben vier Schwachstellen in der Spezifikation identifiziert. Auch wenn diese Schwachstellen, ohne weitere Voraussetzungen, zu keinem praktisch durchführbaren Angriff führen, hat die gematik – zur Aufrechterhaltung der „vielschichtigen Verteidigungsstrategie" – umgehend gehandelt und mit der Version 3.1.3 der Spezifikation entsprechend nachgebessert. Die erfolgreiche Beseitigung ist im Gutachten bestätigt worden.

Das skizzierte Vorgehen zum Gutachten macht deutlich, dass Transparenz herstellen handlungsleitend für die gematik ist. Es zeigt zudem die Qualitätskette zur Sicherheit in der Telematikinfrastruktur mit ihren Komponenten und Anwendungen auf. Denn der Datenschutz und die Informationssicherheit umfassen den gesamten Lebenszyklus der Telematikinfrastruktur und ihrer Produkte – mit der Konzeption, während der Umsetzung und im laufenden Betrieb.

Ein weiteres Beispiel dafür ist das elektronische Rezept (E-Rezept).
Das kommende E-Rezept wird das Erstellen, Einreichen und Verarbeiten von Rezepten sicher und einfacher gestalten. Dazu wird die gematik frühzeitig, neben einem Sicherheitsgutachten, auch den Quellcode offenlegen.

So sorgt die gematik bereits in der Designphase dafür, dass Sicherheitsaspekte umfassend berücksichtigt und dargestellt werden. Im operativen Betrieb steuert und verifiziert sie Komponenten und Anwendungen über das zertifizierte Managementsystem für Informationssicherheit. Dieses wird kontinuierlich weiterentwickelt, um jederzeit dafür Sorge zu tragen, dass die Sicherheitsbestimmungen in der Telematikinfrastruktur eingehalten werden.

Die Telematikinfrastruktur und ihre Anwendungen tragen dazu bei, die Datenschutzrechte und Souveränität des Versicherten zu stärken.

Kontakt: Pressestelle gematik GmbH – Tel. +49 (0) 30 40041-441 – presse@gematik.de

Sicherheitsanalyse zur Sicherheit der kritischen Komponenten der elektronischen Patientenakte nach §291a SGB V

Fokus auf VAU und kryptographische Sicherheitsleistung SGD

Univ.-Prof. Dipl.-Ing. Dr.techn. Wolfgang Slany
gemeinsam mit Mitarbeiterinnen und Mitarbeitern des Instituts

Institut für Softwaretechnologie
Fakultät für Informatik und biomedizinische Technik
Technische Universität Graz

Version: 1.2.0
Stand: 03.03.2020
Status: Abgeschlossen

Inhaltsverzeichnis

1 Management Summary

Es gibt kaum sensiblere Daten als Gesundheitsdaten. Werden diese daher im Rahmen der elektronischen Patientenakte (ePA) elektronisch verarbeitet und gespeichert, ist ein besonderer Schutz erforderlich.

Die gematik trägt dem unter anderem damit Rechnung, indem sie externe Stellen mit Sicherheitsanalysen der ePA beauftragt.

Im Rahmen einer solchen Sicherheitsanalyse wurden im vorliegenden Bericht kritische Komponenten der ePA mit besonderem Fokus auf die VAU und krypotgraphische Sicherheitsleistungen der SGD bewertet.

Insbesondere die kryptographischen Protokolle sind grundsätzlich robust gebaut. Dennoch haben die Gutachter Schwachstellen/Fehler gefunden. Am schwerwiegendsten ist wohl, dass das VAU-Protokoll gegen einen Identity-Misbinding-Angriff anfällig ist.

Nicht alle Fehler führen gleich mit hoher Wahrscheinlichkeit und wenig Aufwand zu einem praxistauglichen, erfolgreichen Angriff. Dennoch empfehlen die Gutachter die Fehler genau zu analysieren und zu beheben. Da sich IT-Sicherheit und damit auch Angriffe auf diese rasch weiter entwickeln, reichen oft schon kleine Details aus, um größere Schäden zu verursachen, wenn aus irgendwelchen Gründen bisher getroffene Annahmen zusammenbrechen und nicht mehr valide sind.

2 Einleitung

Die elektronische Verarbeitung von Gesundheitsdaten ist ein Trend, der in immer mehr Ländern Einzug hält. In Deutschland wird die Einführung der elektronischen Gesundheitskarte (eGK) und deren Anwendungen (Telematikinfrastruktur) durch die gematik koordiniert. Die gematik ist nach §291b SGB V u.a. auch für die Sicherheit der Telematikinfrastruktur verantwortlich.

Dazu hat die gematik eine Studie beauftragt, einen Teilaspekt der Telematikinfrastruktur auf ihre Sicherheitseigenschaften zu untersuchen.

3 Zielsetzung

Die vorliegende Sicherheitsanalyse zur Sicherheit der kritischen Komponenten der elektronischen Patientenakte nach §291a SGB V arbeitet Sicherheitsaspekte mit Fokus auf die VAU (Vertrauenswürdige Ausführungsumgebung) sowie die kryptographische Sicherheitsleistung der SGDs (Schlüsselgenerierungsdienste) heraus. Dabei sind insbesondere die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit der von einem berechtigten Aktenkontonutzer eingestellten Daten zu bewerten.

Ziel ist eine unabhängige Sicherheitsbewertung auf die Eignung der spezifizierten Sicherheitsmaßnahmen, um die gestellten Sicherheitsanforderungen zu erfüllen.

4 Ausgangslage und Aufgabenstellung

Die vorliegende Sicherheitsbewertung soll konkret prüfen, ob getroffene Sicherheitsmaßnahmen in den Spezifikationen für kritische Komponenten der elektronischen Patientenakte nach §291a SGB V mit dem speziellen Fokus auf die VAU (Vertrauenswürdige Ausführungsumgebung) und kryptographische Sicherheitsleistung des SGD (Schlüsselgenerierungsdienst) ausreichen, um ein entsprechendes Sicherheitsniveau gegen ein definiertes Angriffspotenzial zu erzielen.

Es wird dabei keine konkrete Implementierung untersucht, sondern ausschließlich die Spezifikationen.

Aus Sicht der vorliegenden Sicherheitsanalyse sind dabei nachfolgende Rollen potenzielle Angreifer. Dies bedeutet nicht zwangsweise, dass diese einzelnen Rollen auch tatsächlich einen Angriff durchführen. Das kann auch bedeuten, dass ein Angreifer sich Zugriff auf eine der nachfolgenden Rollen verschafft und dann mit den Berechtigungen dieser Rolle weiter angreift.

- **Versicherte:** Der Inhaber des Aktenkontos, ein Versicherter in der gesetzlichen Krankenversicherung.
- **Vertreter:** Ein oder mehrere vom Versicherten berechtigte Personen die im Namen des Versicherten auf die Akte zugreifen können.
- **Leistungserbringer:** Vom Versicherten oder seinem Vertreter für den Zugriff auf die Akte (oder Aktenteile) autorisierte Institutionen oder Personen.
- **Betreiber:** Die Institutionen und deren Mitarbeiter, die den technischen Betrieb des Aktensystems bzw. des Schlüsselgenerierungsdienstes leisten, insb. deren Administratoren.
- **außenstehende Personen:** Alle anderen Personen bzw. Rollen.

Folgende Sicherheitsziele sollen laut Leistungsbeschreibung im Rahmen der Sicherheitsanalyse geprüft werden:

1. Dritte dürfen zu keiner Zeit die Möglichkeit haben auf Daten in einer ePA zuzugreifen.
2. Ein Versicherter (oder sein Vertreter) darf nicht auf die ePA-Inhalte eines anderen Versicherten zugreifen können.
3. Leistungserbringer dürfen nur auf die Akten und Aktenbestandteile zugreifen können, für die sie zuvor berechtigt wurden und die Berechtigungsdauer noch nicht abgelaufen ist.
4. Der Betreiber darf nicht auf medizinische Daten einer Akte zugreifen können. Auch nicht auf die Verarbeitung der „Metadaten“ einer Akte innerhalb der VAU des Aktensystems.
5. Falls ein Angreifer eine serverseitige Schwachstelle im Aktensystem (ausgenommen der VAU) ausnutzen könnte, soll der Angreifer trotzdem keinen Zugriff auf klartextmedizinische Daten erhalten können.
6. Die potentielle Beeinträchtigung der Sicherheit eines Aktenkontos darf die Sicherheit eines anderen Aktenkontos nicht beeinträchtigen.
7. Ein SGD darf nur Schlüsselableitungen für erfolgreich authentisierte Nutzer durchführen. Die abgeleiteten Schlüssel dürfen keinen Dritten zugänglich sein.

4.1 Abgrenzung

Weitere Komponenten, die im Rahmen der elektronischen Patientenakte erforderlich sind, werden in der vorliegenden Sicherheitsanalyse nicht betrachtet. Dies inkludiert auch die Clientkomponenten Konnektor und Frontend des Versicherten. Im Rahmen der vorliegenden Analyse wird jedoch davon ausgegangen, dass alle Clients die Backend-Systeme angreifen könnten, also auch Konnektor bzw. Frontend des Versicherten.

Auch die Verwendung der „alternativen Versichertenidentitäten“ (al.vi) zur Nutzerauthentisierung ist nicht Teil dieser vorliegenden Sicherheitsbetrachtung.

Andererseits wird davon ausgegangen, dass einige weitere Dienste, welche im Rahmen der Telematikinfrastruktur verwendet werden, wie beispielsweise die Public Key Infrastructure (PKI) inklusive der Kartenherausgabe als sicher gilt. Das heißt, die Trust Service Provider der TI erzeugen korrekte Zertifikate und nur berechtigte Personen (eGK) bzw. Institutionsvertreter (SMC-B) erhalten genau die für sie bestimmten Chipkarten und diese Chipkarten sind als sicher anzunehmen.

Kompromittierte FdV (bzw. Fachmodule ePA) werden von den Gutachtern nicht zu den Dritten gezählt (Sicherheitsziel 1), da sie leicht die Rolle eines Versicherten (bzw. LEI)s übernehmen können, und daher besser dem Sicherheitsziel 2 (bzw. Sicherheitsziel 3) untergeordnet werden.

Streng genommen müssten kompromittierte KTRs, kompromittierte Systeme der TI (alle Systeme der TI, die nicht Teil der als sicher angenommenen TI PKI sind), ebenfalls zu den Dritten gezählt werden. Die Gutachter zählen diese jedoch nicht dazu, da die Definition eigener Sicherheitsziele für diese Angreiferrollen weitaus sinnvoller wäre, und eine solche Interpretation die Sinnhaftigkeit der bestehenden Klassifikation in Frage stellen würde.

4.2 Referenzen/Dokumentengrundlagen

Folgende Dokumente dienen als Basis für das erstellte Sicherheitsgutachten:

- **Titel:** Systemspezifisches Konzept ePA
  - **Version:** 1.3.0
  - **Revision:** 166371
  - **Stand:** 02.10.2019
  - **Dateiname:** gemSysL_ePA_V1.3.0.pdf
  - **Referenzierung:** gemSysL_ePA
- **Titel:** Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
  - **Version:** 2.15.0
  - **Revision:** 166406
  - **Stand:** 02.10.2019
  - **Dateiname:** gemSpec_Krypt_V2.15.0.pdf
  - **Referenzierung:** gemSpec_Krypt
- **Titel:** Spezifikation Schlüsselgenerierungsdienst ePA
  - **Version:** 1.2.0
  - **Revision:** 166464

  - **Stand:** 02.10.2019
  - **Dateiname:** gemSpec_SGD_ePA_V1.2.0.pdf
  - **Referenzierung:** gemSpec_SGD_ePA
- **Titel:** Übergreifende Spezifikation Tokenbasierte Authentisierung
  - **Version:** 1.2.0
  - **Revision:** 109264
  - **Stand:** 15.05.2019
  - **Dateiname:** gemSpec_TBAuth_V1.2.0.pdf
  - **Referenzierung:** gemSpec_TBAuth
- **Titel:** Spezifikation Dokumentenverwaltung ePA
  - **Version:** 1.3.0
  - **Revision:** 166393
  - **Stand:** 02.10.2019
  - **Dateiname:** gemSpec_Dokumentenverwaltung_V1.3.0.pdf
  - **Referenzierung:** gemSpec_Dokumentenverwaltung
- **Titel:** Spezifikation Autorisierung ePA
  - **Version:** 1.3.0
  - **Revision:** 167250
  - **Stand:** 02.10.2019
  - **Dateiname:** gemSpec_Autorisierung_V1.3.0.pdf
  - **Referenzierung:** gemSpec_Autorisierung
- **Titel:** Spezifikation Authentisierung des Versicherten ePA
  - **Version:** 1.1.0
  - **Revision:** 109508
  - **Stand:** 15.05.2019
  - **Dateiname:** gemSpec_Authentisierung_Vers_V1.1.0.pdf
  - **Referenzierung:** gemSpec_Authentisierung_Vers
- **Titel:** Spezifikation ePA-Frontend des Versicherten
  - **Version:** 1.3.0
  - **Revision:** 167945
  - **Stand:** 02.10.2019
  - **Dateiname:** gemSpec_Frontend_Vers_V1.3.0.pdf
  - **Referenzierung:** gemSpec_Frontend_Vers
- **Titel:** Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter
  - **Version:** 1.1.0
  - **Revision:** 73176
  - **Stand:** 18.12.2018
  - **Dateiname:** gemSpec_DS_Anbieter_V1.1.0.pdf
  - **Referenzierung:** gemSpec_DS_Anbieter
- **Titel:** Technical Guideline BSI TR-03111: Elliptic Curve Cryptography
  - **Version:** 2.10
  - **Stand:** 01.06.2018
  - **Dateiname:** BSI-TR-03111_V-2-1_pdf.pdf
  - **Referenzierung:** BSI_TR-03111

- **Titel:** Technische Richtlinie TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen
  - **Version:** 2019-01
  - **Stand:** 22.02.2019
  - **Dateiname:** BSI-TR-02102.pdf
  - **Referenzierung:** BSI_TR-02102-1
- **Titel:** Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2: Verwendung von Transport Layer Security (TLS)
  - **Version:** 2019-01
  - **Stand:** 22.02.2019
  - **Dateiname:** BSI-TR-02102-2.pdf
  - **Referenzierung:** BSI_TR-02102-2
- **Titel:** NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
  - **Stand:** November 2007
  - **Dateiname:** nistspecialpublication800-38d.pdf
  - **Referenzierung:** NIST_800-38D

5 Systemüberblick

In diesem Kapitel wird ein kurzer Systemüberblick über das zu begutachtende System gegeben.

5.1 Allgemein

Dieses Kapitel gibt einen groben Überblick über die Gesamtarchitektur des ePA-Systems. Es beschränkt sich vorwiegend auf die hier in dieser Sicherheitsanalyse wichtigsten Systemkomponenten und Kommunikationsrouten.

In Abbildung 1 wird dieser Überblick über die unterschiedlichen Systemkomponenten und deren Zusammenspiel gegeben. Die wichtigsten Komponenten für die nachfolgende Sicherheitsanalyse sind:

- **1) Authentisierungskomponente:** Diese Komponente des ePA-Aktensystems ist für die Authentifizierung eines Versicherten (bzw. dessen Vertreter) zuständig.
- **2) Autorisierungskomponente:** Ein Versicherter (ein Vertreter) welcher eine Authentifizierungsbestätigung der *Authentisierungskomponente* besitzt, muss sich anschließend eine Autorisierungsbestätigung, für die Akte auf die er zugreifen möchte, von der *Autorisierungskomponente* abholen. Diese Komponente ist ebenso Teil des ePA-Aktensystems.
- **3) SGD1 und SGD2:** Hierbei handelt es sich um die beiden Schlüsselgenerierungsdienste. Der SGD1 ist Teil des ePA-Aktensystems, wobei dieser auch an einen anderen Betreiber ausgelagert werden kann. SGD2 hingegen ist unabdingbar ein Teil der zentralen Telematikinfrastruktur (TI) und dadurch immer organisatorisch und betrieblich unabhängig vom jeweiligen ePA-Aktensystem-Betreiber. Die von den Schlüsselgenerierungsdiensten abgeleiteten Schlüssel werden am

Frontend des Versicherten (FdV) dann im “Zwiebelschalenprinzip” zum Ver- und Entschlüsseln der Akten- und Kontextschlüssel verwendet.

- **4) Vertrauenswürdige Ausführungsumgebung (VAU):** Die VAU, welche in Abbildung 1 impliziter Teil der *Dokumentenverwaltung* ist, ermöglicht sowohl das sichere Anlegen und Verwalten von Dokumenten als auch das Durchsuchen der dazugehörigen Metadaten. Aufgrund der Klartextverarbeitung von bereits sehr sensitiven Informationen wie Metadaten, unterliegt diese innerhalb des ePA-Aktensystems besonderen Sicherheitsanforderungen (siehe Abschnitte 6.2, 7.2.1).

Weitere erwähnenswerte Komponenten sind:

- **5) Signaturdienst:** Der in der Abbildung 1 dargestellte Signaturdienst, welcher hier ausschließlich vom FdV verwendet wird, dient der Authentifizierung mittels der *alternativen Versichertenidendität (al.vi)*.
- **6) Zugangsgateway:** “Die Komponente „Zugangsgateway“ ermöglicht dem ePA-Modul Frontend des Versicherten über das Internet die sichere Nutzung des ePA-Aktensystems. Versicherte und Vertreter werden am Zugangsdienst authentifiziert. Außerdem sorgt das Zugangsgateway für die Abwehr gegen Angriffe auf das ePA-Aktensystem und die TI im Allgemeinen. Eine weitere Aufgabe des Zugangsgateways ist die sichere Weiterleitung der Client Requests auf nachgelagerte ePA-Komponenten.” [1, S. 105] Die im Zugangsgateway befindlichen Komponenten sind beispielhaft in Abbildung 2 erkenntlich.
- **7) Frontend des Versicherten (FdV):** “Das ePA-Modul FdV wird in eine Anwendung integriert, welche es Versicherten ermöglicht, ePA-Anwendungsfälle auszuführen. Sie wird als ePA-Frontend des Versicherten (FdV) bezeichnet. Ausführungsumgebung des FdV ist ein Gerät des Versicherten, bspw. ein stationäres Gerät oder ein mobiles Endgerät. Das ePA-Frontend stellt dem Versicherten die Anwendungsfälle über eine grafische Benutzeroberfläche zur Verfügung und bindet die eGK des Versicherten über einen Kartenleser ein.” [1, S. 99] Hierbei wird es sich meistens um ein Smartphone mit installierter App des Kostenträgers handeln. Die beteiligten Komponenten aus Sicht des FdV sind in Abbildung 2 dargestellt.
- **8) Elektronische Gesundheitskarte (eGK):** Bei der eGK handelt es sich um die elektronische Gesundheitskarte, sprich um eine personalisierte Smartcard welche jedem *Versicherten* ausgestellt wird.

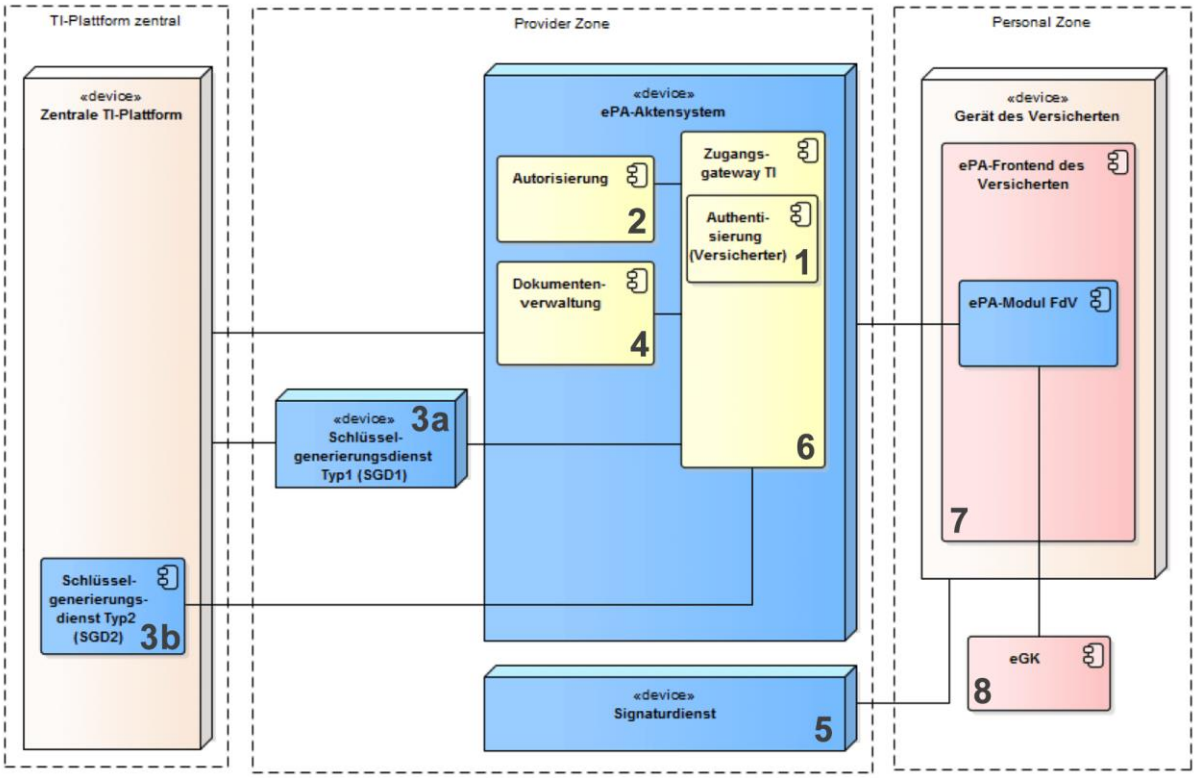


Abbildung 1: Überblick der relevanten Komponenten der ePA Gesamtarchtiktur (vgl. [1, S. 98]).

