Leistungsbeschreibung

Sektoraler Identity Provider (IDP) und ePA Desktop FdV

Inhalt

Abkürzungsverzeichnis

In dieser Leistungsbeschreibung werden die folgenden Abkürzungen verwendet:

AN	Auftragnehmer
API	Application Programming Interface
BAS	Bundesamt für Soziale Sicherung
BSI	Bundesamt für Sicherheit in der Informationstechnik
ePA	elektronische Patientenakte
ePA-FdV	Frontend des Versicherten
FdV	Frontend des Versicherten
FQDN	Fully Qualified Domain Name
IAM	Identity and Access Management
ITSM	IT Service Management
KVNR	Krankenversichertennummer
LB	Leistungsbeschreibung
PU	Produktionsumgebung
QS	Qualitätssicherung
RCA	root cause analysis
RU	Referenzumgebung
RU DEV	Vorintegrationsumgebung (auch bekannt als RU2)
SDK	Software Development Kit
SLA	Service Level Agreement
TI	Telematik-Infrastruktur
TK	Techniker Krankenkasse
TU	Testumgebung
UI	User Interface
UX	User Experience
VAU	Vertrauenswürdige Ausführungsumgebung

Glossar

In dieser Leistungsbeschreibung werden die folgenden Begriffe unterschieden:

ePA	elektronische Patientenakte als Summe aller gesetzlichen und regulatorischen Anforderungen
ePA Desktop FdV	ePA-FdV für Desktop-Plattformen gemäß [gemSpec_ePA_FdV]
sek. IDP	Sektoraler Identity Provider als Summe aller gesetzlichen und regulatorischen Anforderungen
Major Incident	Schwerer Vorfall
Minor Incident	Geringer Vorfall
TK-individuelle Features	umfasst den TK-individuellen Teil der ePA, welcher sowohl durch die TK selbst entwickelt als auch von der TK als TK individuelle Features, die ausschließlich für die TK bestimmt sind, bei dem AN abgerufen werden kann.
TK-Safe	Frontend der TK-Versicherten zur Nutzung der elektronischen Patientenakte als integraler Bestandteil der TK-App
Home-AS	Gemäß gemSpec_Aktensystem_ePAfueralle_1.8.1#3.12 Device Management

1. Ausgangssituation

Die Krankenkassen sind nach § 291 Abs. 8 SGB V dazu verpflichtet, jedem Versicherten eine nach § 325 Abs. 1 SGB V zugelassene digitale Identität zur Verfügung zu stellen. Um den Versicherten die Nutzung ihrer digitalen Identität zu ermöglichen, beabsichtigt die TK im ersten Schritt, eine vom AN durch die gematik zugelassene Whitelabel-Anwendung bereitzustellen. In einem zweiten Schritt beabsichtig die TK, die Whitelabel-Anwendung abzulösen und ein Authenticator-Modul in Form eines SDK in die eigene mobile Anwendung zu integrieren.

Die Krankenkassen sind nach § 342 Abs. 7 SGB V dazu verpflichtet, ein ePA-FdV für Desktop-Plattformen (ePA Desktop FdV) zur Verfügung zu stellen. Für das ePA Desktop FdV wird gemäß gematik Spezifikation ebenfalls ein IDP Authenticator-Modul benötigt, das in die Anwendung integriert werden muss. Die TK benötigt das ePA Desktop FdV als vollständig zugelassene Whitelabel-Anwendung.

2. Leistungsgegenstand

2.1. Überblick

Die Aufgaben des AN umfassen im Wesentlichen die folgenden Leistungen:

- Umsetzung der Vorgaben und Spezifikationen der gematik für den sektoralen Identity Provider
- Bereitstellung und Betrieb des sektoralen Identity Providers (IDP Backend, VAU, Authenticator-Modul und dazugehörige Systeme und Schnittstellen)
- Bereitstellung des IDP-Frontends (Whitelabel-Anwendung)
- Bereitstellung des ePA Desktop FdV inkl. Authenticator-Moduls
- Bereitstellung sämtlicher Komponenten in folgenden Umgebungen: PU, TU, RU, RU DEV
- Bereitstellung des Authenticator-Moduls (SDK(s) für mobile Anwendungen) *auf Abruf*
- Unterstützungsleistungen *auf Abruf*

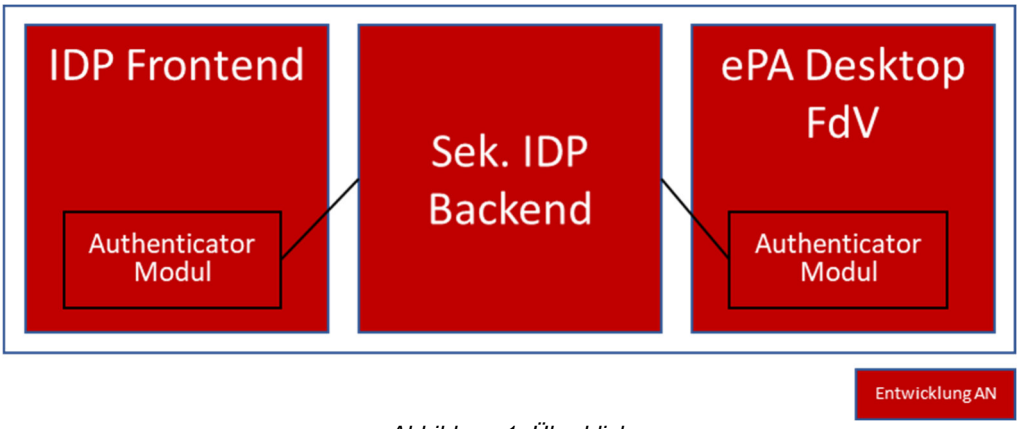

Abbildung 1: Überblick

Der AN muss der TK den sektoralen IDP, das IDP-Frontend, das Authenticator-Modul für das Mobile FdV (*auf Abruf*) und das ePA Desktop FdV inklusive Authenticator Modul fristgerecht nach dem Zeitplan (vgl. Kapitel 4.3) und umfangreich getestet (vgl. Kapitel 4.4) sowie gemäß der geltenden gematik-Spezifikationen bereitstellen.