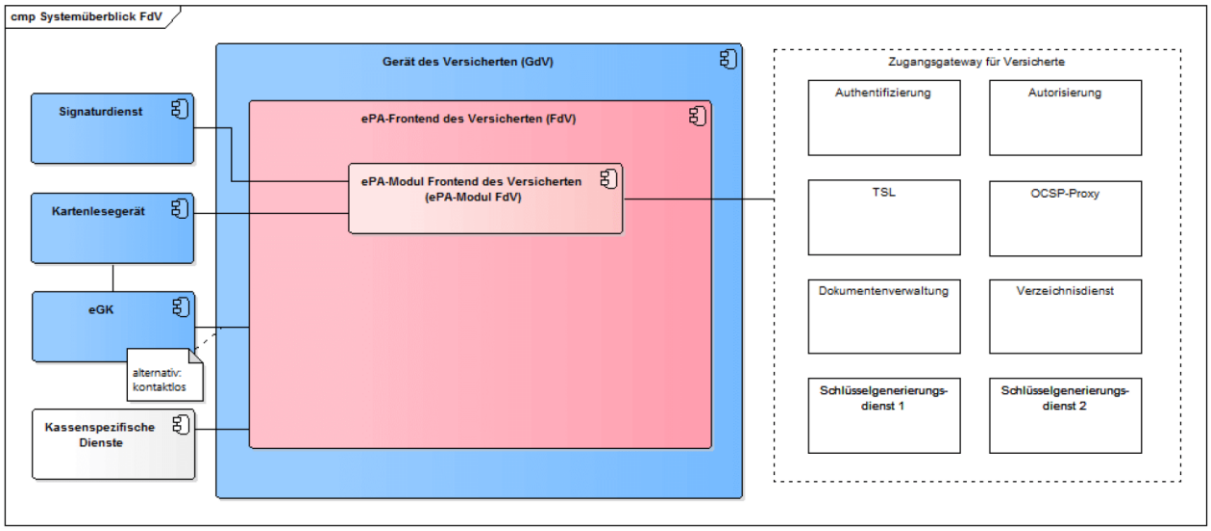


Abbildung 2: Überblick der Komponenten aus Sicht des FdV (vgl. [2, S. 10]).

Das *FdV* kommuniziert über das *Zugangsgateway* mit den einzelnen Komponenten der *Provider Zone* (d. h. den Komponenten des ePA-Aktensystems) bzw. der *zentralen TI-Plattform* (z.B. Verzeichnisdienst und SGD2).

Das *Zugangsgateway* ist der zentrale Knotenpunkt zur Kommunikation zu den einzelnen Subkomponenten innerhalb des ePA-Aktensystems, d. h. jeglicher Zugriff des FdV findet via *Zugangsgateway* statt. Der Zugriff auf gewisse Dienste (z.B. *Autorisierung* oder

Dokumentenverwaltung/VAU) kann eine vorige Authentifizierung bzw. Autorisierung des FdV erfordern.

5.2 SGD

Für den Schlüsselgenerierungsdienst (SGD) werden in den gematik Spezifikationen (primär [gemSpec_SGD_ePA]) eine Reihe von Anforderungen definiert, die den Zugriff von nicht berechtigten Personen auf kryptographische Schlüssel innerhalb des SGD verhindern sollen. Im Konkreten handelt es sich um Schlüssel, mit denen in weiterer Folge der Zugriff auf einzelne Akten und Dokumente möglich ist.

Details zu den Anforderungen sind in späteren Abschnitten verdeutlicht.

5.3 VAU

Für die Vertrauenswürdige Ausführungsumgebung (VAU) werden in den gematik Spezifikationen (primär [gemSpec_Dokumentenverwaltung]) eine Reihe von Anforderungen definiert, die den Zugriff von nicht berechtigten Personen auf Daten einer ePA verhindern sollen. Im Konkreten handelt sich um die Metadaten einer ePA, die während der Verarbeitung innerhalb eines Verarbeitungskontextes im Klartext vorliegen. Unter *Verarbeitungskontext* versteht man eine Instanz einer VAU, in der zeitgleich genau eine ePA-Akte verarbeitet werden darf.

Details zu den Anforderungen sind in späteren Abschnitten verdeutlicht.

6 Sicherheitsanforderungen

In diesem Kapitel finden sich zum Überblick im Rahmen dieser Sicherheitsanalyse betrachtete Sicherheitsanforderungen.

6.1 SGD

In diesem Abschnitt werden jene technischen und organisatorischen Anforderungen an den SGD aus der gematik Spezifikation aufgeführt, welche aus Sicht der Gutachter zusätzlich zur konkreten Definition des kryptographischen SGD-Protokolls in enger Relation zu den definierten Sicherheitszielen (siehe Abschnitt 4) stehen und besonders bzw. speziell fachlich relevant zu dem SGD sind.

Die Liste ist nicht komplett: Eine Reihe weiterer Sicherheitsanforderungen, insbesondere aus [3] (“Basis-IS”, “Basis-ISMS”, “Erweitertes ISMS”, “TI-Sicherheitsbericht” und “„Erweiterter TI-Sicherheitsbericht“), werden an den Betreiber eines SGDs gestellt.

6.1.1 Anforderungen an den SGD

6.1.1.1 Beziehung zwischen ePA-Aktensystem und SGD

- *A_17987* - Anbieter ePA-Aktensystem - Organisatorische, technische und betriebliche Trennung zu SGD2

  Der Schlüsselgenerierungsdienst SGD2 ist ein unärer Dienst und DARF NICHT von einem ePA-Aktensystembetreiber betrieben werden; es muss also eine organisatorische, technische und betriebliche Trennung bestehen.

- *A_17881* - Anbieter SGD - Rollenausschluss für Anbieter des SGD der zentralen TI-Plattform

  Der Anbieter des Schlüsselgenerierungsdienstes der zentralen TI-Plattform MUSS unabhängig von Anbietern von ePA-Aktensystemen sein, d. h. es sind mindestens jeweils eigenständige Rechtspersönlichkeiten mit eigenständigen operativen Geschäfts- und Betriebsführungen und es ist eine strikte Vermeidung von Personenidentitäten bzw. Doppelrollen in den Funktionen Geschäftsführung, leitende Mitarbeiter und Zugangsberechtigte zum Betriebsort des Schlüsselgenerierungsdienstes bzw. ePA-Aktensystems gewährleistet.

- *A_17885* - ePA-Aktensystem-spezifische Ableitungsschlüssel eines SGD-Instanz

  Ein Anbieter eines ePA-Aktensystems MUSS sicherstellen, dass die von ihm verwendete SGD-Instanz (d. h. technisch formuliert “SGD 1”) ePA-Aktensystemanbieter-spezifische Ableitungsschlüssel (Schlüsselableitungsfunktionalität ePA) verwendet.

6.1.1.2 Sichere Betreiberumgebung

- *GS-A_2158-01* - Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen

  Der Anbieter MUSS sicherstellen, dass kryptographische Identitäten bzw. Schlüssel der Produktivumgebung der TI des Anbieters (Umgebungen mit Echtdaten) nicht in Testumgebungen und dass keine kryptographischen Identitäten bzw. Schlüssel aus Testumgebungen in der Produktivumgebung der TI genutzt werden.

- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive

  Der Anbieter einer Schlüsselverwaltung innerhalb der TI MUSS in seinem Sicherheitskonzept notwendige Umstellungsprozesse bei Schwächung von kryptographischen Primitiven beschreiben und die Wirksamkeit der getroffenen Maßnahmen ist nachzuweisen (z.B. durch dokumentierte Notfallübungen, Ablaufprotokolle von abgewickelten Vorfällen).

- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip

  Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Phase seines Lebenszyklus in welcher

Systemkomponente transportiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.

- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip

  Der Anbieter einer Schlüsselverwaltung MUSS in seinem Sicherheitskonzept dokumentieren, welcher Schlüssel in welcher Systemkomponente installiert wird. Es MUSS dabei sichergestellt werden, dass die Schlüssel in Systemkomponenten installiert werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.

- *GS-A_3139* - Krypto_Schlüssel: Dienst Schlüsselableitung

  Der Anbieter einer Schlüsselverwaltung MUSS sicherstellen, dass der Ableitungsprozess unumkehrbar und nicht vorhersehbar ist (die Kompromittierung eines abgeleiteten Schlüssels darf nicht den Ableitungsschlüssel oder andere abgeleitete Schlüssel kompromittieren).

- *GS-A_3141* - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion

  Der Anbieter einer Schlüsselverwaltung MUSS im Falle des Einsatzes einer Schlüsselableitung (nach [ISO11770]) in seinem Sicherheitskonzept Maßnahmen für das Bekanntwerden von Schwächen des kryptographischen Verfahrens, welche die Grundlage der Schlüsselableitung ist, darlegen.

- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip

  Der Anbieter einer Schlüsselverwaltung MUSS, falls er kryptographische Schlüssel archiviert, in seinem spezifischen Sicherheitskonzept beschreiben, welcher Schlüssel in welcher Phase in welcher Systemkomponente archiviert wird. Er MUSS sicherstellen, dass die Schlüssel nur an diejenigen Systemkomponenten verteilt werden, in denen ihr Aufenthalt vorgesehen ist und wo sie hinreichend geschützt sind.

- *GS-A_5557* - Security Monitoring

  Der Anbieter MUSS im Rahmen eines Security Monitoring präventive Maßnahmen zur Erkennung und Analyse von Bedrohungen (z. B. über Korrelation und Auswertung von Log-Daten) durchführen.

- *GS-A_5558* - Aktive Schwachstellenscans

  Der Anbieter MUSS im Rahmen seines Schwachstellenmanagements mindestens monatliche Schwachstellenscans oder vergleichbare Maßnahmen zur Erkennung und Analyse von technischen Schwachstellen („vulnerabilities“) in den vom ihm betriebenen Dienst der TI bzw. RZ-Consumer durchführen.

6.1.1.3 SGD-HSM

- *A_17907* - SGD, Sicherheitsbegutachtung SGD-HSM

Ein SGD ePA MUSS Folgendes sicherstellen:

1. Er MUSS mindestens ein HSM, SGD-HSM genannt, einsetzen.
2. Solch ein SGD-HSM MUSS auf einer Plattform (Hardware und Software) basieren, das zuvor bereits erfolgreich eine Zertifizierung nach FIPS 140-2 [FIPS-140-2] mindestens Level 3 durchlaufen hat.
3. Ein solches SGD-HSM MUSS mit spezieller Firmware ausgestattet sein.
4. Diese Firmware MUSS die Ablauflogik aus [gemSpec_SGD_ePA#4.5-Funktionsablauf Firmware-Modul SGD-HSM] ausführen.
5. Im SGD-HSM MÜSSEN, neben dem speziellen Firmware-Modul, ausschließlich Standard-Firmware-Module verwendet werden (also keine anderen speziellen selbstprogrammierten Firmware-Module).
6. Das Firmware-Modul MUSS eine Sicherheitsbegutachtung durch eine durch die gematik anerkannte unabhängige Instanz (Penetration-Tester etc.) haben. Die gematik nimmt das Gutachten ab und prüft, ob die Anforderung aus dem Produkttypsteckbrief bezogen auf die Schlüsselableitungsfunktionalität ausreichend betrachtet worden sind.
7. Bei der Sicherheitsbegutachtung MUSS sichergestellt sein, dass die unabhängige Instanz aus Punkt 6 mit der gematik Informationen (Frage/Antwort) bezüglich der Sicherheitsbegutachtung austauschen darf.

- *A_17911* - SGD-HSM: Schlüsselerstellung und Veränderung im Mehr-Augen-Prinzip

  Ein SGD ePA MUSS sicherstellen, dass die Schlüssel (S1) bis (S5) aus *A_17910* ausschließlich im Mehr-Augen-Prinzip erstellbar und änderbar sind (bzw. (S4) und (S5) autonom durch das SGD-HSM-Firmware-Modul).

- *A_17912* - SGD-HSM: Root-Schlüssel sind Teil des Firmware-Moduls

  Ein SGD ePA MUSS sicherstellen, dass die Schlüssel (S2) aus *A_17910* Teil des SGD-HSM-Firmware-Moduls sind.

- *A_17913* - SGD-HSM: Exklusive Nutzungsrechte der Schlüssel für das Firmware-Modul

  Ein SGD ePA MUSS technisch sicherstellen, dass

  1. der private Schlüsselbestätigungsschlüssel bei (S1) (vgl. jeweils *A_17910),*
  2. die Ableitungsschlüssel (S3),
  3. die privaten ECIES-Schlüssel (S4), und
  4. die zu den (S4) 1:1-zugeordneten Ableitungsschlüssel (S5) für die Erstellung der Authentisierungstoken ausschließlich durch das SGD-HSM-Firmware-Modul nutzbar sind.

- *A_17915* - SGD: Nicht-Synchronisation der ECIES-Schlüssel (S4) und zugordnete Ableitungsschlüssel (S5)

  Ein SGD ePA DARF die kurzlebigen privaten ECIES -Schlüssel (A_17910 (S4)) und die mit diesen 1:1-zugeordneten Ableitungsschlüssel (A_17910 (S5)) (Erstellung der Authentisierungstoken) NICHT über mehrere SGD-HSM synchronisieren.

- *A_17916* - Verfügbarkeit der Schlüssel in einem SGD-HSM

  Ein SGD ePA MUSS technisch sicherstellen, dass der private Schlüsselbestätigungsschlüssel (A_17910 (S1)) und die geheimen Ableitungsschlüssel

(A_17910 (S3)) in dessen SGD-HSM ausschließlich verschlüsselt und im Mehr-Augen-Prinzip importierbar und exportierbar sind (Ziel: Sicherstellung der Verfügbarkeit dieser Schlüssel). Der SGD ePA MUSS technisch sicherstellen, dass beim Import und Export dieser Schlüssel notwendiger Weise ein Mitarbeiter der gematik beteiligt ist.

- *A_17917* - Schutz des SGD-HSM-Firmware-Moduls

  Ein SGD ePA MUSS durch technische Maßnahmen sicherstellen, dass
  1. das Einbringen und das Update des speziellen Firmware-Moduls in ihrem (oder ihren) SGD-HSM nur im Mehr-Augen-Prinzip möglich ist,
  2. ein Mitarbeiter der gematik an diesem Vorgang beteiligt ist (durch das SGD-HSM durchgesetzt).

6.2 VAU

In diesem Abschnitt werden jene technischen und organisatorischen Anforderungen an die Fachanwendung ePA, bzw. die VAU im Speziellen, aus der gematik Spezifikation aufgeführt, die aus Sicht der Gutachter in enger Relation mit den definierten Sicherheitszielen (siehe Abschnitt 4) stehen, und die kryptographischen Protokolle zur Authentifizierung, Autorisierung sowie den Ende-zu-Ende gesicherten Kanal vom Client in die VAU komplementieren.

6.2.1 Allgemeine Anforderungen an die ePA

6.2.1.1 Datenschutz

- *EPA-EPF-A_0157* - Zusammenführung von Vertragsdaten und Aktendaten verhindern

  Das ePA-Aktensystem MUSS verhindern, dass eine missbräuchliche Profilbildung von Vertragsdaten und Daten der Fachanwendung ePA möglich ist.

- *EPA-EPF-A_0158* - Verbot der Auswertung von Beziehungen zwischen LE, LEI und Versicherten

  Das ePA-Aktensystem MUSS verhindern, dass eine Auswertung von Beziehungen zwischen LE, LEI und Versicherten möglich ist.

- *EPA-EPF-A_0159* - Verbot der Profilbildung

  Das ePA-Aktensystem MUSS verhindern, dass eine missbräuchliche Profilbildung möglich ist.

- *EPA-EPF-A_0161* - Privacy by Default im ePA-Aktensystem

  Das ePA-Aktensystem MUSS sicherstellen, dass bei Konfigurationsmöglichkeiten die datenschutzfreundlichere Option vorausgewählt ist.

- *EPA-EPF-A_0204* - Datenschutzkonformes Logging und Monitoring

Die Dokumentenverwaltung MUSS die für den Betrieb des Fachdienstes erforderlichen Log- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass dem Anbieter keine vertraulichen oder zur Profilbildung geeigneten Daten zur Kenntnis gelangen.

6.2.1.2 Sicherheitsrobustes Systemdesign

- *EPA-EPF-A_0001* - Übergreifende Vorbedingung: Aufrufparameter gültig

  Jeder Produkttyp und jede Komponente der Fachanwendung ePA MÜSSEN bei allen Operationen mit einer qualifizierten Fehlermeldung abbrechen, wenn notwendige Aufrufparameter unvollständig, ungültig oder inkonsistent sind.

- *A_13679* - Sicherheitstechnische Validierung in der Dokumentenverwaltung

  Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS eine Sicherheitsprüfung von allen übergebenen Daten durchführen, bevor die Datenverarbeitung stattfindet.

- *A_15613* - Komponente Authentisierung Versicherter – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachricht

  Die Komponente “Authentisierung Versicherter” MUSS die folgenden Angriffstypen in eingehenden SOAP 1.2-Nachrichten erkennen und mit einem HTTP-Statuscode 400 gemäß [RFC7231] quittieren:
  - XML Injection
  - XPath Query Tampering
  - XML External Entity Injection
- *A_14529* - Komponente Autorisierung - Absicherung gegenüber dem Internet

  Die Komponente Autorisierung MUSS alle Operationsaufrufe der Schnittstellen I_Authorization_Insurant und I_Authorization_Management_Insurant auf Wohlgeformtheit und Zulässigkeit gemäß Protokoll SOAP 1.2 prüfen und bei Schema-, Semantik- oder Protokollverletzungen eine aufgerufene Operation mit dem HTTP-Statuscode 400 gemäß [RFC-7231] abbrechen. Die Prüfung der eingehenden Nachrichten auf Syntax-, Semantik- und Protokollverletzungen soll insbesondere den Angriffstypen XML Injection, XPath Query Tampering und XML External Entity Injection entgegenwirken.

- *EPA-EPF-A_0002* - Übergreifende Vorbedingung: Login nach Notwendigkeit

  Jeder Produkttyp und jede Komponente der Fachanwendung ePA MÜSSEN den Anwendungsfall „Login durch einen Versicherten“, „Login durch einen Leistungserbringer“ oder”Login durch einen Kostenträger" vor der Ausführung einer weiteren fachlichen Operation starten, wenn im Rahmen der internen Session-Verwaltung keine aktuellen Session-Daten vorhanden sind.

- *EPA-EPF-A_0010* - Impliziter Logout nach Inaktivität eines Nutzers

  Das Fachmodul ePA, das ePA-Modul Frontend des Versicherten, die Komponente Zugangsgateway und die Komponente „Dokumentenverwaltung“ MÜSSEN einen

impliziten Logout für ein Aktenkonto nach einem Timeout bei Inaktivität in diesem Aktenkonto starten.

- *EPA-EPF-A_0011* - Expliziter Logout auf Anforderung eines Nutzers

  Das ePA-Modul Frontend des Versicherten MUSS einen expliziten Logout auf Anforderung eines Versicherten starten.

- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem

  Die Komponente „Dokumentenverwaltung“ MUSS für die Verwaltung und den Zugriff der gespeicherten, verschlüsselten Daten ein Berechtigungssystem auf Basis der Authentifzierungs- und Autorisierungsbestätigung authentifizierter Nutzer umsetzen.

- *EPA-EPF-A_0144* - Schutz der Kommunikation

  Alle Produkttypen der Fachanwendung ePA und alle Komponente des ePA-Aktensystems MÜSSEN vertraulich miteinander kommunizieren.

- *EPA-EPF-A_0145* - Informationstechnische Trennung

  Alle Produkttypen der Fachanwendung ePA, die nicht miteinander kommunizieren, MÜSSEN informationstechnisch voneinander getrennt sein

- *EPF-A_0170* - Informationstechnische Trennung der Komponenten des ePA-Aktensystems

  Das ePA-Aktensystem MUSS sicherstellen, dass alle Komponenten des ePA-Aktensystems informationstechnisch voneinander getrennt sind.

- *EPA-EPF-A_0163* - Serverseitige Authentisierung erforderlich

  Das ePA-Aktensystem MUSS sich gegenüber dem ePA-Modul Frontend des Versicherten und dem Fachmodul authentisieren.

- *EPA-EPF-A_0183* - Umsetzung der Dokumentenverwaltung in einer VAU

  Die Komponente Dokumentenverwaltung DARF die Nutzdaten eines Aktenkontos NICHT außerhalb einer VAU verarbeiten.

- *EPA-EPF-A_0184* - Verschlüsselung der Nutzdaten eines Aktenkontos außerhalb der VAU

  Die Komponente Dokumentenverwaltung MUSS sicherstellen, dass alle Nutzdaten eines Aktenkontos außerhalb der VAU nur in verschlüsselter Form vorliegen.

- *EPA-EPF-A_0188* - Sichere Session-Verwaltung

  Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS eine sichere Session-Verwaltung umsetzen.

6.2.1.3 Authentifizierung/Autorisierung

- *EPA-EPF-A_0175* - Integritätsschutz für Bestätigungen

Das ePA-Aktensystem MUSS sicherstellen, dass die Authentifizierungsbestätigung und Autorisierungsbestätigung integritätsgeschützt sind und eine begrenzte Gültigkeitsdauer haben

- *EPA-EPF-A_0176* - Akzeptanz nur von eigenen Autorisierungsbestätigungen

  Das ePA-Aktensystem MUSS sicherstellen, dass nur die vom ePA-Aktensystem selbst ausgestellten Autorisierungsbestätigungen akzeptiert werden.

- *EPA-EPF-A_0169* - Zusätzliche Autorisierung von sensiblen Anwendungsfällen

  Das ePA-Aktensystem MUSS sicherstellen, dass für folgende Anwendungsfälle eine nochmalige Authentifizierung erfolgt, wenn die Authentifizierung zulange zurück liegt.

  – Vertretung einrichten

  – Vertragsdaten ändern

  – Aktenkonto schließen

- *A_14227* - Komponente Authentisierung Versicherter - TLS-Authentisierung innerhalb der TI

  Die Komponente “Authentisierung Versicherter” MUSS für alle innerhalb der TI zur Verfügung gestellten Schnittstellen ausschließlich Verbindungen mit TLS akzeptieren und dabei die einseitige Serverauthentisierung unter Nutzung des X.509-Komponentenzertifikats für TLS C.FD.TLS-S und der Rolle “oid_epa_authn” umsetzen.

- *EPA-EPF-A_0058* - Komponente Autorisierung, Berechtigungssystem

  Die Komponente „Autorisierung“ MUSS für die Verwaltung und den Zugriff auf das gespeicherte, verschlüsselte Schlüsselmaterial ein Berechtigungssystem auf Basis der Authentifizierungsbestätigung authentifizierter Nutzer umsetzen.

- *A_16199* - Komponente Autorisierung - Rollenprüfung §291a

Die Komponente Autorisierung MUSS vor dem Ausstellen einer Autorisierungsbestätigung für den Zugriff auf medizinische Daten prüfen, ob der authentifizierte Nutzer als Versicherter oder gemäß einer Berufsgruppe nach § 291a Abs. 4 Satz 1 Nr. 2 SGB V für den Zugriff berechtigt ist.

- *A_13803* - Ausschluss einer Änderung der KVNR im Aktenkonto

  Der Anbieter ePA-Aktensystem MUSS verhindern, dass die KVNR des Versicherten im ePA-Aktensystem geändert werden kann.

- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem

  Die Komponente „Dokumentenverwaltung“ MUSS für die Verwaltung und den Zugriff der gespeicherten, verschlüsselten Daten ein Berechtigungssystem auf Basis der Authentifzierungs- und Autorisierungsbestätigung authentifizierter Nutzer umsetzen.

6.2.1.4 Zugriff von Geräten eines Versicherten

- *EPA-EPF-A_0164* - Zugriff eines Versicherten über registrierte Geräte

Das ePA-Aktensystem MUSS sicherstellen, dass einen Zugriff eines Versicherten auf das ePA-Aktensystem nur von einem vom Versicherten registrierten Gerät möglich ist.

- *EPA-EPF-A_0165* - Autorisiertes Gerät ist im Besitz des Versicherten

  Das ePA-Aktensystem MUSS während der Gerätregistrierung einen zusätzlichen Authentifizierungsschritt über einen separaten Benachrichtigungskanal durchführen.

- *EPA-EPF-A_0167* - Sperrung von autorisierten Geräten

  Das ePA-Aktensystem MUSS umsetzen, dass einen Zugriff auf das ePA-Aktensystem für ein autorisiertes Gerät gesperrt werden kann.

- *EPA-EPF-A_0168* - Verhindern von Session Hijacking

  Das ePA-Aktensystem MUSS sicherstellen, dass eine ePA-Session nicht von anderen Anwendungen auf dem Gerät übernommen werden kann.

- *EPA-EPF-A_0178* - Nutzung von Bestätigungen nur auf genau einem Gerät

  Das ePA-Aktensystem MUSS sicherstellen, dass die Authentifizierungs- und Autorisierungsbestätigung nur auf jeweils genau einem Gerät nutzbar sind.

- *EPA-EPF-A_0061* - Komponente Autorisierung – Geräteprüfung

  Die Komponente „Autorisierung“ MUSS bei Autorisierungsanfragen über I_Authorization_Insurant prüfen, ob das anfragende Gerät in der Liste der freigeschalteten Geräte des Versicherten bzw. seines Vertreters in diesem Aktenkonto enthalten ist. Ist das Gerät nicht enthalten, MUSS die Autorisierung abgebrochen und ein Freischaltprozess über den hinterlegten Benachrichtigungskanal gestartet werden. Für Autorisierungsanfragen aus der Leistungserbringerumgebung entfällt die Geräteprüfung.

- *EPA-EPF-A_0062* - Komponente Autorisierung – Geräteverwaltung

  Die Komponente „Autorisierung“ MUSS dem authentifizierten Versicherten über eine grafische Oberfläche das Verwalten derjenigen Gerätekennungen anbieten, die der Versicherte bzw. sein Vertreter nutzen, um auf das Aktenkonto zuzugreifen.

- *A_14270* - Komponente Autorisierung - Zugriff aus der Umgebung des Versicherten

  Die Komponente Autorisierung MUSS Zugriffe auf Daten eines Versicherten aus der Personal Zone heraus verhindern, wenn das verwendete Gerät des Versicherten nicht in der Liste der bekannten/freigeschalteten Geräte vorhanden ist.

6.2.1.5 HSM

- *A_14239* - Einsatz zertifizierter HSM

  Das ePA-Aktensystem MUSS beim Einsatz eines HSM sicherstellen, dass deren Eignung durch eine erfolgreiche Evaluierung nachgewiesen wurde. Als Evaluierungsschemata kommen dabei Common Criteria, ITSEC oder Federal Information Processing Standard (FIPS) in Frage. Die Prüftiefe MUSS mindestens

1. FIPS 140-2 Level 3,
2. Common Criteria EAL 4+ mit hohem Angriffspotenzial oder
3. ITSEC E3 der Stärke „hoch“ entsprechen

A_14240 - Sicherer Betrieb und Nutzung eines HSMs

Das ePA-Aktensystem MUSS sicherstellen, dass die im HSM verarbeiteten privaten Schlüssel nicht unautorisiert ausgelesen, unautorisiert verändert, unautorisiert ersetzt oder in anderer Weise unautorisiert benutzt werden können.

- *A_15091* - Komponente Authentisierung Versicherter - Verwendung eines HSM

  Die Komponente “Authentisierung Versicherter” MUSS das private Schlüsselmaterial der Ausstelleridentität C.FD.SIG und der TLS-Server-Identität C.FD.TLS-S in einem HSM speichern

6.2.1.6 Isolation

- *EPA-EPF-A_0170* - Informationstechnische Trennung der Komponenten des ePA-Aktensystems

  Das ePA-Aktensystem MUSS sicherstellen, dass alle Komponenten des ePA-Aktensystems informationstechnisch voneinander getrennt sind.

- *EPA-EPF-A_0187* - Keine Beeinflussung der Sicherheit zwischen Akten

  Die Komponente Dokumentenverwaltung des ePA-Aktensystems MUSS sicherstellen, dass die Beeinträchtigung der Sicherheit eines Aktenkontos nicht die Sicherheit eines anderen Aktenkontos beeinträchtigt.

- *A_13956* - Komponente Autorisierung -Separierung der Schnittstellen für verschiedene Umgebungen

  Die Komponente Autorisierung MUSS die Bereitstellungspunkte der Schnittstellen für die Nutzung durch benachbarte Komponenten und Produkttypen aus verschiedenen Einsatzumgebungen voneinander separieren. Diese Separierung kann beispielsweise umgesetzt werden durch die Erreichbarkeit der Schnittstellen über verschiedene Netzwerkadressen.

6.2.1.7 Schutzmaßnahmen

- *EPA-EPF-A_0171* - Schutzmaßnahmen gegen Angriffe aus der Umgebung des Versicherten

  Das ePA-Aktensystem MUSS sicherstellen, dass Angriffe aus der Umgebung des Versicherten abgewehrt werden.

- *EPA-EPF-A_0172* - Angriffen entgegenwirken

  Das ePA-Aktensystem MUSS Maßnahmen zur Erkennung und zur Schadensreduzierung und -verhinderung von Angriffen umsetzen.

- *EPA-EPF-A_0146* - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

  Alle Produkttypen der Fachanwendung ePA MÜSSEN Maßnahmen zum Schutz vor der aktuellsten Version der OWASP-Top-10-Risiken umsetzen.

6.2.1.8 Monitoring

- *EPA-EPF-A_0173* - Standardaktennutzung

  Das ePA-Aktensystem MUSS eine Standardaktennutzung definieren.

- *EPA-EPF-A_0174* - Abweichung von Standardaktennutzung

  Das ePA-Aktensystem MUSS bei einer erkannten Abweichung von der Standardnutzung darauf reagieren

6.2.2 Spezifische Anforderungen an die VAU

6.2.2.1 Isolation

- *EPA-EPF-A_0191* - Isolation zwischen Aktendatenverarbeitungsprozessen

  Die VAU MUSS die in ihr ablaufenden Verarbeitungsprozesse für die Daten eines Aktenkontos von den Verarbeitungsprozessen für die Daten anderer Aktenkonten trennen.

- *EPA-EPF-A_0192* - Isolation von Datenverarbeitungsprozessen des Anbieters

  Die VAU MUSS die in ihr ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters ePA-Aktensystem trennen.

- *EPA-EPF-A_0193* - Kein physischer Zugang des Anbieters zu Systemen der VAU

  Die VAU MUSS technisch sicherstellen, dass der Anbieter ePA-Aktensystem während der Verarbeitung personenbezogener und medizinischer Daten keinen Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.

6.2.2.2 Wartung

- *EPA-EPF-A_0194* - Nutzdatenbereinigung vor physischem Zugang

  Die VAU MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der VAU nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten mehr extrahiert werden können.

6.2.2.3 Integrität der VAU

- *EPA-EPF-A_0195* - Nur geprüfte Software in der VAU

  Die VAU MUSS sicherstellen, dass ausschließlich integritätsgeprüfte Software in der VAU ausgeführt wird.

- *EPA-EPF-A_0196* - Eine für ein Aktenkonto initialisierte VAU verarbeitet Daten genau zu diesem Aktenkonto

  Die VAU MUSS sicherstellen, dass sie ausschließlich Daten des Aktenkontextes verarbeitet, für den sie initialisiert wurde.

6.2.2.4 Verarbeitungskontext

- *A_14581* - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten

  Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass sämtliche schützenswerten Daten vor einer Speicherung außerhalb der VAU verschlüsselt werden.

- *A_14582* - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU

  Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass sämtliche schützenswerten Daten ausschließlich über sichere Verbindungen an autorisierte Nutzer weitergegeben werden.

- *A_14583* - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU

  Der Verarbeitungskontext der Komponente ePA-Dokumentenverwaltung MUSS für die Verschlüsselung aller Dokumentmetadaten, Policy Documents und des § 291a-Protokolls des Versicherten sowie eigener technischer Daten den Kontextschlüssel des Aktenkontos verwenden.

- *A_14566* - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihr ablaufenden Verarbeitungen für die Daten eines Verarbeitungskontextes von den Verarbeitungen für die Daten anderer Verarbeitungskontexte in solcher Weise trennen, dass mit technischen Mitteln ausgeschlossen wird, dass die Verarbeitungen eines Verarbeitungskontextes schadhaft auf die Verarbeitungen eines anderen Verarbeitungskontextes einwirken können.

6.2.2.5 Ausschluss von nicht autorisierten Zugriffen aus dem Betriebsumfeld

- *A_14558* - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die in ihren Verarbeitungskontexten ablaufenden Datenverarbeitungsprozesse von allen sonstigen Datenverarbeitungsprozessen des Anbieters trennen und damit gewährleisten, dass der Anbieter ePA-Aktensystem vom Zugriff auf die in der VAU verarbeiteten schützenswerten Daten ausgeschlossen ist.

- *A_14559* - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Software der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS eine Manipulation der eingesetzten Software erkennen und eine Ausführung der manipulierten Software verhindern.

- *A_14560* - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Hardware der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die Integrität der eingesetzten Hardware schützen und damit insbesondere Manipulationen an der Hardware durch den Anbieter ePA-Aktensystem ausschließen.

- *A_14561* - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Ausschluss von Manipulationen an der Hardware und der Software durch den Anbieter ePA-Aktensystem mit Mitteln umsetzen, deren dauerhafte und kontinuierliche Wirksamkeit gewährleistet werden kann.

- *A_14562* - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass niemand, auch nicht der Anbieter ePA-Aktensystem, während der Verarbeitung personenbezogener medizinischer Daten Zugriff auf physische Schnittstellen der Systeme erlangen kann, auf denen eine VAU ausgeführt wird.

- *A_14563* - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln sicherstellen, dass physischer Zugang zu Hardware-Komponenten der Verarbeitungskontexte nur erfolgen kann, nachdem gewährleistet ist, dass aus ihnen keine Nutzdaten extrahiert werden können.

- *A_14564* - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM

  Die Komponente ePA-Dokumentenverwaltung MUSS die folgenden privaten Schlüssel in einem Hardware Security Module (HSM) erzeugen und anwenden:

  – TI-Fachdienst-Identität zur Authentisierung des Kontextmanagements gegenüber dem Fachmodul ePA (TLS)
  – TI-Fachdienst-Identität zur Authentisierung des Verarbeitungskontextes gegenüber dem Fachmodul ePA (sicherer Kanal auf Anwendungsebene),
  – Privater Schlüssel des Schlüsselpaars zur Authentisierung des Verarbeitungskontextes gegenüber dem ePA-Frontend des Versicherten (sicherer Kanal auf Anwendungsebene).

  Die Prüftiefe des HSM MUSS dabei den in [gemSpec_Aktensystem#A_15156] angegebenen Standards entsprechen.

- *A_14565* - Komponente ePA-Dokumentenverwaltung – HSM- Kryptographieschnittstelle verfügbar nur für Instanzen der VAU

Die VAU der Komponente ePA-Dokumentenverwaltung MUSS mit technischen Mitteln, die auch Manipulationen durch den Anbieter ePA-Aktensystem ausschließen, gewährleisten, dass nur Instanzen der VAU Zugriff auf die Kryptographieschnittstelle des HSM zur Nutzung des privaten Schlüsselmaterials für ihre Dienstzertifikate erhalten können.

- *A_14567* - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS den Aufbau eines vertraulichen und integritätsgeschützten Kommunikationskanals gemäß [gemSpec_Krypt#3.15] zwischen einem Client und einem Verarbeitungskontext erzwingen, bevor der Verarbeitungskontext durch Übergabe des Kontextschlüssels durch den Client aktiviert werden kann.

6.2.2.6 Kryptographische Aktivierung des Verarbeitungskontextes

- *A_14570* - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung DARF den Kontextschlüssel NICHT über das Ende der Sitzung des letzten verbundenen Nutzers hinaus speichern oder verwenden.

6.2.2.7 Konsistenz der Akte, Logging und Monitoring

- *A_15841* - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sämtliche aktenbezogenen Daten (Nutzdaten, Konfigurationsdaten und Schlüsselmaterial) sicher löschen, wenn die Sitzung des letzten verbundenen Nutzers beendet wird.

- *A_14573* - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS sicherstellen, dass ein konsistenter Zustand des Verarbeitungskontextes auch bei Bedienfehlern oder technischen Problemen immer erhalten bleibt bzw. wiederhergestellt werden kann.

- *A_14574* - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU

  Die VAU der Komponente ePA-Dokumentenverwaltung MUSS die für den Betrieb eines Fachdienstes erforderlichen Logging- und Monitoring-Informationen in solcher Art und Weise erheben und verarbeiten, dass mit technischen Mitteln ausgeschlossen ist, dass dem Anbieter ePA-Aktensystem vertrauliche oder zur Profilbildung geeignete Daten zur Kenntnis gelangen.

7 Analyse und empfohlene Maßnahmen

In diesem Kapitel werden die Analyseergebnisse der Gutachter präsentiert. Von den Gutachtern empfohlene Maßnahmen sind aus Verständlichkeitsgründen unmittelbar mit der Präsentation der Analyse verzahnt angeführt.

7.1 Einleitung

Die gematik definiert an den verschiedensten Stellen in den Spezifikationen zur ePA und dem SGD sicherheitsrelevante Anforderungen. Viele Anforderungen sind dabei sehr konkret, und können daher gut einer Analyse unterzogen werden. So etwa das Design der wesentlichen kryptographischen Architektur des ePA Aktensystems, die eine solide Grundstruktur gegen Angreifer in Bezug auf die definierten Ziele (siehe Abschnitt 4) bildet. Diese Struktur scheint jedenfalls in den Grundfesten eine effektive Festung gegen den äußerst starken Angreifer – einen kompromittierten Betreiber der Fachandwendung ePA – zu bilden, und damit auch erst Recht vor schwächeren Angreifern wie Nutzer oder Dritte zu schützen.

Dies strebt die gematik mittels einer kryptographischen Architektur an, die auf Trust-Diversifikation (2 getrennte SGDs), auf absolutem Vertrauen in eine Trusted Third Party (die zentrale PKI der TI) sowie auf, u.a., aus dem Bankenbereich bewährte, HSMs setzt, und damit eine Quasi-Ende-zu-Ende Sicherheitslösung darstellt.

Eine informelle Analyse der aus der Sicht der Gutachter an diesem Zeitpunkt wichtigsten zu genauer untersuchenden kryptographischen Protokolle dieser Architektur wird in Abschnitt 7.3 präsentiert. Es ist dabei zu beachten, dass die spezifizierte Fachanwendung ePA, wie ähnliche komplexe sicherheitskritische Systeme, mit einer vielschichtigen Verteidigungsstrategie entworfen wurde. Von den Gutachtern identifizierte Schwachstellen (die gravierendste scheint zu sein, dass das VAU-Protokoll gegen Idendity Misbinding Angriffe verwundbar ist und damit die üblichen Erwartungen an einen authentifizierten sicheren Kanal verletzt[1]) führen nicht alle unmittelbar zu praxistauglichen, interessanten Angriffen. In der Praxis führt oft erst eine ungünstige Kombination von verschiedenen Schwachstellen einen realen Angreifer zum Erfolg. Je komplexer ein System ist, desto schwieriger ist es auch, die Bedeutung einzelner Schwachstellen gänzlich richtig einzuschätzen. In Hinblick auf ein sicheres, robustes Gesamtsystem, das sowohl über viele Jahre gut und sicher wartbar und ausbaufähig/erweiterbar bleibt, empfehlen die Gutachter daher jedenfalls, alle identifizierten Schwachstellen, die wichtige Sicherheitsgarantien von Teil-Maßnahmen einer vielschichtigen Gesamtstrategie verletzen, in künftigen Versionen der Spezifikation zu adressieren, auch wenn die Auswirkungen solcher Schwachstellen vielleicht zum jetzigen Zeitpunkt noch nicht greifbar sind.

Viele andere sicherheitsrelevante Anforderungen komplementieren die kryptographische Architektur der Fachanwendung ePA. Es wird dabei weitgehend auf Best Practice gesetzt, und wenig ausgelassen. Dazu zählt etwa, dass (1) alle Komponenten eine Inputvalidierung durchführen müssen (EPA-EPF-A_001), und dass (2) alle Komponenten untereinander nur verschlüsselt miteinander kommunzieren (EPA-EPF-A_0144) – Maßnahmen, die nicht nur

[1] **Wurde in Release 3.1.3 behobe**n

vor Angreifern von Aussen schützen, sondern auch das Risiko von Privilege Escalation Angriffen (vgl. Schutzziel 5 in Abschnitt 4) für Angreifer, die bereits eine Komponente im ePA-System kompromittieren konnten, vermindern.

Bei einigen Details sehen die Gutachter aber auch hier trotzdem noch Verbesserungsbedarf im Sinne des Systemdesigns: Zum Beispiel, wenn alle Komponenten der Fachanwendung ePA bereits untereinander vertraulich miteinander kommunizieren, wie in EPA-EPF-A_0144 spezifiziert, könnte man auch fordern, dass sich alle Komponenten, die miteinander funktional kommunizieren müssen, sich gegenseitig authentifizieren müssen, will man das Risiko weiter in Hinblick auf Schutzziel 5 minimieren.

Empfehlung 1

Authentifizierung aller Kommunikationspartner

Manche sicherheitsrelevanten Anforderungen in der gematik Spezifikation sind so allgemein und abstrakt gehalten, dass sie mehr einer Definition eines Sicherheitsziels gleichen und weniger eine konkrete Maßnahme darstellen. Vgl. etwa Anforderung EPA-EPF-A_0172. Solche Anforderungen entziehen sich einer genaueren Analyse – wie wirksam so eine Anforderung ist hängt dann gänzlich davon ab, wie sie von einem Betreiber interpretiert und umgesetzt wird. Eine klare Trennung und Darstellung von Sicherheitszielen und darauf abgestimmten konkreten Sicherheitsmaßnahmen wäre aus Sicherheitssicht sehr begrüßenswert.

Empfehlung 2

Klare Trennung und Darstellung von Sicherheitszielen und Sicherheitsmaßnahmen

Für eine weiterführende tiefgehende Analyse ist eine detailierte Risiko- und Bedrohungsanalyse erforderlich. Im vorgegebenen Zeitrahmen konnte diese nicht vollständig im Rahmen dieser Begutachtung durchgeführt werden. Es konnte nur eine Auswahl von Risiken und Bedrohungen berücksichtigt werden. Für eine tiefergehende Untersuchung des SGD-Protokolls sowie des VAU-Protokolls empfehlen die Gutachter zusätzlich auch den Einsatz von formalen Methoden.

Empfehlung 3

Durchführung einer tiefgehenden Risiko- und Bedrohungsanalyse

7.2 Zuordnung Sicherheitsanforderungen zu Sicherheitszielen

Die gematik Spezifikationen zu ePA und SGD definieren implizit eine vielschichtige Verteidigungsstrategie. In der Spezifikation sind dabei jedoch (1) Maßnahmen, die der Sicherheit dienen, nicht von funktionalen Maßnahmen hervorgehoben, und ist (2) nicht klar ersichtlich welche Maßnahmen gegen welchen Angreifer bzw. zur Umsetzung welches konkreten Sicherheitsziels intendiert sind. Des Weiteren sind Sicherheitsmaßnahmen quer- und weitverstreut definiert über mehrere hunderte Seiten Spezifikation. Dies erschwert nicht nur eine systematische Beurteilung, ob die definierten Maßnahmen ausreichend für das

Erreichen der jeweiligen Sicherheitsziele sind. Zusätzlich erschwert dies, so die Meinung der Gutachter, einem Hersteller bzw. Betreiber des Systems, sowie den Produkt-/Sicherheitsgutachtern die Arbeit, korrekte Interpretationen von spezifischen Anforderungen abzuleiten; dies insbesondere, wenn einzelne Anforderungen sehr abstrakt mit großem Interpretationsspielraum formuliert sind.

Die folgenden 2 Unterkapitel stellen einen ersten Versuch dar, (1) Sicherheitsanforderungen aus der Spezifikation zu identifizieren, und (2) die identifizierten Sicherheitsanforderungen den definierten Sicherheitszielen (vgl. Abschnitt 4 zuzuordnen. Betrachtet werden hierbei die Anforderungen, die komplementär zu den die kryptographische Architektur im Speziellen definierenden Anforderungen sind. Die Protokolle, die die kryptographische Architektur definieren, werden in Abschnitt 7.3 gesondert betrachtet.