Fordert die TK die oben beschriebene Leistung „Bereitstellung des Authenticator-Modul SDK“ (vgl. Kapitel 2.3.2.9) auf Abruf ein, so ergibt sich folgende Konstellation:

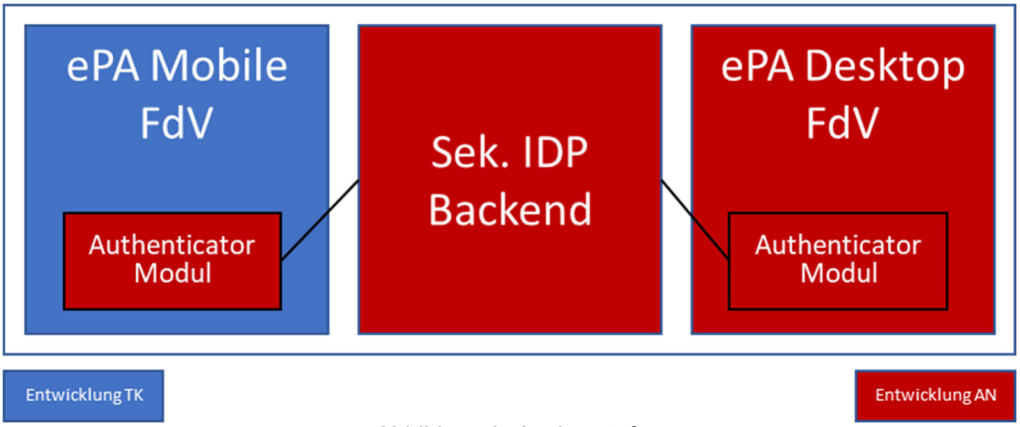

Abbildung 2: Ausbaustufe

2.2. Zulassung und Weiterentwicklung des bestehenden Produktes

Sowohl für die initiale Zulassung als auch für die Aufrechterhaltung und Weiterentwicklung der gültigen Zulassung, sind die durch die gematik gemäß Kapitel 2.3.1 und 2.4.1 zu erbringenden Anforderungen Bestandteil der zu erbringenden Leistung. Der AN verpflichtet sich dazu, die Leistung entsprechend den jeweils zuletzt veröffentlichten Vorgaben und Spezifikationen der gematik anzupassen. Anforderungen, die der AN der gematik gegenüber zu erfüllen hat, müssen auch der TK gegenüber erfüllt werden. Dies betrifft u. a. die Vorgaben zum Betrieb insb. hinsichtlich der Verfügbarkeit und Performance des IDP und die Reaktions- und Lösungszeiten des AN (u. a. TIP1-A_7265-*, GS-A_5561). Ferner gilt dies für alle Komponenten und Schnittstellen, wie z. B. die Verwaltungs- und Synchronisationsschnittstellen als auch die SDKs. Jegliche Informationen, Meldungen und Berichte (wie z. B. zu Ausfällen und Verfügbarkeits-Reports), welche der AN an die gematik weiterreicht, sind auch der TK bereitzustellen. Die für die jeweilige Zulassung zu erbringende Nachweise sind der TK nur auf Nachfrage auszuhändigen. Anforderungen, die andere Mandanten betreffen oder Betriebsgeheimnisse verletzen, sind hiervon ausgenommen (z. B. A_22567-*). Sofern der AN Abweichungen feststellt, können diese mit der TK abgestimmt werden.

Grundsätzlich gilt eine Umsetzungspflicht für KANN-Anforderungen der jeweiligen gematik Spezifikation. Die Pflicht zur Umsetzung gilt im Einzelfall nicht, wenn berechtigte Interessen des AN entgegenstehen. Berechtigte Interessen des AN liegen insbesondere vor, wenn eine Umsetzung einer KANN-Anforderung aus objektiv nachvollziehbaren Gründen nicht sinnvoll erscheint oder aus objektiv nachvollziehbaren Gründen mit der Einordnung als Standard-Produkt, das einheitlich einer Vielzahl an Kunden bereitgestellt wird, nicht vereinbar ist. Wird eine KANN-Anforderung aus vorgenannten Gründen nicht umgesetzt, ist die TK darüber in Kenntnis zu setzen und der AN muss eine nachvollziehbare Begründung vorlegen. Die Parteien sind sich bewusst, dass die Produkthoheit über das Standard-Produkt beim AN liegt.

Im Kontext dieser LB sind bestimmte Vorgaben (Fachkonzepte, Spezifikationen, Produktsteckbriefe etc.) der gematik relevant. Die Aufzählung der vorgenannten Vorgaben ist nicht abschließend, sondern wird fortlaufend um weitere einschlägige Dokumente erweitert, die im Zuge der Weiterentwicklung des sek. IDP oder des ePA Desktop FdV durch die gematik bereitgestellt werden und entsprechend zu berücksichtigen sind. Die jeweils durch die gematik gültigen Vorgaben und Spezifikationen sind der Website der gematik zu entnehmen. Dadurch kann es zu Anpassungen am durch den AN zur Verfügung zu stellenden Liefergegenstand kommen. Diese Anpassungen müssen im Rahmen von Betrieb und Pflege durch den AN umgesetzt und sichergestellt werden.

2.3. Sektoraler IDP

2.3.1. Vorgaben der gematik

Der AN muss gemäß den aktuellen gematik-Spezifikationen das Produkt Sektoraler Identity Provider bereitstellen und die entsprechenden Zulassungen nachweisen:

- Produkttyp Sektoraler Identity Provider in der Produkttypversion 3.2.0-0 V1.0.0 oder höher
- Anbietertyp Sektoraler Identity Provider in der Anbietertypversion 1.8.0 V1.0.0 oder höher

Ist eine Mitwirkung durch die TK zwingend erforderlich, ist der Auftragnehmer verpflichtet, die für die Umsetzung erforderlichen Mitwirkungspflichten zu bewerten und diese gegenüber der TK transparent zu kommunizieren.