Das Sicherheitsmodell, wie in Abschnitt 4 definiert, sieht eine Reihe unterschiedlicher Angreiferklassen vor (mit jeweils unterschiedlich zugeordneten Sicherheitszielen). Allgemein lässt sich sagen: Sicherheitsmaßnahmen, die gegen einen strikt stärkeren Angreifer effektiv greifen, dienen auch zur Abwehr des schwächeren Angreifers. Als stärkster Angreifer wird dabei ein kompromittierter Betreiber (vgl. Sicherheitsziel 4 in Abschnitt 4) angenommen. Die Sicherheitsmaßnahmen, die gegen einen kompromittierten Betreiber schützen, halten auch einen teilkompromittierten Betreiber (vgl. Sicherheitsziel 5) ab, und erst Recht Nutzer (vgl. Sicherheitsziele 2 und 3), sowie Dritte (vgl. Sicherheitsziel 1). In der nachfolgenden Zuordnung werden die für das Schutzziel bezüglich eines stärkeren Angreifers wirksame Anforderungen der Übersichtlichkeit wegen nicht auch bei dem Schutzziel bezüglich des schwächeren Angreifers gesondert angeführt, sofern nicht die unterschiedliche Angreiferklasse oder die unterschiedlichen Sicherheitsziele (welche Daten müssen geschützt werden, etc.) eine unterschiedliche Interpretation der Anforderung implizieren.

7.2.1 SGD

Die nachfolgenden Sicherheitsziele beziehen sich auf die Sicherheitsziele, welche in Abschnitt 4 aufgelistet sind.

7.2.1.1 Sicherheitsziel 1

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 1 (Angriffe durch Dritte) beitragen sollen:

- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive
- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip
- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip
- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip
- *GS-A_5557* - Security Monitoring
- *GS-A_5558* - Aktive Schwachstellenscans

Details zu Sicherheitsmonitoring und Schwachstellenscans sind im Hinblick auf das konkrete Sicherheitsziel zu definieren, deswegen auch extra bei den anderen Zielen angeführt.

Die Auswirkung der Schwächung von kryptographischen Primitiven sollte im Ernstfall immer auch gesondert in Hinblick auf die jeweiligen Sicherheitsziele untersucht werden, damit entsprechende Maßnahmen definiert werden können.

7.2.1.2 Sicherheitsziel 2

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 2 (Versicherter darf keine fremden ePA-Inhalte sehen) beitragen sollen:

- *GS-A_3139* - Krypto_Schlüssel: Dienst Schlüsselableitung
- *GS-A_3141* - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion
- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive
- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip
- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip
- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip
- *GS-A_5557* - Security Monitoring
- *GS-A_5558* - Aktive Schwachstellenscans

7.2.1.3 Sicherheitsziel 3

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 3 (Leistungserbringer darf nur für ihn berechtigte ePA-Inhalte sehen) beitragen sollen:

- *GS-A_3139* - Krypto_Schlüssel: Dienst Schlüsselableitung
- *GS-A_3141* - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion
- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive
- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip
- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip

- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip
- *GS-A_5557* - Security Monitoring
- *GS-A_5558* - Aktive Schwachstellenscans

7.2.1.4 Sicherheitsziel 4

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 4 (Angriffe durch Betreiber) beitragen sollen:

- *A_17987* - Anbieter ePA-Aktensystem - Organisatorische, technische und betriebliche Trennung zu SGD2
- *A_17881* - Anbieter SGD - Rollenausschluss für Anbieter des SGD der zentralen TI-Plattform
- *A_17885* - ePA-Aktensystem-spezifische Ableitungsschlüssel eines SGD-Instanz
- *GS-A_2158-01* - Trennung von kryptographischen Identitäten und Schlüsseln in Produktiv- und Testumgebungen
- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive
- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip
- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip
- *GS-A_3139* - Krypto_Schlüssel: Dienst Schlüsselableitung
- *GS-A_3141* - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion
- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip
- *GS-A_5557* - Security Monitoring
- *GS-A_5558* - Aktive Schwachstellenscans
- *A_17911* - SGD-HSM: Schlüsselerstellung und Veränderung im Mehr-Augen-Prinzip
- *A_17912* - SGD-HSM: Root-Schlüssel sind Teil des Firmware-
- *A_17913* - SGD-HSM: Exklusive Nutzungsrechte der Schlüssel für das Firmware-Modul
- *A_17915* - SGD: Nicht-Synchronisation der ECIES-Schlüssel (S4) und zugordnete Ableitungsschlüssel (S5)
- *A_17916* - Verfügbarkeit der Schlüssel in einem SGD-HSM

- *A_17917* - Schutz des SGD-HSM-Firmware-Moduls

7.2.1.5 Sicherheitsziel 7

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 7 (Schlüsselableitung durch SGD nur für erfolgreich authentisierte Nutzer) beitragen sollen:

- *GS-A_3078* - Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive
- *GS-A_3125* - Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip
- *GS-A_3130* - Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip
- *GS-A_3139* - Krypto_Schlüssel: Dienst Schlüsselableitung
- *GS-A_3141* - Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion
- *GS-A_3149* - Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip
- *GS-A_5557* - Security Monitoring
- *GS-A_5558* - Aktive Schwachstellenscans
- *A_17907* - SGD, Sicherheitsbegutachtung SGD-HSM
- *A_17911* - SGD-HSM: Schlüsselerstellung und Veränderung im Mehr-Augen-Prinzip
- *A_17912* - SGD-HSM: Root-Schlüssel sind Teil des Firmware-Moduls
- *A_17913* - SGD-HSM: Exklusive Nutzungsrechte der Schlüssel für das Firmware-Modul
- *A_17915* - SGD: Nicht-Synchronisation der ECIES-Schlüssel (S4) und zugordnete Ableitungsschlüssel (S5)
- *A_17916* - Verfügbarkeit der Schlüssel in einem SGD-HSM
- *A_17917* - Schutz des SGD-HSM-Firmware-Moduls

7.2.2 VAU

Die nachfolgenden Sicherheitsziele beziehen sich auf die Sicherheitsziele, welche in Abschnitt 4 aufgelistet sind.

7.2.2.1 Sicherheitsziel 1

Die Gutachter haben folgende Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 1 (Angriffe durch Betreiber) beitragen sollen:

- *EPA-EPF-A_0157* - Zusammenführung von Vertragsdaten und Aktendaten verhindern
- *EPA-EPF-A_0158* - Verbot der Auswertung von Beziehungen zwischen LE, LEI und Versicherten
- *EPA-EPF-A_0159* - Verbot der Profilbildung
- *EPA-EPF-A_0161* - Privacy by Default im ePA-Aktensystem
- *EPA-EPF-A_0001* - Übergreifende Vorbedingung: Aufrufparameter gültig
- *A_15613* - Komponente Authentisierung Versicherter – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachricht
- *EPA-EPF-A_0002* - Übergreifende Vorbedingung: Login nach Notwendigkeit
- *EPA-EPF-A_0010* - Impliziter Logout nach Inaktivität eines Nutzers
- *EPA-EPF-A_0011* - Expliziter Logout auf Anforderung eines Nutzers
- *EPA-EPF-A_0144* - Schutz der Kommunikation
- *EPA-EPF-A_0145* - Informationstechnische Trennung
- *EPA-EPF-A_0163* - Serverseitige Authentisierung erforderlich
- *A_15091* - Komponente Authentisierung Versicherter - Verwendung eines HSM
- *EPA-EPF-A_0188* - Sichere Session-Verwaltung
- *EPA-EPF-A_0175* - Integritätsschutz für Bestätigungen
- *EPA-EPF-A_0169* - Zusätzliche Autorisierung von sensiblen Anwendungsfällen
- *A_14227* - Komponente Authentisierung Versicherter - TLS-Authentisierung innerhalb der TI
- *EPA-EPF-A_0058* - Komponente Autorisierung, Berechtigungssystem
- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem
- *EPA-EPF-A_0164* - Zugriff eines Versicherten über registrierte Geräte
- *EPA-EPF-A_0165* - Autorisiertes Gerät ist im Besitz des Versicherten
- *EPA-EPF-A_0167* - Sperrung von autorisierten Geräten
- *EPA-EPF-A_0168* - Verhindern von Session Hijacking
- *EPA-EPF-A_0178* - Nutzung von Bestätigungen nur auf genau einem Gerät

- *EPA-EPF-A_0061* - Komponente Autorisierung – Geräteprüfung
- *EPA-EPF-A_0062* - Komponente Autorisierung – Geräteverwaltung
- *A_14270* - Komponente Autorisierung - Zugriff aus der Umgebung des Versicherten
- *EPA-EPF-A_0171* - Schutzmaßnahmen gegen Angriffe aus der Umgebung des Versicherten
- *EPA-EPF-A_0172* - Angriffen entgegenwirken
- *EPA-EPF-A_0146* - Schutzmaßnahmen gegen die OWASP Top 10 Risiken

7.2.2.2 Sicherheitsziele 2 und 3

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen der Sicherheitsziele 2 (Versicherter darf keine fremden ePA-Inhalte sehen) und 3 (Leistungserbringer darf nur für ihn berechtigte ePA-Inhalte sehen) beitragen sollen:

- *EPA-EPF-A_0161* - Privacy by Default im ePA-Aktensystem
- *EPA-EPF-A_0001* - Übergreifende Vorbedingung: Aufrufparameter gültig
- *A_13679* - Sicherheitstechnische Validierung in der Dokumentenverwaltung
- *A_15613* - Komponente Authentisierung Versicherter – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachricht
- *A_14529* - Komponente Autorisierung - Absicherung gegenüber dem Internet
- *A_14529* - Komponente Autorisierung - Absicherung gegenüber dem Internet
- *EPA-EPF-A_0002* - Übergreifende Vorbedingung: Login nach Notwendigkeit
- *EPA-EPF-A_0010* - Impliziter Logout nach Inaktivität eines Nutzers
- *EPA-EPF-A_0011* - Expliziter Logout auf Anforderung eines Nutzers
- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem
- *EPA-EPF-A_0144* - Schutz der Kommunikation
- *EPA-EPF-A_0163* - Serverseitige Authentisierung erforderlich
- *EPA-EPF-A_0188* - Sichere Session-Verwaltung
- *EPA-EPF-A_0175* - Integritätsschutz für Bestätigungen
- *EPA-EPF-A_0176* - Akzeptanz nur von eigenen Autorisierungsbestätigungen
- *EPA-EPF-A_0169* - Zusätzliche Autorisierung von sensiblen Anwendungsfällen
- *A_14227* - Komponente Authentisierung Versicherter - TLS-Authentisierung innerhalb der TI
- *EPA-EPF-A_0058* - Komponente Autorisierung, Berechtigungssystem

- *A_16199* - Komponente Autorisierung - Rollenprüfung §291a
- *A_13803* - Ausschluss einer Änderung der KVNR im Aktenkonto
- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem
- *EPA-EPF-A_0164* - Zugriff eines Versicherten über registrierte Geräte
- *EPA-EPF-A_0165* - Autorisiertes Gerät ist im Besitz des Versicherten
- *EPA-EPF-A_0167* - Sperrung von autorisierten Geräten
- *EPA-EPF-A_0168* - Verhindern von Session Hijacking
- *EPA-EPF-A_0178* - Nutzung von Bestätigungen nur auf genau einem Gerät
- *EPA-EPF-A_0061* - Komponente Autorisierung – Geräteprüfung
- *EPA-EPF-A_0062* - Komponente Autorisierung – Geräteverwaltung
- *A_14270* - Komponente Autorisierung - Zugriff aus der Umgebung des Versicherten
- *EPA-EPF-A_0187* - Keine Beeinflussung der Sicherheit zwischen Akten
- *A_13956* - Komponente Autorisierung -Separierung der Schnittstellen für verschiedene Umgebungen
- *EPA-EPF-A_0171* - Schutzmaßnahmen gegen Angriffe aus der Umgebung des Versicherten
- *EPA-EPF-A_0172* - Angriffen entgegenwirken
- *EPA-EPF-A_0146* - Schutzmaßnahmen gegen die OWASP Top 10 Risiken
- *EPA-EPF-A_0173* - Standardaktennutzung
- *EPA-EPF-A_0174* - Abweichung von Standardaktennutzung
- *EPA-EPF-A_0191* - Isolation zwischen Aktendatenverarbeitungsprozessen
- *EPA-EPF-A_0192* - Isolation von Datenverarbeitungsprozessen des Anbieters
- *EPA-EPF-A_0196* - Eine für ein Aktenkonto initialisierte VAU verarbeitet Daten genau zu diesem Aktenkonto
- *A_14582* - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU
- *A_14566* - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU
- *A_14567* - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU
- *A_14573* - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU

7.2.2.3 Sicherheitsziel 4

Die Gutachter haben folgende Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 4 (Angriffe durch Betreiber) beitragen sollen:

- *EPA-EPF-A_0161* - Privacy by Default im ePA-Aktensystem
- *EPA-EPF-A_0001* - Übergreifende Vorbedingung: Aufrufparameter gültig
- *A_13679* - Sicherheitstechnische Validierung in der Dokumentenverwaltung
- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem
- *EPA-EPF-A_0183* - Umsetzung der Dokumentenverwaltung in einer VAU
- *EPA-EPF-A_0184* - Verschlüsselung der Nutzdaten eines Aktenkontos außerhalb der VAU
- *EPA-EPF-A_0188* - Sichere Session-Verwaltung
- *EPA-EPF-A_0187* - Keine Beeinflussung der Sicherheit zwischen Akten
- *EPA-EPF-A_0191* - Isolation zwischen Aktendatenverarbeitungsprozessen
- *EPA-EPF-A_0192* - Isolation von Datenverarbeitungsprozessen des Anbieters
- *EPA-EPF-A_0193* - Kein physischer Zugang des Anbieters zu Systemen der VAU
- *EPA-EPF-A_0194* - Nutzdatenbereinigung vor physischem Zugang
- *EPA-EPF-A_0195* - Nur geprüfte Software in der VAU
- *EPA-EPF-A_0196* - Eine für ein Aktenkonto initialisierte VAU verarbeitet Daten genau zu diesem Aktenkonto
- *A_14581* - Komponente ePA-Dokumentenverwaltung – Verschlüsselung von außerhalb des Verarbeitungskontextes der VAU gespeicherten Daten
- *A_14582* - Komponente ePA-Dokumentenverwaltung – Geschützte Weitergabe von Daten an autorisierte Nutzer durch die VAU
- *A_14583* - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU
- *A_14566* - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU
- *A_14558* - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters
- *A_14559* - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Software der VAU
- *A_14560* - Komponente ePA-Dokumentenverwaltung – Ausschluss von Manipulationen an der Hardware der VAU

- *A_14561* - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
- *A_14562* - Komponente ePA-Dokumentenverwaltung – Kein physischer Zugang des Anbieters zu Systemen der VAU
- *A_14563* - Komponente ePA-Dokumentenverwaltung – Nutzdatenbereinigung vor physischem Zugang zu Systemen der VAU
- *A_14564* - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM
- *A_14565* - Komponente ePA-Dokumentenverwaltung – HSM- Kryptographieschnittstelle verfügbar nur für Instanzen der VAU
- *A_14567* - Komponente ePA-Dokumentenverwaltung – Sicherer Kanal vom Client zum Verarbeitungskontext der VAU
- *A_14570* - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU
- *A_15841* - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes
- *A_14573* - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU
- *A_14574* - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU

7.2.2.4 Sicherheitsziel 5

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 5 (kein Zugriff auf medizinische Daten bei Teilkompromittierung des Backends außer VAU) beitragen sollen:

- *EPA-EPF-A_0161* - Privacy by Default im ePA-Aktensystem
- *EPA-EPF-A_0001* - Übergreifende Vorbedingung: Aufrufparameter gültig
- *A_13679* - Sicherheitstechnische Validierung in der Dokumentenverwaltung
- *A_15613* - Komponente Authentisierung Versicherter – Erkennung von Denial-of-Service-Angriffen hinsichtlich dem Parsen von SOAP 1.2-Nachricht
- *A_14529* - Komponente Autorisierung - Absicherung gegenüber dem Internet
- *EPA-EPF-A_0002* - Übergreifende Vorbedingung: Login nach Notwendigkeit
- *EPA-EPF-A_0010* - Impliziter Logout nach Inaktivität eines Nutzers
- *EPA-EPF-A_0011* - Expliziter Logout auf Anforderung eines Nutzers
- *EPA-EPF-A_0064* - Komponente Dokumentenverwaltung – Berechtigungssystem

- *EPA-EPF-A_0144* - Schutz der Kommunikation
- *EPA-EPF-A_0145* - Informationstechnische Trennung
- *EPF-A_0170* - Informationstechnische Trennung der Komponenten des ePA-Aktensystems
- *EPA-EPF-A_0188* - Sichere Session-Verwaltung
- *EPA-EPF-A_0170* - Informationstechnische Trennung der Komponenten des ePA-Aktensystems
- *EPA-EPF-A_0172* - Angriffen entgegenwirken
- *EPA-EPF-A_0146* - Schutzmaßnahmen gegen die OWASP Top 10 Risiken
- *EPA-EPF-A_0173* - Standardaktennutzung
- *EPA-EPF-A_0174* - Abweichung von Standardaktennutzung

7.2.2.5 Sicherheitsziel 6

Die Gutachter haben folgende direkte Sicherheitsanforderungen gefunden, welche zum Erreichen des Sicherheitsziels 6 (keine Beeinflussung anderer Aktenkonten) beitragen sollen:

- *EPA-EPF-A_0191* - Isolation zwischen Aktendatenverarbeitungsprozessen
- *EPA-EPF-A_0196* - Eine für ein Aktenkonto initialisierte VAU verarbeitet Daten genau zu diesem Aktenkonto
- *A_14583* - Komponente ePA-Dokumentenverwaltung – Verschlüsselung der Dokumentmetadaten und technischen Daten der VAU
- *A_14566* - Komponente ePA-Dokumentenverwaltung – Isolation zwischen Datenverarbeitungsprozessen mehrerer Verarbeitungskontexte der VAU
- *A_14570* - Komponente ePA-Dokumentenverwaltung – Keine Speicherung des Kontextschlüssels in der VAU
- *A_15841* - Komponente ePA-Dokumentenverwaltung – Löschen aller aktenbezogenen Daten beim Beenden des Verarbeitungskontextes
- *A_14573* - Komponente ePA-Dokumentenverwaltung – Konsistenter Systemzustand des Verarbeitungskontextes der VAU
- *A_14574* - Komponente ePA-Dokumentenverwaltung – Datenschutzkonformes Logging und Monitoring des Verarbeitungskontextes der VAU
- *EPA-EPF-A_0192* - Isolation von Datenverarbeitungsprozessen des Anbieters
- *A_14558* - Komponente ePA-Dokumentenverwaltung – Isolation der VAU von Datenverarbeitungsprozessen des Anbieters

- *A_14561* - Komponente ePA-Dokumentenverwaltung – Kontinuierliche Wirksamkeit des Manipulationsschutzes der VAU
- *A_14564* - Komponente ePA-Dokumentenverwaltung – Private Schlüssel von Dienstzertifikaten im HSM
- *A_14565* - Komponente ePA-Dokumentenverwaltung – HSM- Kryptographieschnittstelle verfügbar nur für Instanzen der VAU

7.3 Analyse der kryptographischen Protokolle

7.3.1 Allgemein

Auf Grund der zeitlichen Rahmenbedingungen der vorliegenden Sicherheitsanalyse konnte in diesem Abschnitt nur eine Auswahl, der für die Sicherheit des ePA-Systems aus Sicht der Gutachter besonders relevanten, Protokolle und Abläufe im Detail dargestellt und analysiert werden.

Die Illustrationen in diesem Kapitel werden auf die kryptographisch relevanten Teile reduziert, um ein einfacheres und gezielteres Verständnis zu erreichen.

Bei den nachfolgenden Analysen beschränkt sich die Darstellung auf das Szenario FdV (Frontend des Versicherten) unter Verwendung einer eGK. Die Variante, wie sie z.B. aus Sicht eines Arztes ist, unter Verwendung eines Konnektors und einer SMC-B, wird in den Abbildungen und Sequenzen nicht gesondert dargestellt, sofern die Prozesse aus Sicherheitsbeurteilungssicht im Wesentlichen isomorph sind. Die einzelnen Findings können damit auf alle gleichen Szenarien analog umgelegt werden.

7.3.1.1 Überblick eines gesamten Client-Durchlaufs

Für die Verwaltung von Akten bzw. Dokumenten im ePA-System durch einen *Versicherten* bzw. *Berechtigten*[2] muss durch das ePA-System *immer* ein VAU-Kontext in der VAU (*Vertrauenswürdige Ausführungsumgebung*) initialisiert werden. Dieser Kontext wird durch eine sequentielle Abhandlung von Authentisierungs-, Autorisierungs-, Schlüsselableitungs- und Kontext-Initialisierungs-Protokollen geöffnet und bleibt dann kurzzeitig (wenige Minuten) als sicher initialisierter Kontext in der VAU erhalten, bevor dieser wieder geschlossen und sicher vernichtet werden muss.

Wenn ein Client, was entweder das *Frontend eines Versicherten* (z.B. Mobile App) oder das *Fachmodul ePA* (innerhalb eines Konnektors) sein kann, einen VAU-Kontext initialisieren will, werden folgende Aktionen durchgeführt:

- Login durch Authentifizierung und Erhalten eines *Authentisierungstokens* an der *Authentisierungskomponente*.