2.3.2. Vorgaben der TK

Nachfolgend werden relevante Anwendungsfälle für den sek. IDP beschrieben, die zusätzlich zu den durch die gematik festgelegten Anwendungsfällen durch den AN umgesetzt werden müssen:

2.3.2.1. Bereitstellung einer White Label App für das IDP-Frontend

Das IDP-Frontend wird vom AN als customized White Label App bereitgestellt. Diese App ist Teil des sektoralen IDP. Die Basisanforderungen an das Authenticator Modul ergeben sich aus den Spezifikationen der gematik. Zusätzlich gelten folgende Anforderungen:

- Die App ist im CI & D (Corporate Identity und Design) der TK zu gestalten und folgt den Navigations- und Bedienungsgrundsätzen (UX) der TK-App. Dem AN werden diese Guidelines nach Vertragsschluss übermittelt. Die Anwendung ist mit der TK abzustimmen und wird durch die TK freigegeben.
- Die durch die App beim Betriebssystem angefragten Berechtigungen müssen mit der TK abgestimmt werden. Vor der Verwendung von Berechtigungen stellt der AN ein detailliertes Konzept zur Verfügung, aus dem hervor geht, warum die Berechtigungen verwendet werden und welche Sicherheits- und/oder Datenschutzimplikationen aus der Verwendung der Berechtigungen folgen. Die TK prüft das Konzept und gibt die Verwendung frei. Diese Beschreibung wird zusätzlich fortgepflegt. Der AN verpflichtet sich mit jedem Release zu prüfen, ob die Verwendung

noch notwendig ist und liefert mit jedem Release das ggf. angepasste Konzept und die ggf. angepasste Begründung.

- Der AN stellt der TK eine ausführliche Dokumentation der App bereit, inklusive aller Anwendungsfälle, Screen-Flows und Screen-Designs. Die Dokumentation ist mit jeder neuen Release-Version zu aktualisieren.
- Der AN stellt der TK ein geeignetes Tool bereit, um Textanpassungen für zukünftige Releases selbstständig vornehmen zu können.
- Die App wird vollumfänglich in deutscher und englischer Sprache bereitgestellt.

2.3.2.2. Plattformunterstützung und Veröffentlichung

Die White Label Anwendung muss vom AN für die Betriebssysteme iOS und Android manipulationssicher in die jeweiligen Stores, zum Zwecke der Veröffentlichung durch die TK, eingestellt werden. Die TK stößt die Store-Reviews an, sofern es von den Store-Herstellern gefordert wird und nimmt die Veröffentlichung vor. Zum Zwecke der Legitimation des Uploads einer App in den jeweiligen Store stellt die TK dem AN ein Herstellerzertifikat zur Verfügung. Der AN verpflichtet sich, missbräuchliche Nutzung zu verhindern, indem er z. B. die Zugriffsdaten geheim hält und den Zugang einschränkt.

Stores:

- iOS: App Store Connect
- Android: Google Play Store

Die unterstützten OS-Versionen umfassen mindestens die von den jeweiligen Herstellern aktiv unterstützen Major-Versionen. Abweichungen von dieser Regel können durch kritische Sicherheitslücken und bei anderen wichtigen Gründen (bspw. hoher Anteil aktiver Nutzer mit einer älteren OS-Version) in gegenseitigem Einvernehmen vereinbart werden. Ändern sich während der Vertragslaufzeit maßgeblich die technischen Rahmenbedingungen des Marktes (z. B. neue Betriebssystemversionen, Änderungen von Hardware-Standards oder Display-Formaten), verpflichten sich der AN und die TK, gemeinsam angemessene Maßnahmen zu erarbeiten, um die Funktionsfähigkeit und Nutzbarkeit der App weiterhin sicherzustellen. Anpassungen erfolgen nach gemeinsamer Abstimmung über den notwendigen Umfang und die Zuständigkeiten.

Die gelieferten Versionen für alle Ausführungsumgebungen müssen vollständig proxy-fähig sein und den Betrieb hinter HTTP(S)-Proxys unterstützen.

2.3.2.3. Identifikationsmethoden

Das IDP-Frontend bietet dem Nutzer zusätzlich zu einer Smartcard-Identifikation (eID und eGK) auch die Identifikation mit dem ePASS-Verfahren an. Dazu erfolgt die Anbindung an eine durch die gematik zugelassene Dritt-App. Zur Nutzung des ePASS-Verfahren wird der aktuell bestehende Vertrag der TK mit dem ePASS-Dienstleister nachgenutzt. Die Umsetzungsdetails sind zwischen AN und der TK abzustimmen.

Weitere, von der gematik aktuell geduldete Identifikationsverfahren (wie z. B. Identifikation in der Kundenberatung), werden zum aktuellen Zeitpunkt von der TK nicht gefordert.

2.3.2.4. Kopplung mit Diensten außerhalb der Föderation

Es besteht die Möglichkeit, Dienste, die nicht Teil der Föderation sind, direkt mit dem sek. IDP der TK in einer 1:1 Beziehung zu koppeln (Beispiel: Signaturdienst, TK-App). Hierzu gehört die Vergabe einer Client-ID und die Konfiguration von Re-Direct-URLs. Die Umsetzungsdetails sind zwischen AN und der TK abzustimmen. Die Kopplung mit dem Signaturdienst muss vor Inbetriebnahme des sek. IDP erfolgen. Der Zeitplan für weitere Kopplungen ist nach Vertragsabschluss abzustimmen.

2.3.2.5. Prüfidentitäten

Es besteht die Möglichkeit, Prüfkarten, die von der gematik erworben werden können, mit dem sek. IDP der TK in der Produktionsumgebung zu nutzen. Das Authenticator-Modul muss dazu in der Lage sein, Prüfkarten eindeutig zu identifizieren und deren Verwendung zuzulassen. Ob zu einer konkreten Prüfkarte eine GesundheitsID angelegt wird, ist vom Ergebnis abhängig, dass die TK im Rahmen der Registrierung zurück liefert (analog dem Registrierungsprozess für Versicherte der TK).