[2] Der Nachweis einer Berechtigung erfolgt durch: eGK, alternative Versichertenidentität (al.vi), SMC-B oder SMC-ORG/KTR

- Erhalten der Autorisierung durch Abholen eines *Autorisierungstokens* und der *AuthorizationKeys* (verschlüsselte Akten- und Kontextschlüssel) an der *Autorisierungskomponente*.
- Erhalten der Schlüsselverschlüsselungsschlüssel (später im Dokument als SK_{SGD1} und SK_{SGD2} bezeichnet, diese werden zum Ver- bzw. Entschlüsseln der Akten- und Kontextschlüssel verwendet) durch erneutes Ableiten eben dieser an den beiden *Schlüsselgenerierungsdiensten*.
- Initialisieren eines VAU-Kontexts durch Anwendung des VAU-Protokolls (Authentifizierung, Aufbau eines sicheren Kanals und übermitteln des Kontextschlüssels) an die *VAU-Komponente*.

Nachfolgend, in Abbildung 3, ist eine etwas vereinfachte, aber dennoch sehr detaillierte Darstellung eines Client-Durchlaufs zum Öffnen eines VAU-Kontexts im gesamtheitlichen ePA-System veranschaulicht. Diese gibt einen guten Überblick über den Ablauf und die darin beteiligten Systeme.

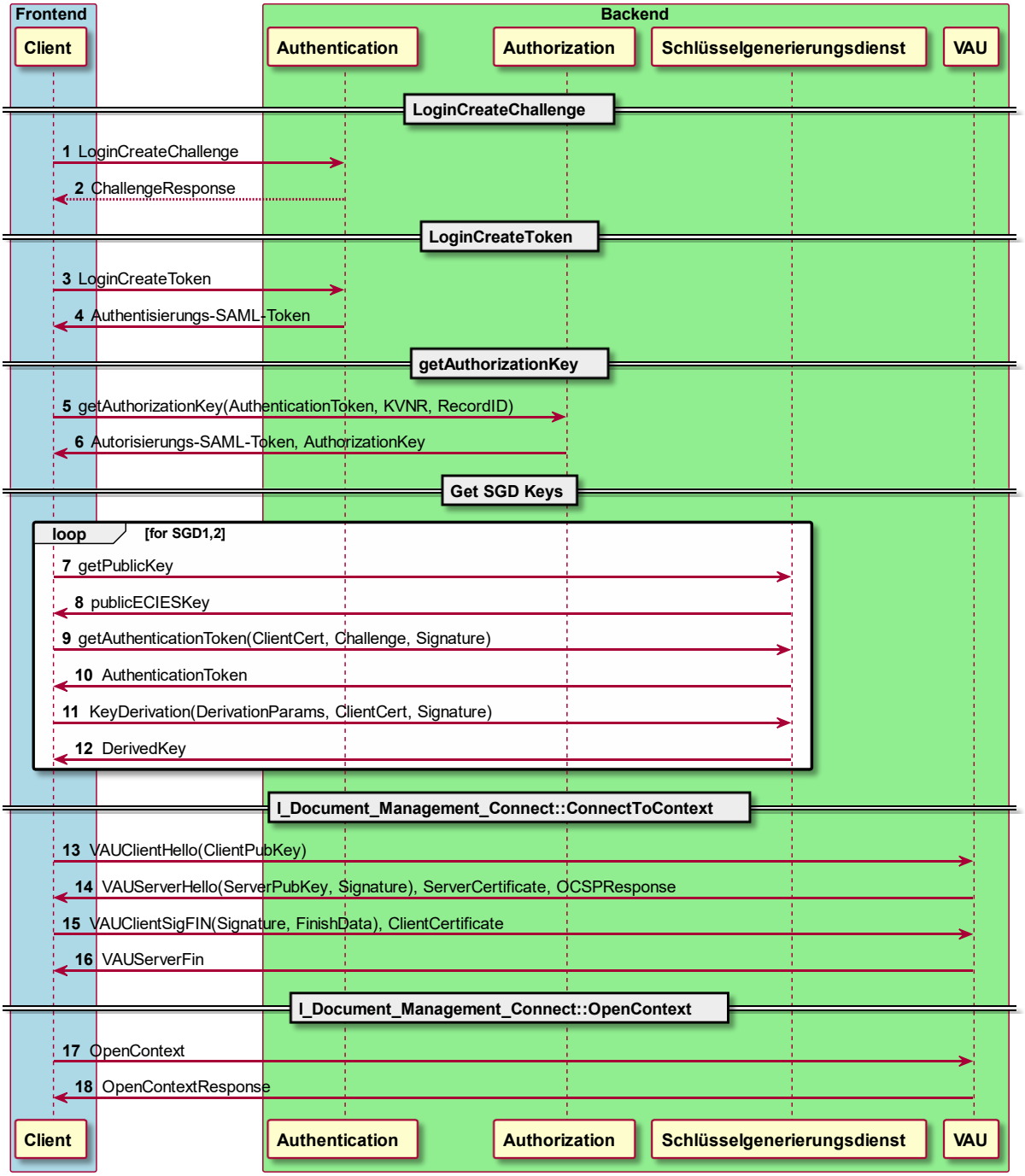


Abbildung 3: Sequenzdiagramm eines gesamten Client-Durchlaufs vom Login bis zum offenen Kontext.

7.3.2 Schlüsselableitung via HKDF

Innerhalb der nachfolgend im Detail beschriebenen Abläufe bzw. Protokolle werden an verschiedensten Stellen symmetrische Schlüssel abgeleitet. Diese Ableitung erfolgt, wenn nicht explizit anders angegeben, in der Regel unter Verwendung von HKDF [4]. In aller Regel

werden, falls nicht explizit anders angegeben, im Kontext des ePA-Systems 256-bit AES-Schlüssel erzeugt, d. h. `L=256`.

Dieses Ableitungsverfahren ist detailliert in Abbildung 4 dargestellt und wird innerhalb dieses Dokuments weiterführend mit *KDF* bzw. *HKDF* referenziert.

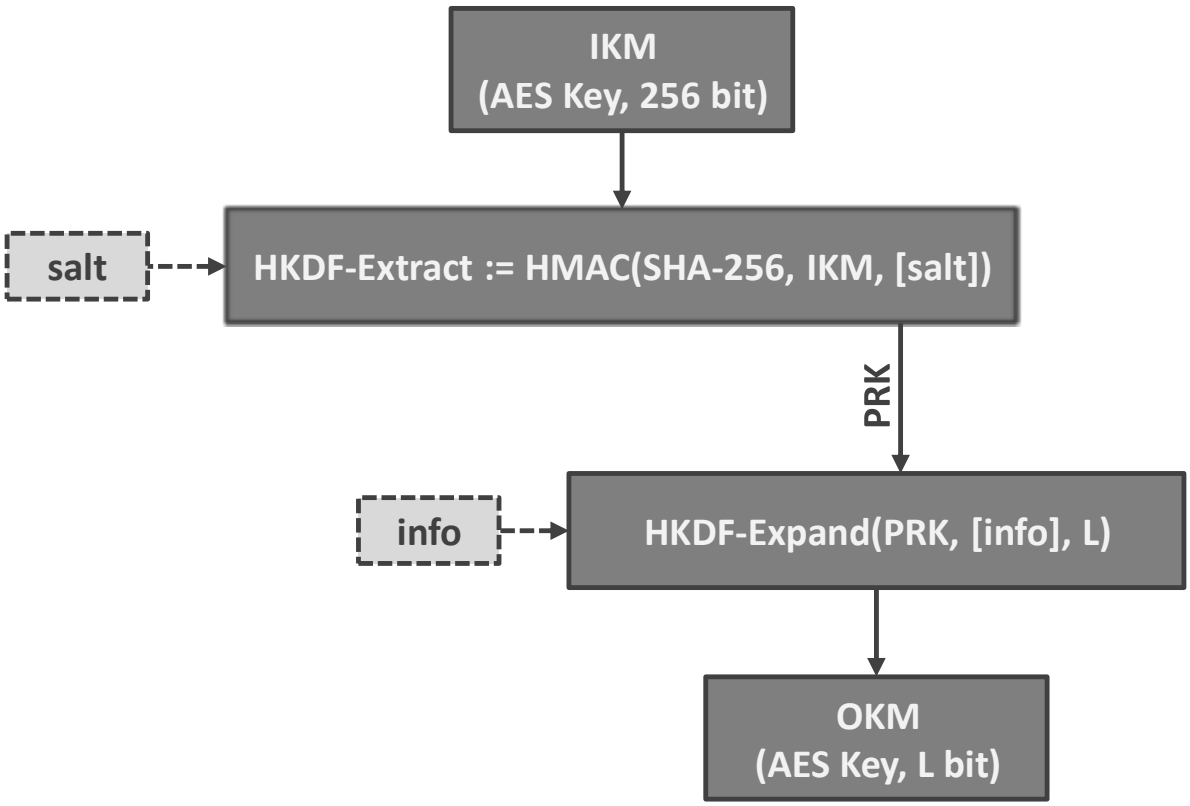


Abbildung 4: Schlüsselableitung von AES-Schlüssel via HKDF.

Beim HKDF-Schlüsselableitungsverfahren handelt es sich nach dem im Jahr 2019 aktuellen Stand der Technik um einen gut analysierten Algorithmus zur Schlüsselableitung. Der Algorithmus weist bisher keine Sicherheitsschwachstellen auf. Die von der gematik spezifizierte HKDF-Variante basiert auf SHA-256.

Als State-of-the-Art Schlüsselableitungsmechanismus hat es HKDF als Basis zur Schlüsselableitung auch in die neueste TLS-Version TLS 1.3 [5] geschafft. Diese Wahl ist daher grundsätzlich sehr gut.

7.3.2.1 Weitere Empfehlung

Der Aufruf von HKDF innerhalb des ePA-Systems erfolgt meistens ohne der Verwendung des *Salt*-Inputs und des Öfteren ohne der Verwendung des *Info*-Inputs. Dies wäre jedoch idealerweise zur weiteren Diversifizierung bzw. Abgrenzung der abgeleiteten Schlüssel empfehlenswert.

Empfehlung 4

Verwendung von Salt-Input und Info-Input bei HKDF – siehe Abschnitte 7.3.2.1.1, 7.3.2.1.2

So ein Vorgehen macht das System aus Sicherheitssicht robuster, auch in Hinblick auf künftige Änderungen und wird daher empfohlen, auch wenn im Rahmen der durchgeführten Analyse kein unmittelbares Verfehlen der definierten Sicherheitsziele für die vorgesehenen Angriffspotentiale identifiziert werden konnte.

7.3.2.1.1 Salt

Laut der Spezifikation von HKDF [4], Abschnitt 3.1, ist der *Salt* als optional aber dringend empfohlen eingestuft:

"We stress, however, that the use of salt adds significantly to the strength of HKDF, ensuring independence between different uses of the hash function, supporting "source-independent" extraction, and strengthening the analytical results that back the HKDF design.

[...]

Ideally, the salt value is a random (or pseudorandom) string of the length HashLen. Yet, even a salt value of less quality (shorter in size or with limited entropy) may still make a significant contribution to the security of the output keying material (OKM); designers of applications are therefore encouraged to provide salt values to HKDF if such values can be obtained by the application."

Als *Salt* könnte jeweils für die verschiedenen Protokolle innerhalb des ePA-Systems ein in der Spezifikation definierter, aber dann statischer Wert, für den jeweiligen ePA-Use-Case für die Schlüsselableitungen definiert werden. Dieser sollte laut HKDF [4], Abschnitt 3.1, idealerweise die Länge der benutzten Hashfunktion, in diesen Fällen also immer 256-Bit, haben.

7.3.2.1.2 Info

In Abschnitt 3.2 von HKDF[4] wird ebenso darauf hingewiesen, dass der *Info*-Input zwar optional ist, aber in vielen Applikationen große Wichtigkeit besitzt:

While the 'info' value is optional in the definition of HKDF, it is often of great importance in applications. Its main objective is to bind the derived key material to application- and context-specific information. For example, 'info' may contain a protocol number, algorithm identifiers, user identities, etc. In particular, it may prevent the derivation of the same keying material for different contexts (when the same input key material (IKM) is used in such different contexts).

Als Beispiel wäre es hier z.B. im VAU-Protokoll (siehe Abschnitt 7.3.5) bei der Ableitung des Schlüsselidentifiers $ID_{AES\text{-}Key}$ bzw. des Schlüssels SK_{C_S} von Vorteil, wenn man spezifische Information des Kontexts bzw. konkret der aufzubauenden Sitzung einfließen lassen würde.

Dies könnten unter Umständen folgende Informationen sein:

- *Client Information*: PuK.C1 (oder idealerweise gleich $hash_{VCHD}$)
- *Server Information:* $CipherConf_S$, C_{VAU} und PuK.S1

7.3.3 Authentisierung/Autorisierung

7.3.3.1 Authentifizierung

7.3.3.1.1 Überblick

Laut gematik Spezifikationen werden im Rahmen der Authentifizierung OASIS Standards und ein Challenge-Response-Verfahren kombiniert eingesetzt. Das Verfahren ermöglicht es einen Nutzer anhand seiner eGK bzw. SMC-B zu authentifizieren. Der Ablauf der Kommunikation mit einem Authentifizierungsdienstes ist in Abbildung 5 dargestellt.

Beim Login stellt der Authentifizierungsdienst eine *AuthenticationAssertion* aus, diese wird im weiteren Verlauf vom Client dazu verwendet, um sich am ePA-System zu autorisieren. Aufgrund der kurzen Gültigkeit der *AuthenticationAssertion* wird den Clients vom Authentifizierungsdienst eine Operation *Renew* angeboten, um auf Basis einer gültigen Assertion eine neue zu bekommen, die alte ist ab diesem Zeitpunkt nicht mehr gültig. Ein solches *AuthenticationAssertion* ist eine SAML2-Assertion, wobei in dieser insbesondere folgende sicherheitsrelevante Werte eingebettet und anschließend vom Aussteller signiert werden:

- *FQDN* ist der anbieterspezifische Fully-Qualified Domain Name
- *X509SubjectName* aus dem Zertifikat (C.CH.AUT bzw. C.CH.AUT_ALT) des anfragenden Clients
- *NotBefore* wird auf die Systemzeit gesetzt
- *NotOnOrAfter* wird auf die Systemzeit + 5 Minuten gesetzt
- *AudienceRestriction* wird auf den FQDN des Anbieters des Aktensystems gesetzt

Durch das Signieren der *AuthenticationAssertion* durch den Aussteller wird erreicht, dass der Empfänger der *AuthenticationAssertion* zB. die eigene Identität, den Aussteller oder den gültigen Zeitraum nicht verändern kann, um damit einen Vorteil gegenüber dem ePA-System, z.B. durch die Annahme einer fremden Identität, zu erwirken.

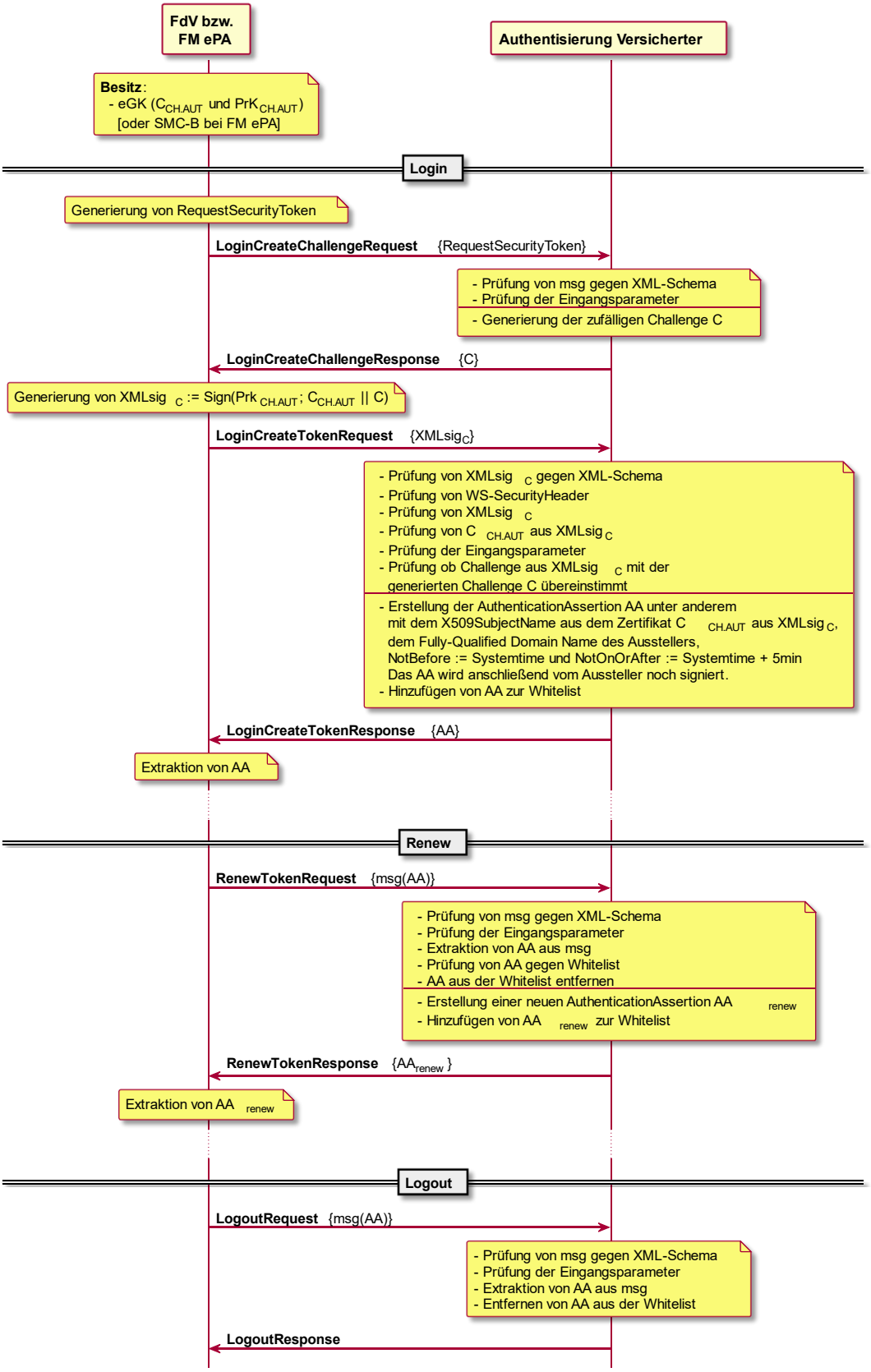


Abbildung 5: Authentication-Protokoll

7.3.3.1.2 Schwachstelle im Authentifizierungsverfahren: Identity Misbinding Angriff

Schwachstelle 1

Identity Misbinding Angriff

Wenn ein Angreifer im Besitz einer validen eGK oder SMC-B ist und die TLS-Verbindung aufbrechen kann, kann dieser einen Identity Misbinding Angriff durchführen. Dazu muss er zuerst die `LoginCreateChallengeResponse` Nachricht aufzeichnen. Sobald der Nutzer nun die Nachricht `LoginCreateTokenRequest` sendet, tauscht der Angreifer diese durch eine von ihm erstellte und signierte `LoginCreateTokenRequest` Nachricht aus. Der Server stellt dann ein *AuthenticationAssertion* für den Angreifer an den Nutzer aus. Da dieser nicht prüft, ob in dieser Assertion seine eigene Identität vorhanden ist, sondern diese einfach verwendet, wird er sich ab diesem Zeitpunkt für den Angreifer ausgeben.

***Behebung**: Mit Release 3.1.3 wird die Schwachstelle erfolgreich beseitigt: Ein ePA-Client überprüft (A_18985) eine erhaltene AuthenticationAssertion auf Korrektheit. Damit ist die Schwachstelle 'Identity Misbinding Angriff' obsolet.*

7.3.3.2 Autorisierung

Nach erfolgreicher Authentifizierung eines Clients am Authentifizierungsdienst muss sich ein Nutzer mittels *AuthenticationAssertion* autorisieren, um Zugriff zu den angeforderten Dokumenten zu bekommen.

Die Autorisierung eines Versicherten oder Vertreters mit einer eGK ist nur mittels “More-Factor-Authentication” möglich, was sehr zu begrüßen ist. Dadurch wird die Sicherheit gegen unerlaubten Zugriff im Vergleich beispielsweise zu einer ausschließlichen Authentifizierung mittels 1 Faktor (etwa einer PIN) weiter erhöht. Die Registrierung eines zusätzlichen Faktors (Gerät des Nutzers, neben Karte und PIN) erfolgt zudem über einen alternativen Kanal (E-Mail), womit es einem Angreifer erschwert wird, eigene Geräte hinzuzufügen.

Wenn ein Nutzer durch den Autorisierungsdienst erfolgreich autorisiert wird, erhält er vom Autorisierungsdienst eine *AuthorizationAssertion* und einen *AuthorizationKey*. Der *AuthorizationKey* ist ein verschlüsselter Container, in welchem der Akten- sowie Kontextschlüssel abgelegt ist. Der *AuthorizationKey* kann mittels der Schlüssel, die vom SGD1 und SGD2 abgeleitet werden, entschlüsselt werden. Dies sollte ausschließlich der berechtigte Client durchführen können.

Die *AuthorizationAssertion* ist eine SAML2-Assertion und wird durch das Signieren durch die Ausstelleridentität geschützt. Damit wird verhindert, dass der Client die *AuthorizationAssertion* ändern kann.

Eine solche *AuthorizationAssertion* enthält unter anderem folgende Elemente:

- *FQDN* des Ausstellers
- *Signatur* über die AuthorizationAssertion mit dem privaten Schlüssel des Ausstellers
- *X509SubjectName* des anfragenden Clients aus der AuthenticationAssertion
- *NotBefore* muss auf die Systemzeit des Ausstellers gesetzt werden
- *NotOnOrAfter* muss auf die Systemzeit + 15 Minuten
- *RecordIdentifier* der Akte für die diese AuthorizationAssertion gilt
- *AuthorizationType* (Document/Recovery/Account)

- *DeviceID* aus der Anfrage

7.3.4 SGD

7.3.4.1 Überblick

Das SGD-Protokoll dient dem Ziel die Berechtigtenschlüssel für Versicherte und Berechtigte herzuleiten. Diese Schlüssel werden später im Dokument als SK_{SGD1} und SK_{SGD2} bezeichnet, wobei es sich hierbei um jene kryptographische Schlüssel handelt, welche zur Verschlüsselung der Akten- und Kontextschlüssel dienen.