2.3.2.6. Zwei-Geräte-Flow

Für den 2-Geräte-Flow und weitere Anwendungsfälle wird die Web-Oberfläche des IDP angesprochen. Die Web-Oberfläche ist im CI/CD (Corporate Identity und Design) der TK zu gestalten. Die Web-Oberfläche muss den Navigations- und Bedienungsgrundsätzen (UX) der TK-Webseite folgen. Dem AN werden diese Guidelines nach Vertragsschluss übermittelt. Die Web-Oberfläche ist mit der TK abzustimmen und wird durch die TK freigegeben.

2.3.2.7. Funktionalitäten außerhalb der sek. IDP Spezifikation

Werden von der gematik funktionale Anforderungen definiert, die gemäß gematik-Spezifikation von dem IDP-Frontend zu erfüllen sind, so stellt der AN diese Funktionalitäten der TK in der Whitelabel-Anwendung und im SDK (vgl. Kapitel 2.3.2.9) zur Verfügung. Dies gilt auch für den Fall, wenn die funktionalen Anforderungen nicht direkt dem Produkt Sektoraler Identity Provider zugeordnet sind.

2.3.2.8. Backend Kommunikation

Für die Kommunikation zwischen sek. IDP und Kassen-Backend müssen Endpunkte für folgende Anwendungsfälle bereitgestellt werden:

- Der AN muss sicherstellen, dass die Signatur der Daten aus dem jeweiligen Identifikationsprozess (eGK-PIN, eID, ePASS) auf Gültigkeit überprüft wird. Bei einer fehlenden Gültigkeit ist der Identifikationsprozess mit einem nicht erfolgreichen Resultat abzubrechen.
- Übertrag der Daten (inkl. gültiger Signatur) aus dem Identifikationsprozess vom sek. IDP an das Kassen-Backend, damit die TK ein Stammdaten-Matching durchführen kann.

- Übertrag der Stammdaten vom Kassen-Backend an den sek. IDP zur Anlage einer GesundheitsID: Die Überprüfung und Übermittlung der Stammdaten an den sek. IDP erfolgt bei jeder Registrierung individuell
- Sobald sich der Status der Registrierung ändert, soll das Kassen-Backend vom sek. IDP aufgerufen werden
- Status der Registrierung: Endpunkt, über den die TK den aktuellen Status der Registrierung für die GesundheitsID abrufen kann. Außerdem sollen alle Detailinformationen je angefragte Person, die im sek. IDP gespeichert sind, zurückgegeben werden
- Datenaktualisierung von Kassen-Backend an sek. IDP: Ändern sich Stammdaten der Versicherten in dem Bestandssystem der TK, so sollen diese automatisiert für die GesundheitsID aktualisiert werden
- Auskunft, Sperrung oder Löschung durch die TK: Mitarbeitende der TK sollen die GesundheitsID oder Geräte, auf dem der Authenticator installiert ist, im Auftrag der Versicherten sperren und löschen und Auskünfte über Anmeldungen (ohne Preisgabe der Zielanwendungen) für einen bestimmten Versicherten erteilen können
- Geräteinformationen: Endpunkt, um je User abzufragen, für welche Geräte eine aktiv gültige Gerätebindung zur jeweiligen GesundheitsID besteht
- Health-Check: Endpunkt, um die Verfügbarkeit des sek. IDP regelmäßig abzufragen

Grundsätzlich soll für alle verfügbaren Endpunkte eine asynchrone Architektur verwendet werden, damit eine nachgelagerte Verarbeitung stattfinden kann, sollte eines der Systeme beim Schnittstellenaufruf nicht verfügbar sein.

Die genaue Konzeption der Backend-Architektur wird nach Vertragsschluss zwischen dem AN und der TK abgestimmt.

2.3.2.9. Auf Abruf: Bereitstellung eines Headless-SDK zur Integration in eine mobile Anwendung der TK

Die TK hat die Option, das Authenticator Modul als SDK zur Integration in eine mobile Anwendung der TK einzufordern.

Wird diese Option durch die TK benötigt, stellt der AN das zugelassene Authenticator-SDK neun Monate nach Beauftragung durch die TK als release-fähige Version bereit.

Grundsätzliches
Alle SDKs werden grundsätzlich für die Lauffähigkeit unter iOS und Android für den deutschen Markt entwickelt. Bei der Entwicklung muss der AN die jeweils aktuellen Richtlinien und Vorgaben von Apple und Google zur Implementierung von Apps anwenden. Die geforderte Funktionalität muss im SDK über native Schnittstellen in Swift/Kotlin bereitgestellt werden. Schnittstellen sollen plattformübergreifend die gleichen Signaturen aufweisen und zu denselben Ergebnissen führen. Plattformspezifische Abweichungen sind durch den AN in der Dokumentation zu begründen. Nach Absprache mit der TK können

Cross-Platform-Technologien (wie z. B. Kotlin Multiplatform) eingesetzt werden. Die TK kann den Einsatz bestimmter Cross-Platform-Technologien ablehnen.

Das SDK darf nur Code enthalten, der notwendig für die Erfüllung der geforderten Funktionalität ist.

Das SDK muss headless sein, damit die TK das User Interface und die Nutzersteuerung für die Funktionalitäten selbst entwickeln und gestalten kann. Headless bedeutet, Aufrufe von Schnittstellen des SDKs haben keine implizite Auswirkung auf das präsentierte User Interface. Das SDK soll keine Benutzeroberflächen oder dafür notwendige Komponenten enthalten und Schnittstellen sollen so gestaltet sein, dass sie unabhängig vom User Interface sind. Ausnahmen können gemacht werden, wenn dies unabdingbar für die Erfüllung der geforderten Funktionalität ist. Diese Ausnahmen müssen von der TK genehmigt werden.

Analysierbarkeit
Das SDK muss durch Logging-Mechanismen Informationen liefern, die zur Laufzeit Auskunft über vom SDK gesteuerte Ereignisse und Zustandsveränderungen geben. Es muss der TK über Programmschnittstellen möglich sein, den Detailgrad dieser Logs in den Testumgebungen anzupassen. Es muss der TK über Programmschnittstellen möglich sein, vom SDK ausgehendes Logging zu unterbinden. Das SDK muss für Testumgebungen im Fehlerfall möglichst detaillierte Informationen liefern können. Laufzeitfehler müssen so spezifisch wie möglich sein.

Berechtigungen
Die durch das SDK beim Betriebssystem angefragten Berechtigungen müssen mit der TK abgestimmt werden. Vor der Verwendung von Berechtigungen stellt der AN ein detailliertes Konzept zur Verfügung, aus dem hervor geht, warum die Berechtigungen verwendet werden und welche Sicherheits- und/oder Datenschutzimplikationen aus der Verwendung den Berechtigungen folgen. Die TK prüft das Konzept und gibt die Verwendung frei. Diese Beschreibung wird zusätzlich fortgepflegt. Der AN verpflichtet sich mit jedem Release zu prüfen, ob die Verwendung noch notwendig ist und liefert mit jedem Release das ggf. angepasste Konzept und die ggf. angepasste Begründung.

Einsatz von Open-Source
Das SDK darf keine Open-Source Lizenzen verwenden, die voraussetzen, dass die Mantelapp, in der das SDK eingebunden wird, ihren Quellcode offenlegen muss.

Drittbibliotheken
Die verwendeten Drittbibliotheken müssen abgegolten sein und kompatible Lizenzen aufweisen. Werden bei einer Lieferung Änderungen an den verwendeten Versionen von Drittbibliotheken erbracht, die zu notwendigen Anpassungen führen (Breaking Changes), müssen diese Änderungen rechtzeitig vor der Lieferung des Releases mit der TK abgestimmt werden. Die verwendeten Abhängigkeiten jeder gelieferten Version müssen inklusive der zugehörigen Lizenz zwecks Darstellung zur Laufzeit über SDK-Schnittstellen ermittelt werden können oder alternativ in einem maschinenlesbaren Format mit jedem

Release geliefert werden. Bei der Verwendung von Drittbibliotheken muss die Einhaltung der einzuhaltenden Sicherheitsstandards durch den AN sichergestellt werden.

Gerätehärtung
Es muss über eine Gerätehärtung-Konfiguration des SDKs oder eine separate SDK-Variante möglich sein, im SDK enthaltene Härtungsmechanismen zu aktivieren oder zu deaktivieren (es muss ermöglicht werden, das SDK in eine App mit oder ohne bereits bestehende Härtungsmechanismen einzubetten).

Kompatibilität
Die gelieferten SKDs unterstützen mindestens die von den jeweiligen Herstellern aktiv unterstützten Major-OS-Versionen (iOS und Android). Abweichungen von dieser Regel können durch kritische Sicherheitslücken und bei anderen wichtigen Gründen (bspw. hoher Anteil aktiver Nutzer mit einer älteren OS-Version) in gegenseitigem Einvernehmen vereinbart werden. Die gelieferten Versionen für alle Ausführungsumgebungen müssen vollständig proxy-fähig sein und den Betrieb hinter HTTP(S)-Proxys unterstützen.

Das SDK muss (ausschließlich für Entwicklungszwecke) auf Emulatoren / Simulatoren lauffähig sein. Es muss für Entwicklungszwecke auch funktional sein, wenn ein HTTP(S)-Proxy eingesetzt wird.

Bei der Speicherung von Daten in Komponenten, die auch von der einbettenden App genutzt werden könnten, müssen abrufbare Identifier (z. B. Schlüssel von Schlüssel-Wert-Paaren) mit einem Präfix versehen werden, um Konflikte zu vermeiden.

Das Android-SDK muss auf armeabi-v7a-, arm64-v8a- und auf x86_64-Architekturen lauffähig sein. Alle Schnittstellen im SDK müssen als Protokolle bzw. Interfaces bereitgestellt werden, damit die TK die Möglichkeit hat, Schnittstellen des SDKs durch eigene Implementierungen zu ersetzen (beispielsweise für das Testing).

Anforderungen an die Sicherheit
Die TK plant, das SDK in die TK-App (ePA-FdV) zu integrieren. Damit gelten die Sicherheitsanforderungen der gematik und des BSI, die an ein ePA-FdV gestellt werden, auch für das SDK. Der AN verpflichtet sich, diese Anforderungen für sein SDK umzusetzen. Dazu gehört insbesondere der sichere Entwicklungsprozess (SEP).

Es muss auf Wunsch der TK eine Variante des SDKs bereitgestellt werden, die das Durchführen eines Penetration-Tests möglich macht. Zu dieser Variante gehört:

- Die Variante des SDKs darf keine Mechanismen erzwingen, die das Mitlesen oder Manipulieren des Netzwerkverkehrs verhindern.
- Die Variante des SDKs darf keine Mechanismen erzwingen, die das Auslesen oder Analysieren von Speicherinhalten und Laufzeitverhalten verhindern.
- Anti-Tamper-, Hardening- und Anti-Debug-Funktionen müssen deaktiviert, deaktivierbar oder gezielt abschwächbar sein.

Bereitstellung
Das Android-SDK muss in einem Maven Repository gehostet werden, welches aus der TK-Infrastruktur erreichbar ist und durch eine starke Authentifizierung abgesichert ist.

Das iOS-SDK muss als Swift Package ausgeliefert werden in einem privaten Repository. Das Repository muss aus der TK-Infrastruktur erreicht werden können und durch eine starke Authentifizierung abgesichert sein. Alle Lieferartefakte müssen einen eindeutigen unveränderlichen Bezeichner haben.