Das SGD-Protokoll beinhaltet den Aufbau eines beidseitig authentifizierten sicheren Ende-zu-Ende Kanals zwischen dem SGD-HSM und dem FdV (kryptographisch unter Verwendung der eGK). Die Sicherheit dieses Ende-zu-Ende-Kanals dient als wesentliches Instrument zur Erreichung der Schutzziele Integrität und Vertraulichkeit der Daten einer ePA.

Das Design des Protokolls wurde so gewählt, dass es trotz der Einschränkung der kryptographischen Operationen auf einer eGK und der zu erwartenden großen Last auf dem HSM-Modul implementierbar bleibt und skaliert.

Um keinem der Diensteanbieter die Möglichkeit der Totalkontrolle des zur Entschlüsselung der Akten erforderlichen Schlüsselmaterials zu geben, wurden von gematik zwei SGD-Instanzen spezifiziert. Diese beiden Instanzen müssen laut gematik zudem auf zwei unabhängige, strikt organisatorisch und technisch getrennte, Anbieter verteilt werden. Der *SGD1* ist bei dem jeweiligen Anbieter des ePA-Aktensystems im Betrieb, wobei der *SGD2* immer in der betrieblichen und organisatorischen Obhut der *zentralen Telematikinfrastruktur* (TI) ist.

Sowohl die abgeleiteten Schlüssel, als auch die zugrunde liegenden Ableitungsschlüssel der beiden SGD-Instanzen sind somit unabhängig voneinander und werden anschließend am FdV im “Zwiebelschalenprinzip” zur Verschlüsselung der Akten-, Dokument- und Kontextschlüssel verwendet (siehe *Use Case: Put Authorization Key* in Abbildung 8, Abschnitt 7.3.4.4).

7.3.4.2 Vertrauensanker

In der nachfolgenden Abbildung 6 ist eine stark vereinfachte Repräsentation der primär beim SGD-Protokoll beteiligten Komponenten und dem verwendeten kryptographischem Material inkl. der Veranschaulichung der existierenden Vertrauensanker und deren Einsatz innerhalb des SGD-Protokolls zu finden.

Alle in *rot* hervorgehobenen Objekte und Bereiche bilden Vertrauensanker und sind für die Sicherheit bzw. Vertraulichkeit der Dokumente elementar. Dies beinhaltet vorwiegend die für das SGD-Protokoll relevanten kryptographischen Schlüssel, auch aber den *Akten- und Kontextschlüssel*, den *verschlüsselten Aktenschlüssel* und den *verschlüsselten Dokumentenschlüssel*.

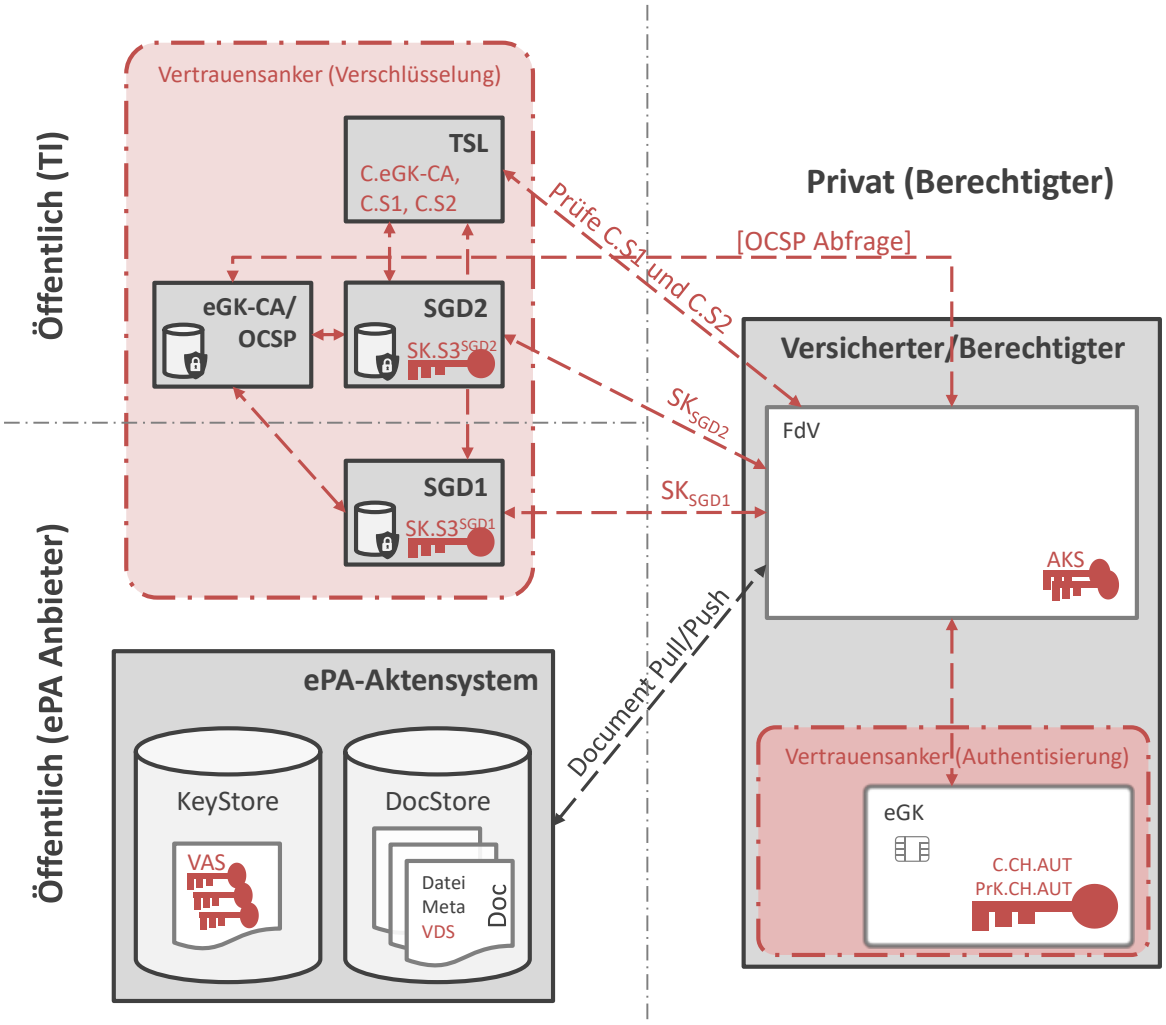


Abbildung 6: Simplifizierte Repräsentation der Vertrauensanker beim SGD-Protokoll.

Bedeutung der Variablen und Abkürzungen:

- **AKS:** Akten- und KontextSchlüssel
- **VAS:** Verschlüsselter AktenSchlüssel
- **VDS:** Verschlüsselter DokumentenSchlüssel
- **Datei:** Verschlüsselte Dokumentendatei
- **Meta:** Verschlüsselte Metadaten zur Dokumentendatei
- **$SK.S3_{SGDx}$:** Ableitungsschlüssel des SGDx
- **C.CH.AUT:** Kartenbesitzerzertifikat der eGK (ausgestellt von der PKI der TI)
- **C.Sx:** Schlüsselbestätigungszertifikat des SGDx (ausgestellt von der PKI der TI)

7.3.4.3 Handshake und Sitzungsschlüsselableitung

Nachfolgend, in Abbildung 7, ist eine vereinfachte Darstellung der Authentifizierung und Schlüsselableitung zwischen dem Client (FdV) und den SGDs als Sequenzdiagramm dargestellt. Diese Darstellung legt den Fokus auf die kryptographisch relevanten Aspekte eben dieser, und kombiniert aufgrund der leichteren Verständlichkeit und der besseren

Übersichtlichkeit die beiden SGDs auf einen “Teilnehmer”. Da der Client mit beiden SGDs den selben Protokollablauf vollzieht, ist dies zur Betrachtung des Handshakes hier nicht relevant.

Bei diesem Handshake handelt es sich um einen gegenseitig authentifizierten Key Exchange auf Basis von ECDH-ECIES.

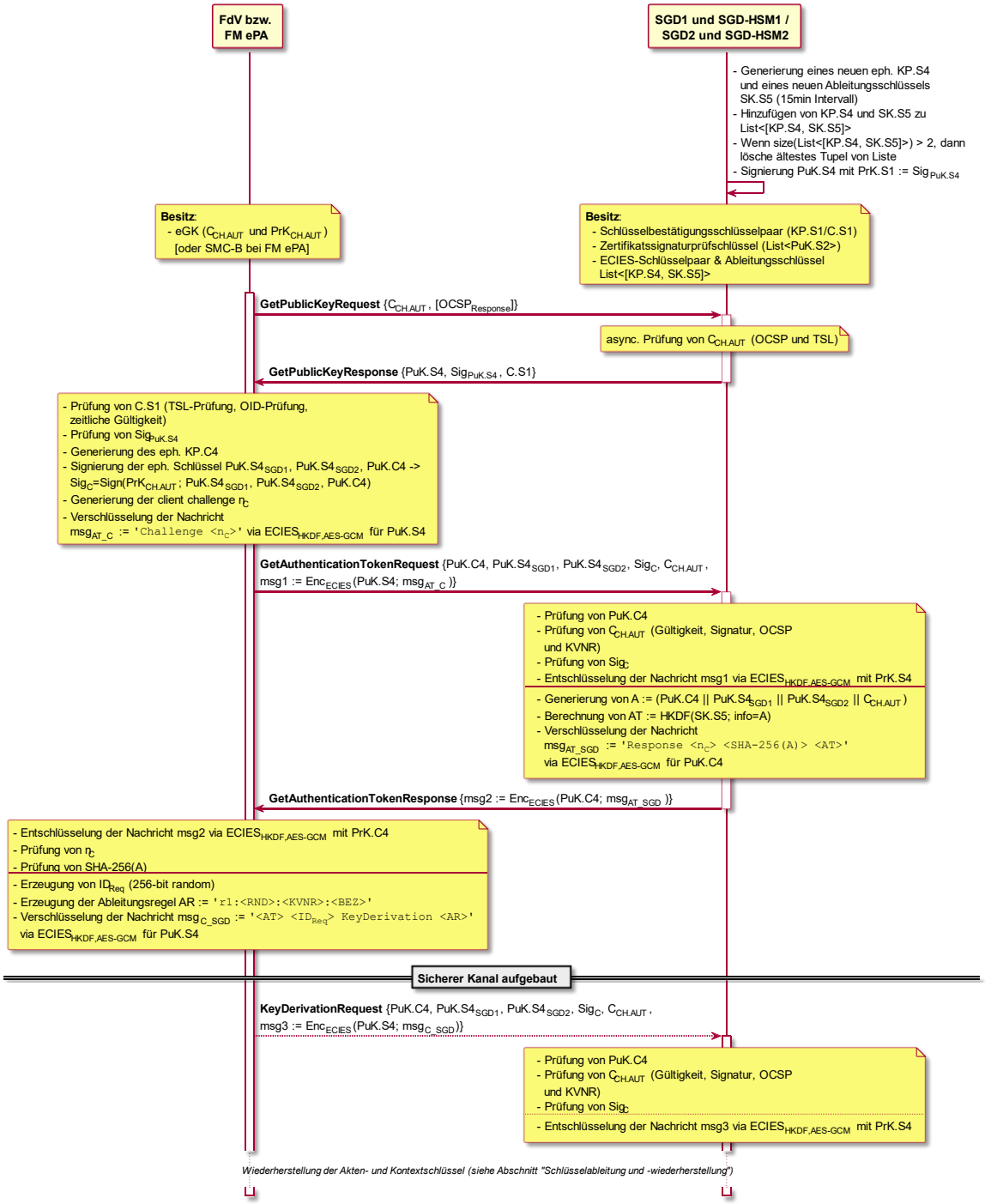


Abbildung 7: Sequenzdiagramm der simplifizierten Client-SGD-Authentifizierung.

7.3.4.4 Schlüsselableitung und -wiederherstellung

Eine vereinfachte Darstellung mit dem Fokus auf die kryptographisch relevanten Aspekte der Schlüsselableitung und -wiederherstellung zwischen dem Client (FdV) und den SGDs ist nachfolgend in Abbildung 8 illustriert.

Bei dem in diesem Sequenzdiagramm dargestellten Protokollablauf gibt es zu Beginn des Ablaufs eine Überschneidung mit dem Ende des Ablaufs in Abbildung 7, da dieser nahtlos an den Handshake mit Sitzungsschlüsselableitung anschließt.

Im Kasten *Verschlüsselung im "Zwiebelschalenprinzip"* in der Abbildung 8 ist das Zusammenspiel bzw. die Verwendung der relevantesten symmetrischen Schlüssel, die Akten- und Kontextschlüssel (AKS) und Schlüsselverschlüsselungsssschlüssel (SK_{SGD1} und SK_{SGD2}), am FdV dargestellt. Diese sicher hinterlegen und erneut abholen zu können ist der Fokus des ganzen SGD-Protokolls. Hier ist deutlich zu erkennen, dass die Akten- und Kontextschlüssel im Zwiebelschalenprinzip verschlüsselt im *AuthorizationKey* resultieren.

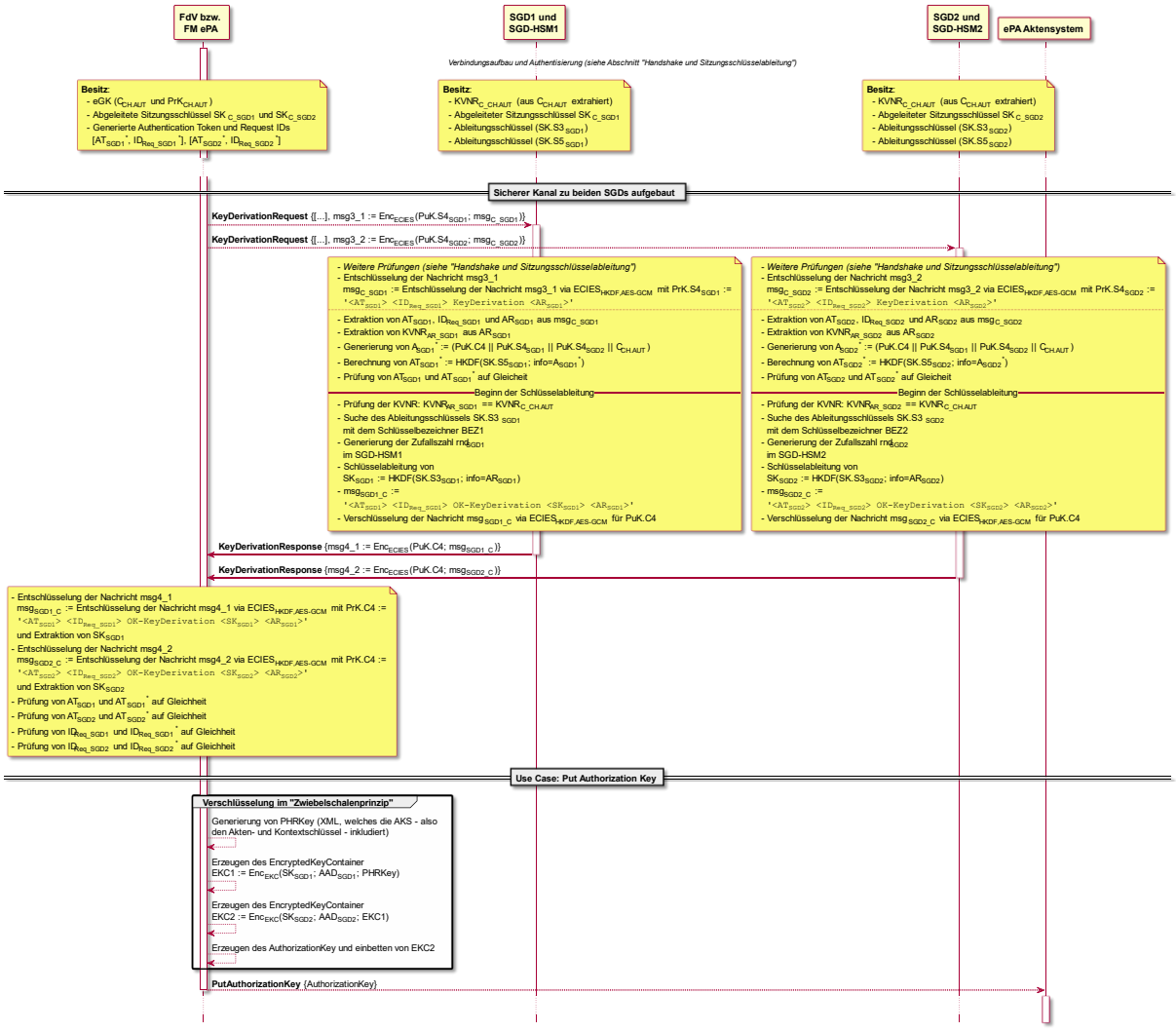


Abbildung 8: Sequenzdiagramm der simplifizierten Client-SGD-Schlüsselableitung.

7.3.4.5 Abgeleitete Sicherheitsaspekte des Protokolls

7.3.4.5.1 Schlüsselableitung

Für die Schlüsselableitung wird innerhalb des SGD-Protokolls die Funktion HKDF (siehe Abschnitt 7.3.2) verwendet. Die konkrete Verwendung im Rahmen des SGD-Protokolls führt zu einem hohen Sicherheitslevel, da sowohl der primäre als auch der sekundäre Input in die HKDF, d. h. sowohl *IKM* als auch *info*, durch den hochwertigen Zufallszahlengenerator eines nach FIPS 140-2 mind. Level 3 zertifizierten HSM generiert bzw. mitbestimmt werden. Die Erzeugung des *IKM* ist zufällig und darüber hinaus wird dieser alle sechs Monate neu im HSM generiert. Ebenso beinhaltet der Input *info* als zentrale Komponente eine Zufallszahl RND, welche ebenso im HSM generiert wird.

Die Schlüsselableitung kann daher unter den Annahmen dieser Analyse als sicher bewertet werden.

7.3.4.5.2 Verschlüsselung des AuthorizationKeys

Die Verschlüsselung der *AuthorizationKeys* findet unter Verwendung von State-of-the-Art-Kryptographie statt, hier wird der Algorithmus *Advanced Encryption Standard* (AES) gemäß FIPS-197 im Galois/Counter Mode (GCM) eingesetzt. Damit AES-GCM seine Sicherheitseigenschaften erfüllen kann, ist die korrekte Generierung und Verwendung des Initialisierungsvektors (IVs), die Länge des *Authentication Tags* und die Schlüsselgenerierung wesentlich.

Die IV-Generierung hierbei findet zufällig statt und hat eine fixe Bitlänge von 96 Bit. Gemäß NIST Kapitel 8.3 [6] ist die maximale Anzahl an Verschlüsselungsoperationen mit dem selben Schlüssel unter Verwendung eines 96-Bit-Random-IVs auf 2^{32} Operationen begrenzt.

Da hier mit den beiden Schlüsselverschlüsselungsschlüsseln (SK_{SGD1} und SK_{SGD2}) im Wesentlichen nur zwei Verschlüsselungsoperationen durchgeführt werden – nämlich die Verschlüsselung des Akten- und Kontextschlüssels – stellt diese Limitierung hierbei kein Problem in Bezug auf die maximale Anzahl an Verschlüsselungsoperationen mit dem selben Schlüssel dar.

7.3.4.5.3 Verschlüsselung des Dokumentenschlüssels

Die Verschlüsselung des Dokumentenschlüssels, welcher für jedes Dokument neu erzeugt und verschlüsselt wird, wird ebenso mit AES-GCM mit Random-IV durchgeführt. Hierbei könnte jedoch rein theoretisch durch die Anzahl an Dokumenten, dieses Limit überschritten werden. Dadurch wird die Wahrscheinlichkeit für eine IV-Kollision erhöht und AES-GCM verliert seine Sicherheit. Dies würde die Integrität des Dokumentenschlüssels gefährden.

Empfehlung 5

Einsatz eines Monitorings auf Thresholds für die Anlage von Dokumenten in ePA

Bei der von uns angenommenen Anwendung, nämlich dem Verschlüsseln ärztlicher Dokumente, gehen wir jedoch nicht davon aus, diese Anzahl in der Praxis im Normalfall nur

annähernd zu erreichen, noch kann dies durch einen Angreifer realistisch ohne auffallen zu können erzwungen werden. Dies impliziert, dass von der gematik Anforderungen an ein Monitoring durch einen Betreiber eines ePA-Systems gestellt werden, welche Thresholds für das Anlegen von Dokumenten – generell, sowie in zeitlichem Rahmen – definieren: Es muss durch den Betreiber eines ePA-Systems kontrolliert werden, dass nicht mehr als 2^{32} Dokumente abgelegt werden. Unter diesen Voraussetzungen gehen wir davon aus, dass den aktuellen Empfehlungen, sowohl aus NIST SP 800-38D [6] als auch aus BSI TR-02102-1 [7], entsprochen wird.

Die Verwendung eines Ableitungsschlüssels `SK.S3` im SGD-HSM ist laut gematik Spezifikationen auf maximal ein halbes Jahr beschränkt. Dies bedeutet jedoch nur, dass in diesem Zeitraum ein und derselbe Ableitungsschlüssel in einem SGD-HSM verwendet wird, um **neue** Schlüsselableitungsschlüssel für **neue** Akten zu erzeugen. Es bedeutet jedoch nicht, dass die Schlüsselableitungsschlüssel eine maximale Lebensdauer von sechs Monaten besitzen und danach getauscht werden.

Empfehlung 6

> *Tausch symmetrischer Schlüssel berücksichtigten*

Es ist weder eine Umschlüsselung der Schlüsselableitungsschlüssel noch eine Umschlüsselung der Akten- und Kontextschlüssel spezifiziert. Dies hat zur Folge, dass laut derzeitigem Spezifikationsstand diese Schlüssel einmalig beim Anlegen einer Akte – wovon es pro Versichertem nur eine gibt – generiert werden und solange die Akte existiert diese Schlüssel unverändert bleiben. Eine derartige Langzeitverwendung von den gleichen symmetrischen Schlüsseln ist problematisch, da es Best Practice ist, dass Schlüssel austauschbar sind.