2.4. ePA Desktop FdV

2.4.1. Vorgaben der gematik

Der AN muss gemäß den aktuellen gematik-Spezifikationen das Produkt Sektoraler Identity Provider bereitstellen und die entsprechenden Zulassungen nachweisen:

- Produkttyp ePA-Frontend des Versicherten in der Produkttypversion 3.1.3-2 V1.0.0 oder höher

Ist eine Mitwirkung durch die TK zwingend erforderlich, ist der Auftragsnehmer verpflichtet, die für die Umsetzung erforderlichen Mitwirkungspflichten zu bewerten und diese gegenüber der TK transparent zu kommunizieren.

2.4.2. Vorgaben der TK

2.4.2.1. Bereitstellung einer White Label Anwendung für das ePA Desktop FdV

Das ePA Desktop FdV wird vom AN als customized White Label Anwendung bereitgestellt. Die Basisanforderungen ergeben sich aus den gematik Spezifikationen. Zusätzlich gelten folgende Anforderungen, die durch den AN umgesetzt werden müssen:

- Die Anwendung ist im CI/CD (Corporate Identity und Design) der TK zu gestalten. Dem AN werden diese Guidelines nach Vertragsschluss übermittelt. Die Anwendung ist mit der TK abzustimmen und wird durch die TK freigegeben.
- Der AN stellt der TK eine ausführliche Dokumentation der Anwendung bereit, inklusive aller Anwendungsfälle, Screen-Flows und Screen-Designs. Die Dokumentation ist mit jeder neuen Release-Version zu aktualisieren.
- Die Anwendung wird vollumfänglich in deutscher und englischer Sprache bereitgestellt.

2.4.2.2. Nutzerauthentifizierung

Es muss möglich sein, dass der Nutzer sich ausschließlich mit eGK+PIN über das ePA Desktop FdV an die ePA anmelden kann. Die TK kann über eine Liste zulässiger Institutionskennzeichen den Nutzerkreis einschränken. Dafür wird das Haupt-IK der eGK ausgelesen. Die Anmeldung an ein

Identity and Access Management (IAM) darf nicht Voraussetzung für die Nutzung sein. Die für die Geräteregistrierung notwendige Benachrichtigungsadresse wird durch die TK an das Aktensystem übermittelt. Fehlt die Benachrichtigungsadresse, so muss dem Nutzer ein Verweis auf eine Internetseite der TK dargestellt werden. Die TK teilt dem AN die URL mit.

Neben der Möglichkeit der o.g. Anmeldung mit eGK+PIN muss auch der 2-Geräte-Flow mit einem mobilen Authenticator möglich sein. Die URL für den zu verwendenden sektoralen IDP wird von der TK für das ePA Desktop FdV definiert und ist vom Nutzer nicht änderbar.

2.4.2.3. Verbindung zum Aktensystem

Das ePA Desktop FdV muss in der Lage sein, sich mit unterschiedlichen Aktensystemen zu verbinden und diese als Home-AS anzuerkennen. Die FQDN für das Aktensystem, das zuerst kontaktiert wird, legt die TK fest (nicht änderbar). Ist die Akte am Aktensystem nicht vorhanden, werden die weiteren zugelassenen Aktensysteme angefragt. Das bedeutet u. a., dass eine neue TK-versicherte Person mit dem ePA Desktop FdV in die Lage versetzt wird, ihre ePA zu nutzen, auch wenn die Akte noch beim ePA-Anbieter ihrer vorherigen Kasse verweilt. Das Aktensystem, welches die Akte tatsächlich hält, darf für eine konkrete KVNR im Frontend gespeichert werden und fortan als erstes kontaktiert werden.

2.4.2.4. Authenticator-Modul

Das Authenticator-Modul im ePA Desktop FdV muss keine Gerätebindung unterstützen. Die beschriebene Nutzerauthentifizierung in Kapitel 2.4.2.2 ist abschließend. Weitere Verfahren wie eID und e-PASS sind für das Authenticator-Modul im ePA Desktop FdV nicht notwendig.

2.4.2.5. Plattformunterstützung und Veröffentlichung

Das ePA Desktop FdV muss vom AN für die Betriebssysteme Microsoft Windows Home, Apple MacOS und Linux (Distribution Ubuntu) manipulationssicher in die jeweiligen Stores, zum Zwecke der Veröffentlichung durch die TK, eingestellt werden. Die TK stößt die Store Reviews an, sofern es von den Store-Herstellern gefordert wird und nimmt die Veröffentlichung vor. Zum Zwecke der Legitimation des Uploads eines ePA Desktop FdV in den jeweiligen Stores stellt die TK dem AN ein Herstellerzertifikat zur Verfügung. Der AN verpflichtet sich, missbräuchliche Nutzung zu verhindern, indem er z. B. die Zugriffsdaten geheim hält und den Zugang einschränkt.

Stores:

- Microsoft Windows: Microsoft Partner Center
- MacOS: App Store Connect
- Linux (Distribution Ubuntu): Canonical Snapcraft

Die unterstützten OS-Versionen umfassen mindestens die von den jeweiligen Herstellern aktiv unterstützen Major-Versionen. Abweichungen von dieser Regel können durch kritische Sicherheitslücken und bei anderen wichtigen Gründen (bspw. hoher Anteil aktiver Nutzer mit einer älteren OS-Version) in

gegenseitigem Einvernehmen vereinbart werden. Die gelieferten Versionen für alle Ausführungsumgebungen müssen vollständig proxy-fähig sein und den Betrieb hinter HTTP(S)-Proxys unterstützen.

3. Betriebsanforderungen

3.1. Verfügbarkeit

Die Verfügbarkeitsanforderungen richtet sich nach den jeweils aktuell gültigen Anforderungen der gematik (vgl. Kapitel 2.2).

Bei geplanten Pflege- und Wartungsarbeiten an Systemen und Anwendungen der PU, die zu einer Abweichung von den vereinbarten Betriebszeiten führen oder führen können, muss der AN die TK mit einem Vorlauf von fünf Werktagen informieren. Für die Systeme und Anwendungen in allen Testumgebungen gilt ebenfalls ein Vorlauf von fünf Werktagen. Dies hat in Textform an die vereinbarte Ansprechperson / Stelle der TK zu erfolgen. Von der Vorlaufzeit darf im Einzelfall mit Zustimmung der TK abgewichen werden. Pflege- und Wartungsarbeiten werden in die Verfügbarkeit eingerechnet, sofern im Einzelfall mit der TK nicht abweichend vereinbart.

Pflege- und Wartungsarbeiten sind nach den Anforderungen der Gematik durchzuführen. Alle Abstimmungspflichten, die der AN mit der Gematik vorzunehmen hat, sind auch mit der TK durchzuführen. Alle Mitbestimmungsrechte der Gematik gelten ebenfalls für die TK.

3.2. Störung

3.2.1. Verfahren und Inhalt der Störungsmeldung

Eine Störung wird initial an festgelegte Ansprechpersonen der TK mit einem Informationsgehalt analog zu 3.2.3 „Statusbericht“ gemeldet.

Der AN benennt eine Ansprechperson / Stelle für die TK, die 24/7 in Bezug auf Störungen erreichbar ist.

3.2.2. Störungsdefinition

PU:
Ein Service gilt für den Erfassungszeitraum als ausgefallen, wenn im Erfassungszeitraum von fünf Minuten für einen der Anwendungsfälle gemäß [gemSpec_Perf#Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP] 20% oder mehr der zugehörigen Anfragen nicht erfolgreich verarbeitet werden und damit die Kernfunktionalität der Dienste eingeschränkt ist. Diese Regelung gilt analog für die jeweiligen Aufrufe an den IDP-Backendschnittstellen gemäß 2.3.2.8.

TU/RU/RU DEV:
Ein Service gilt für den Erfassungszeitraum als ausgefallen, wenn im Erfassungszeitraum von fünf Minuten für einen der Anwendungsfälle gemäß [gemSpec_Perf#Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP] 20% oder mehr der zugehörigen Anfragen nicht erfolgreich verarbeitet werden und damit die Kernfunktionalität der Dienste eingeschränkt ist. Diese Regelung gilt analog für die jeweiligen Aufrufe an den IDP-Backendschnittstellen gemäß 2.3.2.8.

Fehlerklassen

PRIO		Auswirkung		
		hoch	mittel	niedrig
Dringlichkeit	hoch	Priorität 1	Priorität 2	Priorität 3
	mittel	Priorität 2	Priorität 3	Priorität 4
	niedrig	Priorität 3	Priorität 4	Priorität 4

Auswirkung hoch	• Es liegt ein Ausfall vor (s. Störungsdefinition). • Der durch die Störung verursachte Schaden weitet sich schnell aus, falls nicht unmittelbar eine Lösung bereitgestellt werden kann. • Die Störung führt zu Verletzung gesetzlicher Vorschriften (z. B. Datenschutz und Informationssicherheit). • Die Störung hat eine hohe Auswirkung in der öffentlichen Wahrnehmung und führt zu einem erheblichen Imageverlust.
Auswirkung mittel	• Das Produkt ist mit sehr starken Einschränkungen nutzbar. • Die Störung kann zur Verletzung gesetzlicher Vorschriften führen (z. B. Datenschutz und Informationssicherheit).
Auswirkung niedrig	• Das Produkt ist mit Einschränkungen nutzbar. • Eine Verletzung gesetzlicher Vorschriften ist nicht gegeben.

Dringlichkeit hoch	• Durch die Störung steht das Produkt (und/oder Funktionen) nicht zur Verfügung bzw. nur so eingeschränkt, dass die Nutzung nicht zumutbar ist. • Die Sicherheit der Infrastruktur ist nicht mehr gewährleistet. • Die Störung des Produktes (und/oder Funktionen) lässt sich nicht durch eine Umgehungslösung unmittelbar beseitigen.
Dringlichkeit mittel	• Durch die Störung steht das Produkt (und/oder Funktionen) erheblich eingeschränkt zur Verfügung. Die Nutzung ist jedoch mit Einschränkungen möglich. • Es ist absehbar, dass sich die Störung ausweitet, wenn keine Gegenmaßnahmen ergriffen werden.
Dringlichkeit niedrig	• Durch die Störung steht das Produkt (und/oder Funktionen) mit leichten Einschränkungen zur Verfügung. • Der von dem Incident verursachte Schaden nimmt im Verlauf der Zeit nicht oder nur unwesentlich zu.

Sollten sich Abweichungen dazu verschärfend in der gemRL_Betr_TI ergeben, so gelten diese zusätzlich.

Alle Kriterien dieses Kapitels sind ODER-Kriterien.

Prioritäten 1 und 2 werden als Major Incident bezeichnet.

3.2.3. Statusbericht

Ein Statusbericht für Störungen der Priorität 1 und 2 in der PU hat zu den Hauptzeiten in einstündigen Intervallen und zu den Nebenzeiten in zweistündigen Intervallen zu erfolgen. Der Bericht beschreibt den Status der Störungsbearbeitung unter Angabe folgender Informationen:

- Beschreibung des Fehlerbildes aus Sicht eines Versicherten und der TK
- Identifizierte Ursache, soweit bekannt
- eventuell vorhandene Umgehungslösungen
- chronologische Auflistung aller bisher getroffenen Maßnahmen (technisch / Kundenkommunikation)
- weitere geplante Maßnahmen zur Störungsbeseitigung
- voraussichtlicher Zeitpunkt des Abschlusses der Störungsbearbeitung

3.2.4. Wiederherstellungszeit

Die Störung ist innerhalb der im Service-Level (vgl. gematik Spezifikation) festgelegten Dauer zu beheben. Sie beginnt nach den in Punkt 3.2.2 (Störungsdefinition) genannten Kriterien. Sie endet mit der Behebung der Störung, einer Entstörungsbeschreibung oder der vollständigen Installation eines von der TK akzeptierten Workarounds (temporäre Ersatzlösung). Bei Lieferung eines Workarounds muss eine dauerhafte Lösung einvernehmlich und in einem abgestimmten Zeitraum erfolgen. Wartezeiten, die durch Verletzung der Mitwirkungspflichten der TK entstehen, zählen nicht zur Wiederherstellungszeit.