Die Wahl der Länge des *Authentication Tags* ist hinreichend. Ebenso ist die Wahl der resultierenden AES-Schlüssellänge, d. h. 256-Bit AES-Schlüssel eine Zukunftssichere.

7.3.4.5.4 Sicherer Kanal zwischen Client und SGD-HSM

Die Kommunikation zwischen Client und SGD-HSM wird mit einer effizienten ad-hoc Protokollkonstruktion abgesichert. Bestandteil dieser ad-hoc Konstruktion ist das IND-CCA2 sichere ECIES Verschlüsselungsverfahren. Die formal bestätigten Sicherheitseigenschaften (ciphertext indistinguishability against adaptively chosen ciphertext attack) des ECIES Verfahrens alleine sind dabei nicht ausreichend, um die für die Anwendung notwendigen Sicherheitseigenschaften in der Kommunikation zwischen Client und SGD-HSM zu erreichen, und das ECIES Verfahren wird erweitert mittels Signaturen und per HKDF abgeleiteten Authentication Token, etc., um gegenseitige Authentifizierung zwischen Client und SGD-HSM sicherzustellen. Um Gewissheit über die Sicherheit dieser Konstruktion zu erlangen, empfiehlt es sich (und ist es Best Practice), die für die Anwendung notwendigen Sicherheitseigenschaften dieser Konstruktion formal zu beweisen (und dabei gegebenenfalls im Sinne eines proof-driven designs die Konstruktion in einer der nächsten Versionen der Spezifikation derart zu erweitern bzw. zu modifizieren, sodass die Beweisbarkeit möglich wird).

Empfehlung 7

> *Formale Beweisbarkeit der notwendigen Sicherheitseigenschaften an die Kommunikation Client mit SGD-HSM erwirken.*

Es sei noch einmal darauf hingewiesen, dass die formal bestätigten Sicherheitseigenschaften des ECIES Protokolls alleine nicht ausreichend sind, um die für die Anwendung notwendigen Sicherheitseigenschaften zu erreichen (dies kann man leicht sehen, in dem man etwa Idendity Misbinding Angriffe auf Basis eines mit ECIES inkorrekt abgesicherten Kommunikationskanals als Gegenbeispiel konstruiert). Für einen sicheren Kanal zur Kommunikation zwischen Client und Server haben sich in der Wissenschaft formale Modelle etabliert, die gut auf die Anforderungen der vorliegenden Anwendung zu passen scheinen: Das der Anwendung zugrundeliegende Protokoll lässt sich als Secure Channel [8] modellieren, und folglich der Aufbau dieses sicheren Kanals unter einem der üblichen Modelle eines Authenticated Key Exchanges formaliseren. Andere Ansätze um die Beweisbarkeit der tatsächlich notwendigen Sicherheitseigenschaften zu erlangen sind auch denkbar, die vorgeschlagene Vorgangsweise erscheint dem Gutachter aber am zielführendsten, da hier auf passende in der Literatur etablierte Modelle und Beweistechniken zurückgegriffen werden kann. Mittels eines solchen formalen Beweises kann Gewissheit über die Sicherheit des Protokolls bezüglich einer Reihe von praktischen relevanten Angriffen gewonnen werden. Unter der Perspektive einer solchen formalen Beweisbarkeit erfolgt die weitere Analyse.

Zum Aufbau des verschlüsselten und beidseitig authentifizierten sicheren Kanals zwischen SGD-HSM und Client wird mittels ECIES-Verfahren ein Authenticated Key Exchange (AKE) Protokoll auf Basis von ECDH realisiert (mittels der Messages `GetPublicKeyResponse`, `GetAuthenticationTokenRequest`, `GetAuthenticationTokenResponse`). Das Protokoll ist dabei auf Seiten des SGD-HSMs stateless. Um trotzdem auf die im AKE-Protokoll erfolgreiche Client-Authentifizierung durch den SGD-HSMs zurückgreifen zu können, generiert der SGD-HSM ein symmetrisch signiertes *AuthenticationToken*. Außerdem muss das im ECDH-Exchange abgeleitete Secret im Anschluss an den Authenticated Key Exchange für jeden Nachrichtenaustausch des sicheren Kanals vom SGD-HSM wieder neu berechnet werden. Der abgeleitete Session-Schlüssel rotiert dabei mit jeder Nachricht, da immer ein neuer ephemeral Sender-Schlüssel durch das ECIES-Verfahren in die Ableitung miteinfließt (So ein Mechanismus ist als 'ratcheting' [15] bekannt und kann eine starke Form von Forward Secrecy garantieren)

Unter dieser Betrachtungsweise halten die Gutachter folgende Punkte für überarbeitungswürdig:

Empfehlung 8

> *AKE-Protokoll macht unnötig starke Annahmen über die Sicherheit der CA: Anpassung Protokoll*

- Das AKE-Protokoll macht unnötig starke Annahmen über die Sicherheit der CA: Das Protokoll ist nur sicher gegen *Unknown Key Share Attacks*, wenn die CA beim Signieren eines Certificate Signing Requests (CSR) für ein SGD-HSM Zertifikat (`C.S1`) einen Nachweis über Besitz des zugehörigen privaten Schlüssels verlangt. Dies ist zwar Best Practice, wird aber oft in der Realität nicht eingehalten. Diese zusätzliche Abhängigkeit an die Anforderung an die CA über den Nachweis des Besitzes des privaten Schlüssels eines CSRs macht das Gesamtsystem unnötig fragiler: Mehr Annahmen an ein Protokoll impliziert üblicher Weise, dass es mehr Angriffsoberfläche gibt. Die Robustheit gegen diesen Angriff könnte ein durch minimale Modifikationen verändertes AKE-Protokoll ohne bemerkbaren Effizienzverlust erreichen. Aufgrund der minimal notwendigen Anpassungen des Protokolls sind daher im Sinne eines “multlilayered defense” jedenfalls Maßnahmen auch dann empfehlenswert, wenn diese zusätzlichen

Anforderungen an die PKI gemacht (und überprüft und getestet) werden. Dies erfolgt derzeit nach Abstimmung mit gematik über Verträge mit dem Betreiber.

7.3.5 VAU

7.3.5.1 Allgemeines

Das VAU-Protokoll wurde von gematik sehr einfach gehalten und auf das erforderliche Ausmaß reduziert, im Wesentlichen handelt es sich um eine simplifizierte Variante des TLS-Protokolls. Daraus resultiert ein klarer Ablauf des Protokolls, in dem keine optionalen Zwischenschritte vorhanden sind (siehe Abbildung 9). Durch dieses Design wird sichergestellt, dass es nicht möglich ist, wichtige und erforderliche Schritte im Aufbau eines sicheren Kommunikationskanals auszulassen, um dadurch die Sicherheit dessen zu schwächen[11]. Ein weiterer Sicherheitsvorteil ist, dass von gematik lediglich eine Cipher-Suite spezifiziert ist, welche nach BSI_TR-02102-2 [12] als ausreichend sicher zu erachten ist. Dadurch werden auch sogenannte Downgrade-Angriffe auf schwächere Algorithmen unterbunden[13].

Bei der Vereinfachung des TLS-Protokolls wurden erforderliche Sicherheitsmechanismen nicht umgesetzt. Dies ermöglicht gezielte Angriffe wie *Identity Misbinding* (siehe Abschnitt 7.3.5.2) beziehungsweise führt zu Schwächen durch *unsachgemäße Verwendung des IV in AES-GCM* (siehe Abschnitt 7.3.5.3). Auch wird die Verwendung des selben AES-Schlüssels für Nachrichten in beide Richtungen aus Sicherheitssicht von den Gutachtern nicht empfohlen.

Nachfolgend, in Abbildung 9, ist eine vereinfachte Darstellung des VAU-Protokolls mit dem Fokus auf die kryptographisch relevanten Aspekte des Protokolls zwischen dem Client (FdV) und der *vertrauenswürdigen Ausführungsumgebung* (VAU) illustriert.

Die rot markierten Stellen im Sequenzdiagramm des VAU-Protokolls sind von den Gutachtern empfohlene Änderungen, welche erforderlich sind, um den in Abschnitt 8 zu Anforderung A_16952 vorgestellten Sicherheitsfehler zu beheben.

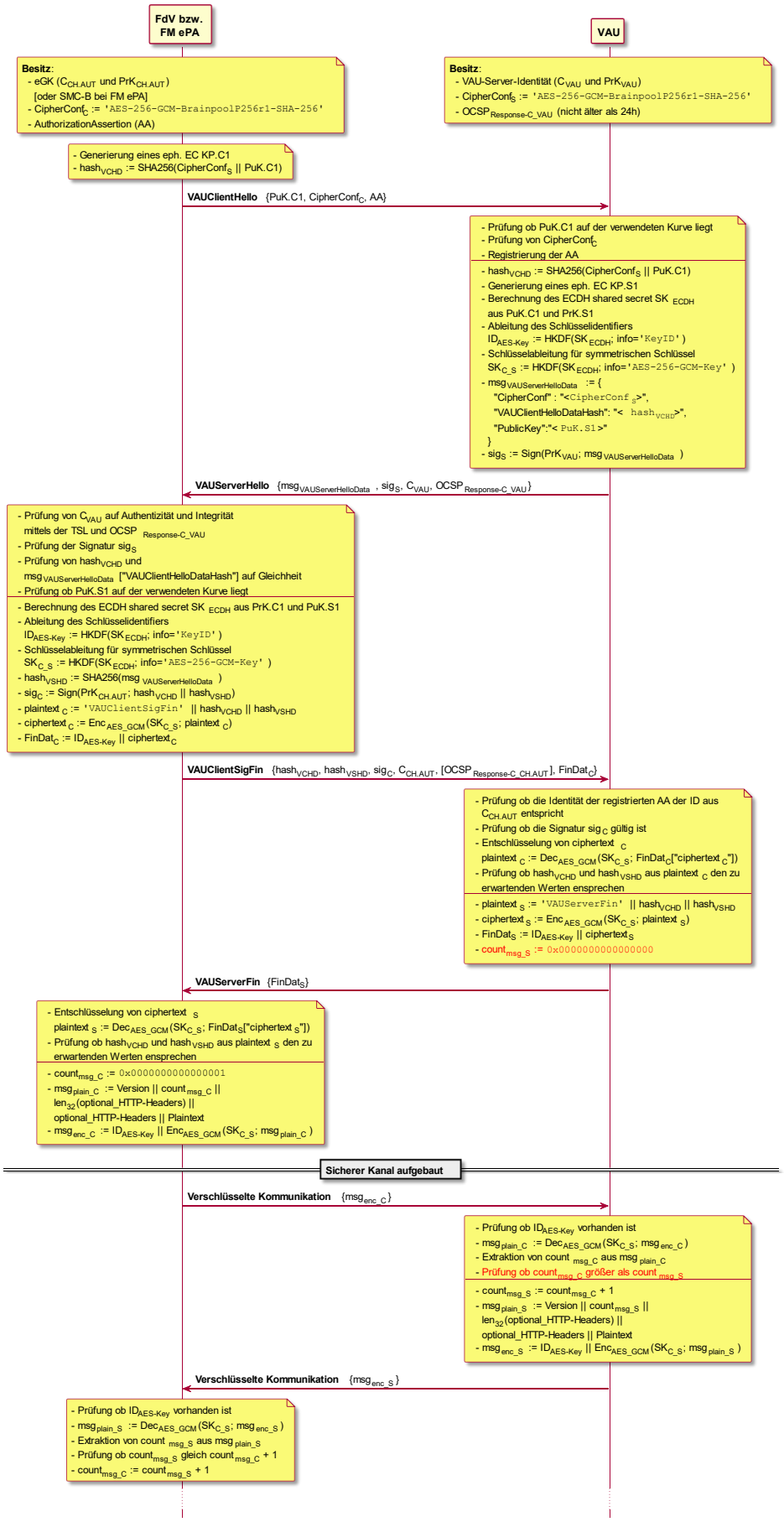

FdV bzw. FM ePA
VAU
Besitz:
- eGK ($C_{CH.AUT}$ und $PrK_{CH.AUT}$)
[oder SMC-B bei FM ePA]
- $CipherConf_C$:= 'AES-256-GCM-BrainpoolP256r1-SHA-256'
- AuthorizationAssertion (AA)
Besitz:
- VAU-Server-Identität (C_{VAU} und PrK_{VAU})
- $CipherConf_S$:= 'AES-256-GCM-BrainpoolP256r1-SHA-256'
- $OCSP_{Response-C\_VAU}$ (nicht älter als 24h)
- Generierung eines eph. EC KP.C1
- $hash_{VCHD}$:= SHA256($CipherConf_S$ || PuK.C1)
VAUClientHello {PuK.C1, $CipherConf_C$, AA}
- Prüfung ob PuK.C1 auf der verwendeten Kurve liegt
- Prüfung von $CipherConf_C$
- Registrierung der AA
- $hash_{VCHD}$:= SHA256($CipherConf_S$ || PuK.C1)
- Generierung eines eph. EC KP.S1
- Berechnung des ECDH shared secret SK_{ECDH} aus PuK.C1 und PrK.S1
- Ableitung des Schlüsselidentifiers $ID_{AES-Key}$:= HKDF(SK_{ECDH}; info='KeyID')
- Schlüsselableitung für symmetrischen Schlüssel SK_{C_S} := HKDF(SK_{ECDH}; info='AES-256-GCM-Key')
- $msg_{VAUServerHelloData}$:= { "CipherConf" : "<$CipherConf_S$>", "VAUClientHelloDataHash": "< $hash_{VCHD}$>", "PublicKey":"< PuK.S1>" }
- sig_S := Sign(PrK_{VAU}; $msg_{VAUServerHelloData}$)
VAUServerHello {$msg_{VAUServerHelloData}$, sig_S, C_{VAU}, $OCSP_{Response-C\_VAU}$}
- Prüfung von C_{VAU} auf Authentizität und Integrität mittels der TSL und $OCSP_{Response-C\_VAU}$
- Prüfung der Signatur sig_S
- Prüfung von $hash_{VCHD}$ und $msg_{VAUServerHelloData}$ ["VAUClientHelloDataHash"] auf Gleichheit
- Prüfung ob PuK.S1 auf der verwendeten Kurve liegt
- Berechnung des ECDH shared secret SK_{ECDH} aus PrK.C1 und PuK.S1
- Ableitung des Schlüsselidentifiers $ID_{AES-Key}$:= HKDF(SK_{ECDH}; info='KeyID')
- Schlüsselableitung für symmetrischen Schlüssel SK_{C_S} := HKDF(SK_{ECDH}; info='AES-256-GCM-Key')
- $hash_{VSHD}$:= SHA256($msg_{VAUServerHelloData}$)
- sig_C := Sign($PrK_{CH.AUT}$; $hash_{VCHD}$ || $hash_{VSHD}$)
- $plaintext_C$:= 'VAUClientSigFin' || $hash_{VCHD}$ || $hash_{VSHD}$
- $ciphertext_C$:= Enc_{AES_GCM}(SK_{C_S}; $plaintext_C$)
- $FinDat_C$:= $ID_{AES-Key}$ || $ciphertext_C$
VAUClientSigFin {$hash_{VCHD}$, $hash_{VSHD}$, sig_C, $C_{CH.AUT}$, [$OCSP_{Response-C\_CH.AUT}$], $FinDat_C$}
- Prüfung ob die Identität der registrierten AA der ID aus $C_{CH.AUT}$ entspricht
- Prüfung ob die Signatur sig_C gültig ist
- Entschlüsselung von $ciphertext_C$ $plaintext_C$:= Dec_{AES_GCM}(SK_{C_S}; $FinDat_C$["$ciphertext_C$"])
- Prüfung ob $hash_{VCHD}$ und $hash_{VSHD}$ aus $plaintext_C$ den zu erwartenden Werten ensprechen
- $plaintext_S$:= 'VAUServerFin' || $hash_{VCHD}$ || $hash_{VSHD}$
- $ciphertext_S$:= Enc_{AES_GCM}(SK_{C_S}; $plaintext_S$)
- $FinDat_S$:= $ID_{AES-Key}$ || $ciphertext_S$
- $count_{msg\_S}$:= 0x0000000000000000
VAUServerFin {$FinDat_S$}
- Entschlüsselung von $ciphertext_S$ $plaintext_S$:= Dec_{AES_GCM}(SK_{C_S}; $FinDat_S$["$ciphertext_S$"])
- Prüfung ob $hash_{VCHD}$ und $hash_{VSHD}$ aus $plaintext_S$ den zu erwartenden Werten ensprechen
- $count_{msg\_C}$:= 0x0000000000000001
- msg_{plain_C} := Version || $count_{msg\_C}$ || len_{32}(optional_HTTP-Headers) || optional_HTTP-Headers || Plaintext
- msg_{enc_C} := $ID_{AES-Key}$ || Enc_{AES_GCM}(SK_{C_S}; msg_{plain_C})
Sicherer Kanal aufgebaut
Verschlüsselte Kommunikation {msg_{enc_C}}
- Prüfung ob $ID_{AES-Key}$ vorhanden ist
- msg_{plain_C} := Dec_{AES_GCM}(SK_{C_S}; msg_{enc_C})
- Extraktion von $count_{msg\_C}$ aus msg_{plain_C}
- Prüfung ob $count_{msg\_C}$ größer als $count_{msg\_S}$
- $count_{msg\_S}$:= $count_{msg\_C}$ + 1
- msg_{plain_S} := Version || $count_{msg\_S}$ || len_{32}(optional_HTTP-Headers) || optional_HTTP-Headers || Plaintext
- msg_{enc_S} := $ID_{AES-Key}$ || Enc_{AES_GCM}(SK_{C_S}; msg_{plain_S})
Verschlüsselte Kommunikation {msg_{enc_S}}
- Prüfung ob $ID_{AES-Key}$ vorhanden ist
- msg_{plain_S} := Dec_{AES_GCM}(SK_{C_S}; msg_{enc_S})
- Extraktion von $count_{msg\_S}$ aus msg_{plain_S}
- Prüfung ob $count_{msg\_S}$ gleich $count_{msg\_C}$ + 1
- $count_{msg\_C}$:= $count_{msg\_S}$ + 1

Abbildung 9: VAU-Protokoll

7.3.5.2 Schwachstelle im VAU-Protokoll: Identity Misbinding

Schwachstelle 2

Identity Misbinding im VAU-Protokoll

Das VAU-Protokoll ist nach Analyse der Gutachter verwundbar für Identity-Misbinding-Angriffe. Diese sind in beide Richtungen möglich, das bedeutet, es ist möglich die Identität eines Servers oder Clients auszutauschen. Im Falle eines Tausches der Server-Identität, glaubt ein Client (FdV bzw. FM ePA) er kommuniziert z.B. mit Server 1 (VAU), obwohl er mit Server 2 kommuniziert. Auch ist es möglich die Identität eines Clients auszutauschen und somit dem Server eine andere Identität vorzuspielen.

Um die Identität des Servers auszutauschen, reicht es wie in Abbildung 10 dargestellt aus, dass der Angreifer (z.B. Mallory) die richtige `VAUServerHello` Nachricht abfängt und die Signatur sowie das Zertifikat austauscht und die neue Nachricht an den Client sendet.

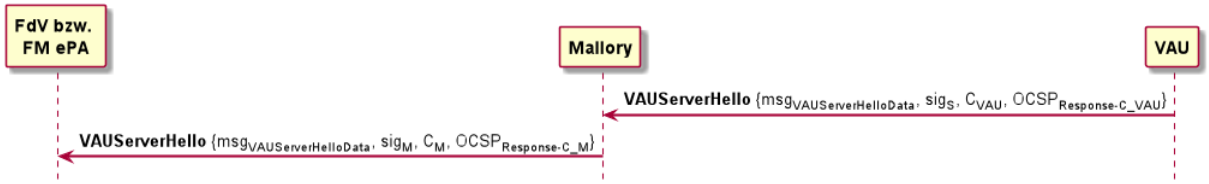
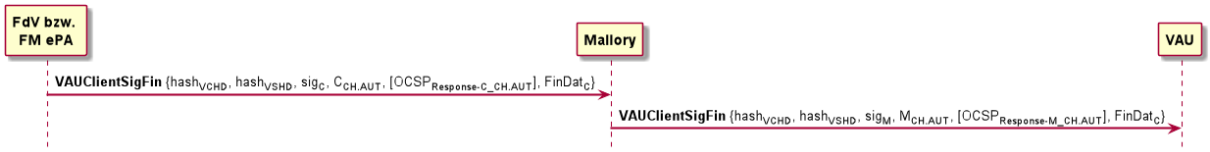


Abbildung 10: Identity Misbinding Server

Wenn die Identität des Clients getauscht werden soll, so wie Abbildung 11 illustriert, so muss das Zertifikat und die Signatur der `VAUClientSigFin` Nachricht ausgetauscht werden. Dies hat zur Folge, dass ein Client den falschen Verarbeitungskontext übergeben bekommt, nämlich den des Angreifers Mallory.



Abbil dung 11: Identity Misbinding Client

Für diese Angriffe sind eine valide eGK oder eine VAU-Server-Identität, welche in der TSL hinterlegt ist, erforderlich.

***Behebung**: Mit Release 3.1.3 ist die Schwachstelle 'Identity Misbinding im VAU-Protokoll' erfolgreich behoben.*

7.3.5.3 Schwachstelle im VAU-Protokoll: Initialization Vector mit AES-GCM

Schwachstelle 3

Generierung des Initialization Vectors mit AES-GCM

Die Generierung des Initialization Vectors mittels Zufall ist nach NIST Abschnitt 8.3 [6] nur bis 2^{32} Aufrufe pro Schlüssel erlaubt. Da im VAU-Protokoll bis zu 2^{64} Nachrichten mit dem

selben Schlüssel unterstützt werden, ist diese Anforderung nicht mehr erfüllt. Für die Unterstützung von mehr als 2^{32} Operationen schreibt [6] einen deterministischen IV mit 96-Bit Länge vor. Dadurch wird die Wahrscheinlichkeit für eine IV-Kollision erhöht und AES-GCM verliert seine Sicherheit. Dies würde die Integrität der über das VAU-Protokoll übertragenden Daten gefährden.

Des Weiteren darf die Wahrscheinlichkeit, dass ein und derselbe IV für einen Schlüssel zweimal verwendet wird, nicht größer als 2^{-32} sein (siehe [6]). Bei einem zufälligen IV der Länge 96-Bit und 2^{64} Nachrichten ist diese Anforderung ebenfalls nicht erfüllt. Denn die Wahrscheinlichkeit, dass zweimal der selbe IV, aus der Menge ($N = 2^{96}$) der Möglichen, bei `k`-Ziehungen gezogen wird ist:

$$1 - 1(\frac{N-1}{N})(\frac{N-1}{N})\dots(\frac{N-k+1}{N}) = 1 - \prod_{i=1}^{k-1}(1 - \frac{i}{N})$$

Diese Wahrscheinlichkeit lässt sich mit

$$1 - x \leq e^{-x}$$

auf

$$1 - \prod_{i=1}^{k-1}(1 - \frac{i}{N}) \geq 1 - \prod_{i=1}^{k-1}(e^{-\frac{i}{N}}) = 1 - e^{-\frac{1}{N}\sum_{i=1}^{k-1} i} \geq 1 - e^{-\frac{k^2}{2N}}$$

vereinfachen bzw. reduzieren. Dieses Ergebnis setzten wir nun mit der oben dargestellten Anforderung von [6], dass die Wahrscheinlichkeit höchstens 2^{-32} betragen darf, gleich.

$$1 - e^{-\frac{k^2}{2N}} = \frac{1}{2^{32}} \Rightarrow -\frac{k^2}{2N} = ln(1 - \frac{1}{2^{32}}) \Rightarrow k = \sqrt{N}\sqrt{-2 * ln(1 - \frac{1}{2^{32}})}$$

Wir können nun `k` folgendermaßen einschränken:

$$2^{32} < k < 2^{33}$$

Somit liegt die maximale Anzahl der erlaubten Nachrichten (äquivalent zu Generierungen von perfekt zufälligen IVs) zwischen 2^{32} und 2^{33}. Dies deckt sich auch mit der Anforderung aus Abschnitt 8.3 [6]. Daraus folgt, dass wenn zufällige IVs verwendet werden wollen, sich der Verschlüsselungsschlüssel mindestens alle 2^{32} Nachrichten ändern muss. Im VAU-Protokoll wird der selbe Verschlüsselungsschlüssel für bis zu 2^{64} Nachrichten verwendet und das in Kombination mit einem zufälligem IV, was der NIST-Spezifikation [6] widerspricht.

Behebung: Mit den Änderungen im Release 3.1.3 wurde die Schwachstelle behoben.

Empfehlung 9

Ersetzung zufällige IV-Generierung durch garantiert eindeutigen IV

Die Gutachter empfehlen, dass anstatt der zufälligen IV-Generierung ein IV auf Basis des vorhandenen garantiert eindeutigen 64-Bit Nachrichtenzählers $count_{msg}$, welcher im VAU-Protokoll im Payload jeder Nachricht gesetzt wird, verwendet wird. Die NIST-Spezifikation [6]

sieht in Abschnitt 8.2.1, *IV Constructions: Deterministic Construction*, exakt einen 64-Bit Nachrichtenzähler mit einem vorangestellten 32-Bit *fixed field* (z.B. Richtungsanzeiger) vor, was zu einem deterministischen IV mit 96-Bit Länge führt. Diese Lösung ist dann für die Verwendung von bis zu 2^{64} Nachrichten geeignet.

***Behebung**:* Mit den Änderungen im Release 3.1.3 (A_16943-01, A_16945-01) ist eine Mehrfachverwendung desselben IVs auch bei bis zu 2^64^ Nachrichten ausgeschlossen.

7.3.6 Schwachstellen im Systemkontext

Wenn ein Angreifer die Möglichkeit besitzt, die TLS-Verbindung zwischen Nutzer und TI zu kompromittieren, und eine valide eGK besitzt, kann er Identity Misbinding Angriffe durchführen. Ein solcher Angriff setzt sich aus den zwei bereits dargestellten Angriffen zusammen, erstens, er verursacht ein Identity Misbinding in der Authentisierungskomponente und zweitens, ein Identity Misbinding im VAU-Protokoll. Darüber hinaus passt der Angreifer bei der Anfrage für die *AuthorizationKeys* die *DeviceID* und den *RecordIdentifier* an.

Dadurch verwendet der Nutzer den VAU-Kontext des Angreifers, ohne dies zu realisieren. Der Nutzer kann nun Daten in diesem speichern und diese so verwenden als wäre es sein eigener Kontext, zumindest wenn der Angreifer zuvor diese noch nie aufgerufen, d. h. initialisiert, hat. Dies ist ein Verstoß gegen die Integrität.

***Behebung**: Mit Release 3.1.3 wurden beide Schwachstellen behoben.*

8 Mögliche Spezifikationsfehler

Die Gutachter haben die in den referenzierten Spezifikationen (siehe Abschnitt 4.2) dargestellten Sicherheitsanforderungen bewertet. Bei diesen Betrachtungen haben die Gutachter neben den in Abschnitt 7 bereits aufgeführten Problemen noch weitere Fehler wahrgenommen, welche in diesem Abschnitt näher erläutert werden.

8.1 Schutzmaßnahmen gegen XML Signature Wrapping Angriffe

Schwachstelle 4

XML Signature Wrapping Angriffe

Es ist nicht ersichtlich, wie weit Schutzmaßnahmen gegen XML Signature Wrapping (XSW) Angriffe vorgesehen sind. Sowohl AuthenticationAssertion als auch AuthorizationAssertion scheinen ohne zusätzliche Maßnahmen verwundbar zu sein, aber auch die Signatur der Challenge im `LoginCreateTokenRequest`. Manche effektive Gegenmaßnahmen gegen XSW Angriffe, wie etwa FastXPath [14], das insbesondere für die Härtung des `LoginCreateTokenRequests` geeignet scheint, müssten aus Interoperabilitätsgründen über die Spezifikation mandatiert werden.

***Behebung**: Mit Release 3.1.3 ist diese Schwachstelle behoben.*

Empfehlung 10

Evaluierung von Gegenmaßnahmen gegen XSW, die eine Spezifikationsänderung erfordern.

8.2 gemSpec_Krypt / A_16883

Empfehlung 11

Klarstellung zum Aufbau der `VAUClientHello`-Nachricht

In der Anforderung **A_16883** aus *gemSpec_Krypt* wird der Aufbau der `VAUClientHello`-Nachricht folgendermaßen definiert:

```
{
"MessageType" : "VAUClientHello",
"Data"        : "...Base64-kodierte-VAUClientHelloData..."
}
```

In der Anforderung **A_15592** aus *gemSpec_Dokumentenverwaltung* wird definiert, dass die `VAUClientHello`-Nachricht um ein `"Schlüssel-Wert-Paar zur Übermittlung der Authorization Assertion in Base64-Kodierung"` erweitert werden muss, sodass diese folgendermaßen definiert ist:

```
{
"MessageType" : "VAUClientHello",
"Data" : "VAUClientHelloData (Base64-kodiert)",
"Authorization" : "Authorizaton Assertion (Base64-kodiert)"
}
```

Da beide Dokumente, sowohl *gemSpec_Krypt* als auch *gemSpec_Dokumentenverwaltung*, den selben Dokumentenstand vom 02.10.2019 repräsentieren, handelt es sich hier um eine Inkonsistenz, welche von gematik bereinigt werden soll.

***Behebung**: Mit Release 3.1.3 ist diese Inkonsistenz aufgelöst.*

8.3 gemSpec_Krypt / A_16952: Falsche Extraktion des Zählerwerts

Empfehlung 12

Klarstellung Anforderung A_16952

Der zweite Absatz in dieser Anforderung definiert, wie nach der Entschlüsselung der Nachricht mit der Interpretation dieser fortgefahren werden muss. Diese Definition beginnt mit:

```
Falls die Entschlüsselung erfolgreich war, MUSS der Server die erste
n 64-Bit (8 Byte) als Nachrichtenzähler [...] interpretieren und die
se vom folgenden Plaintext entfernen.
```

Die vom Client generierte und gesendete Nachricht `P1` ist jedoch folgendermaßen definiert:

```
P1 = Version (ein Byte mit dem Wert 0x01) ||
     Nachrichtenzähler (unsigned 64-Bit im Big-Endian-Format) ||
     [...]
```

Dies würde fälschlicherweise bedeuten, dass der Server das `Version`-Byte und die ersten sieben MSB vom übertragenen Nachrichtenzähler als Zählerwert extrahiert. Dies würde bei korrekter Implementierung der Zählerwertprüfung dazu führen, dass das Protokoll niemals erfolgreich abgehandelt werden kann.

***Behebung**: Mit Release 3.1.3 ist dieses Problem behoben.*

8.4 gemSpec_Krypt / A_16952: Fehler bei Nachrichtenzähler

Empfehlung 13

Fehler bei Nachrichtenzähler in Anforderung A_16952 beheben

Der zweite Absatz in dieser Anforderung definiert wie nach der Entschlüsselung der Nachricht mit der Interpretation dieser fortgefahren werden muss. Diese Definition endet mit:

```
[...] Der Zählerwert MUSS größer als der letzte auf diese Art empfan
gene Zählerwert (für die aktuelle KeyID) plus 1 sein. (Zähler + 1 wa
r der Zählerwert der Server-Response.)
```

Diese generische Definition ist an dieser Stelle auf diese Art und Weise nicht möglich, da der Server bis zu diesem Zeitpunkt noch nie eine verschlüsselte Server-Response gesendet hat. Darüber hinaus ist die Definition `Zähler + 1 war der Zählerwert der Server-Response` verwirrend und würde dazu führen, dass der Nachrichtenzähler auf Serverseite mit `-1` initialisiert werden müsste. Da es sich beim Nachrichtenzähler um einen unsigned Integer handelt, ist dies aber nicht möglich.

Erstens sollte die Initialisierung des Nachrichtenzählers auf Serverseite hier – äquivalent zu **A_16945** auf Client-Seite – explizit verschriftlicht werden, und dies mit dem Wert `0` (`0x0000000000000000`). Zweitens sollte die Prüfung auf Serverseite simplifiziert bzw. korrigiert werden.

Wenn vorher die Initialisierung des Server-Nachrichtenzählers definiert wird, könnte die Prüfung in etwa das Folgende aussagen und wäre auch bereits beim Empfang der ersten Nachricht korrekt:

```
[...] Der empfangene und extrahierte Zählerwert MUSS größer als der
aktuelle Server-Nachrichtenzähler (für die aktuelle KeyID) sein.
```

***Behebung**: Mit Release 3.1.3 ist dieses Problem behoben.*

8.5 gemSpec_Krypt / A_16901, A_17070 und A_16851: Kodierung der ECDSA-Signatur

Empfehlung 14

Klarstellung der Kodierung er ECDSA-Signatur

In den Anforderungen **A_16901**, **A_17070** und **A_16851**, wobei es sich um die Signaturerstellung und -kodierung für ECDSA-Signaturen bei den `VAU*`-Nachrichten handelt, ist jeweils Folgendes definiert:

```
Eine ECDSA-Signatur im "Signature"-Feld MUSS nach [TR-03111#5.2.2. X
9.62 Format] (inkl. OID "ecdsa-with-Sha256") kodiert sein.
```

In der darin referenzierten Spezifikation *BSI_TR-03111* wird in Abschnitt 5.2.2 das ANSI X9.62 Format zum Kodieren einer ECDSA-Signatur als ASN.1 Struktur wie folgt definiert:

```
ECDSA-Sig-Value ::= SEQUENCE {
  r INTEGER,
  s INTEGER
}
```

Ebenso definiert ist die OID für den angegebenen Algorithmus:

```
ecdsa-with-Sha256 OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecds
a-with-Specified(3) ecdsa-with-Sha256(2)
}
```

Problematischerweise wird weder in der Spezifikation *BSI_TR-03111* noch in *gemSpec_Krypt* die Kombination des Tupels `AlgorithmIdentifier` und `ECDSA-Sig-Value` konkret spezifiziert. Die Struktur für ECDSA Signaturen sollte zumindest ähnlich der Kodierung des öffentlichen Schlüssels im *Hinweis* der Anforderung **A_16883**, welche die ASN.1 Struktur für öffentliche EC Schlüssel definiert, spezifiziert werden.

8.6 Weitere Fehler

Weitere Fehler und Unklarheiten in Spezifikationen, die per se nicht sicherheitskritisch sind, allerdings durch Unklarheiten gegebenenfalls (Sicherheits-)Probleme verursachen können, sind nachfolgend gelistet. Die Gutachter empfehlen diese ebenfalls zu beheben.

Empfehlung 15

Behebung weiterer Fehler und Unklarheiten

- **gemSpec_Krypt / A_17070:** Die Aussage `"Im "VAUClientServerDataHash"-Feld [...]"` muss auf `"Im "VAUServerHelloDataHash"-Feld [...]"` geändert werden.
- **gemSpec_Krypt / A_16901:** Der Satz `"Der Server MUSS die in der Datenstruktur (VAUServerHello) angegebene Signatur (vgl. A_16901)`

erzeugen (über den Base64-kodieren Wert im "Data"-Feld)" im letzten Absatz sollte umformuliert werden, da er in dieser Form unverständlich ist.

- **gemSpec_Krypt / A_16883:** Um Konsistenz innerhalb des Dokuments zu bewahren und Missverständnissen vorzubeugen sollte in dem Satz "In das Datenfeld "Data" in der folgenden VAUClientHello-Nachricht MUSS er die kodierte VAUClientHelloData-Daten eintragen", ebenso von Base64-kodierte anstatt nur von kodierte die Rede sein.
- **gemSpec_Krypt / A_16852:** In A_16852 ist definiert: "Das dabei erzeugte gemeinsame Geheimnis ist folgend Grundlage von zwei Schlüsselableitungen". Dies sollte, wie an den meisten anderen Stellen in der Spezifikation, um ein Verweis auf **A_16943**, z.B. (vgl. A_16943), ergänzt werden.
- **gemSpec_Krypt / A_16943:** In dieser Anforderung werden die Input-Parameter der HKDF-Funktion nicht konkret definiert:
  - Das zu verwendende IKM (Input Keying Material) wird nicht definiert, hier sollte zumindest ein Verweis auf **A_16852**, z.B. (vgl. A_16852), ergänzt werden.
  - Die beiden genannten Ableitungsvektoren, sollten besser erkennbar als ASCII-String definiert bzw. formatiert werden. Darüber hinaus wird nicht definiert, ob bzw. dass dieser *Ableitungsvektor* als Input info für die HKDF verwendet werden soll.
  - Da in den Anforderungen **A_17070** und **A_17072** auf die sogenannte 256-Bit KeyID referenziert werden, sollte hier die Klarstellung getroffen werden, dass es sich bei dem Ergebnis der ersten Schlüsselableitung (d. h. dem Schlüsselidentifier) weiterführend um die KeyID handelt.
- **gemSpec_Krypt / A_17875:** Die Ableitung des AES-Schlüssels in Schritt 3 ist unterspezifiziert, es wird nicht definiert, wie der info Parameter für die HKDF zu setzen ist.
- **gemSpec_SGD / A_18025**: Im letzten Satz sollte A_18201 wahrscheinlich A_18021 heißen.
- **gemSpec_SGD / 2.3 Basisablauf Kommunikation…:** Im Schritt 6 fehlt die Erwähnung, das dieser analog zu Schritt 3 ist.
- **gemSpec_SGD / A_17896:** Ein Client kann nach A_18021 keine OCSPResponse mehr mitgeben.
- **gemSpec_SGD / A_18021:** Punkt 2. Die Kodierung und die Signatur... Die Signaturprüfung wird weder in A_17900 noch A_17901 beschrieben.
- **gemSpec_SGD / A_18026:** Generierung von A ist unterspezifiziert [...] Das SGD-HSM MUSS die Zeichenkette A als Aneinanderführung [...]:
  - Was ist mit signierten Client-ECIES Schlüssel gemeint?
  - Wie sollte das Client-AUT-Zertifikat codiert sein?
- **gemSpec_SGD / A_18030:** Im vorletzten Absatz sollte Anfangswert klarer formuliert werden, sprich, dass das gesamte AT Token gemeint wird.
- **gemSpec_SGD / A_18024:** In Punkt 3. Ist das erhaltene Zertifikat zeitlich gültig hier fehlt die Gültigkeitsdauer (15min).
- **gemSpec_SGD / Tabelle 4:** Zwischen Schritt 11 und 11.3 sollte s[1] auf ungleich "" (leere Zeichenkette) geprüft werden.
- **gemSpec_SGD / Tabelle 4:** Zwischen Schritt 12 und 12.7 sollte s[2] auf ungleich "" (leere Zeichenkette) geprüft werden.

9 Conclusio

Die gematik spezifiziert mit der ePA ein Dokumentenverwaltungssystem mit höchsten Sicherheitszielen: Die Integrität und Vertraulichkeit medizinischer Daten müssen selbst gegenüber Betreibern in der Angreiferrolle bzw. Angreifern, die das ePA-Backend kompromittieren können, erhalten werden.

IT-Sicherheit ist in einem solchen System ein wesentlicher Punkt. Daher hat die gematik eine Sicherheitsanalyse zur Sicherheit der kritischen Komponenten der elektronischen Patientenakte nach §291a SGB V mit dem Fokus auf die VAU und die kryptographische Sicherheitsleistung der SGD beauftragt.

Für die vorliegende Sicherheitsanalyse wurden eine grundlegende Risko- und Bedrohungsanalyse durchgeführt, um wesentliche Risiken und Bedrohungen zu finden. Sicherheitsanforderungen sowie -protokolle wurden anschließend analysiert und schlussendlich auf ihre Sicherheitsleistungen analysiert.

Zentrale Maßnahme für die Absicherung der elektronischen Patientenakte ist einerseits eine umfassende kryptographische Architektur auf Basis von Trust-Diversifizierung, sowie zahlreiche weitere technische und organisatorische Maßnahmen, mit denen die Grundlagen für ein System geschaffen werden, das den Sicherheitsanforderungen entspricht.

Die Grundstruktur dieses Systems ist angesichts des spezifizierten Bedrohungsmodells solide und gut durchdacht. Die identifizierten Schwachstellen zeigen, dass bei einigen Details – wie auch zu erwarten bei einem System dieser Komplexität – noch Nachbesserungsbedarf besteht.

Alle Schwachstellen und einige Empfehlungen sind bereits im Release 3.1.3 erfolgreich behoben, bzw. umgesetzt. Diese wurden daher in dieser Sicherheitsanalyse entsprechend markiert.

Bearbeitungszeiträume für Sicherheitsanalysen sind naturgemäß zeitlich begrenzt – Angreifer hingegen haben potenziell unendlich lange Zeit, um Angriffe zu planen und gegebenenfalls durchzuführen. Daher ist es in solchen komplexen Systemen erforderlich regelmäßig Sicherheitsanalysen durchzuführen, auf neue Angriffswege und Analysetechniken zu reagieren und die Sicherheit eines Systems erneut zu bewerten. Dies ist gerade bei einer ePA wichtig. Die Gutachter empfehlen daher, auf der vorliegenden Analyse aufsetzend, weitere ergänzende, umfangreiche Sicherheitsanalysen durchzuführen, um eventuell noch vorhandene Details bzw. Angriffskombinationen erkennen zu können.

10 Bibliografie

[1] gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, „Elektronische Gesundheitskarte und Telematikinfrastruktur – Systemspezifisches Konzept ePA“..

[2] gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, „Elektronische Gesundheitskarte und Telematikinfrastruktur – Spezifikation ePA-Frontend des Versicherten“..

[3] gematik - Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH, „Spezifikation Datenschutz- und Sicherheitsanforderungen der TI an Anbieter“..

[4] H. Krawczyk und P. Eronen, „RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)“. Mai-2010.

[5] E. Rescorla, „RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3“. Aug-2018.

[6] National Institute of Standards and Technology, „NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC“. Nov-2007 [Online]. Verfügbar unter: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[7] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths“, 2019 [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=9

[8] R. Canetti und H. Krawczyk, „Analysis of Key-Exchange Protocols and Their Use for Building Secure Channels“, in *Advances in Cryptology - EUROCRYPT 2001*, Bd. 2045, B. Pfitzmann, Hrsg. Springer Berlin Heidelberg, 2001, S. 453–474 [Online]. Verfügbar unter: http://dx.doi.org/10.1007/3-540-44987-6_28

[9] N. Koblitz und A. J. Menezes, „Another Look at "Provable Security"“, *Journal of Cryptology*, Bd. 20, Nr. 1, S. 3–37, Jän. 2007.

[10] H. Krawczyk, „SIGMA: The ‚SIGn-and-MAc‘ Approach to Authenticated Diffie-Hellman and Its Use in the IKE Protocols“, *Advances in Cryptology - CRYPTO 2003*, Bd. 2729, S. 400–425, 2003.

[11] B. Beurdouche *u. a.*, „A Messy State of the Union: Taming the Composite State Machines of TLS“, in *2015 IEEE Symposium on Security and Privacy*, 2015, S. 535–552.

[12] Bundesamt für Sicherheit in der Informationstechnik, „BSI TR-02102-2: Cryptographic Mechanisms: Recommendations and Key Lengths – Part 2: Use of Transport Layer Security (TLS)“, 2019 [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=9

[13] D. Wagner und B. Schneier, „Analysis of the SSL 3.0 Protocol“, in *Proceedings of the 2Nd Conference on Proceedings of the Second USENIX Workshop on Electronic Commerce*

- *Volume 2*, 1996, S. 4–4 [Online]. Verfügbar unter: http://dl.acm.org/citation.cfm?id=1267167.1267171

[14] S. Gajek, M. Jensen, L. Liao, und J. Schwenk, „Analysis of Signature Wrapping Attacks and Countermeasures“, in *2009 IEEE International Conference on Web Services*, 2009, S. 575–582.

[15] K. Cohn-Gordon, C. Cremers, B. Dowling, L. Garrat und D. Stebila, „A Formal Security Analysis of the Signal Messaging Protocol“, *in Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS&P 2017*, 2017, S. 451–466.