3.2.5. Entstörungsbericht (Root Cause Analysis)

Jede Störungsbehebung einer Störung der Priorität 1 und 2 ist in einem Bericht zu dokumentieren. Die Protokolle sind der TK binnen fünf Tagen nach Entstörung zur Verfügung zu stellen.

Folgende Inhalte sind mindestens in einem Bericht aufzusetzen:
Es ist die gematik Vorlage zu verwenden. Alle von der gematik geforderten Informationen sind auszufüllen, darunter zählen u. a.:

- Störungsmeldungsnummer
- Eingangszeit der Störungsmeldung
- Priorität der Erstmeldung
- Kontaktdaten des Störungsmeldenden und -annehmenden
- Alle an die TK erfolgten Rückmeldungen mit Zeiten
- Entstörungsbeschreibung mit Zeitpunkt der Meldung
- Ggf. erfolgte Eskalationen mit jeweiligen Ansprechpersonen

3.3. Monitoring

3.3.1. Anforderungen an das Monitoring

Das Monitoring ist so auszugestalten, dass es als Grundlage für einen fachlichen Leitstand dient und eine schnelle Einordnung von Auffälligkeiten sowie fundierte operative Entscheidungen unterstützt. Die Daten müssen sowohl aktuelle Zustände als auch historische Entwicklungen der letzten drei Monate abbilden.

3.3.2. Technische Bereitstellung der Monitoring-Daten

Zur Überprüfung der vollständigen Servicegesundheit muss der AN der TK mindestens eine offene Schnittstelle (API) bereitstellen, über die Antwortzeit- und Verfügbarkeitsmetriken in Intervallen von maximal fünf Minuten unverzüglich und maschinenlesbar abgerufen werden können.
Die Daten müssen nach den Four Golden Signals aufbereitet werden und über HTTPS-Metric-Endpoints (z. B. nach Prometheus-Standard oder OpenTelemetry-Spezifikationen) geliefert werden.

3.3.3. Monitoring-Modell (Four Golden Signals)

Maßgeblich für das Monitoring ist das Modell "Four Golden Signals" von Google SRE (https://sre.google/sre-book/monitoring-distributed-systems/) zu verwenden.
Der AN stellt sicher, dass das Monitoring nach den gematik Use Cases auf Basis der folgenden vier Dimensionen erfolgt:

- Latenz (Latency)
- Durchsatz (Traffic)
- Fehler (Errors)
- Sättigung (Saturation)

Diese vier Dimensionen sind verbindlich für alle zu überwachenden Services umzusetzen. Abweichungen sind mit der TK abzustimmen.

3.3.4. Use Case basiertes Monitoring

Das Monitoring ist nicht rein technisch, sondern entlang fachlicher Anwendungsfälle (Use Cases) umzusetzen. Die Grundlage bilden die relevanten Use Cases gemäß gemSpec_Perf#Tab_gemSpec_Perf_Berichtsformat_sektoraler_IDP. Die Metriken müssen fachlich nachvollziehbar dem jeweiligen Use Case zugeordnet sein.

3.3.5. Anforderungen an Metriken und Messpunkte

Für jeden überwachten Use Case sind durch den AN strukturierte Informationen bereitzustellen, darunter:

- Beschreibung des Messpunkts
- Zuordnung zu einem Golden Signal
- Messintervall (max. fünf Minuten)
- Fachliche Aussagekraft der Metrik
- Eindeutige Benennung der Metriken

Die Darstellung hat in einfacher Sprache und verständlicher Form zu erfolgen.

3.3.6. Schwellenwerte und Bewertung

Für alle Messpunkte sind Schwellenwerte zu definieren und gemeinsam mit der TK abzustimmen:

- *OK* - bedeutet, dass der überwachte Service fehlerfrei läuft und alle Messwerte innerhalb der definierten Grenzwerte liegen.
- Optional: *Warning* - bedeutet, dass der Service grundsätzlich funktioniert, aber der überwachte Wert bereits außerhalb des optimalen Bereichs liegen und Aufmerksamkeit benötigt.
- *Error* - bedeutet, dass der Service ausgefallen oder stark beeinträchtigt ist und sofortiges Eingreifen erforderlich ist

3.3.7. Alerting und Nachvollziehbarkeit

Der AN stellt eine Anbindung an ein Alerting für die TK bereit. Zusätzlich legt der AN der TK ein Konzept zur Nachvollziehbarkeit des Monitorings vor und hat diese unaufgefordert bei jeder Aktualisierung bereitzustellen.
Die Dokumentation soll wie folgt aufgebaut werden:

Name Alert	**Rule - betroffenes Golden Signal**	**Logik**	**Beschreibung der Alarmierungsregeln**	**Beschreibung der Auswirkungen**
	Welches Golden Signal wird damit unterstützt?	Beschreibung der Alarmierungslogik (bspw. Zustand über X Min über Schwellenwert Y)	Bsp.: Team Z wird per Push Notification informiert.	Verweis auf das Betriebshandbuch oder anderen Dokumentationen.

3.4. Service Review & Service Report

Zu Beginn eines jeden Kalendermonats wird ein Service Review durch die TK veranstaltet. In diesem Service Review werden die Verfügbarkeitswerte und Service-Level Kennzahlen des vergangenen Monats in abgestimmter Form betrachtet und ggf. Maßnahmen abgeleitet und nachverfolgt. Pönalen-relevante Störungen oder Verletzungen werden abgestimmt und in den Report aufgenommen. Der Service Review wird in einem Report durch den AN protokolliert und in einem abgestimmten Freigabeverfahren beidseitig freigegeben, um dann Grundlage der Pönalen-Berechnung zu werden.

4. Qualitäts- und Release-Anforderungen

4.1. Allgemeines

Sämtliche nachfolgende Regelungen beziehen sich auf alle vom AN verantworteten Komponenten, soweit nicht im Einzelnen ausdrücklich davon abgewichen wird. Darüber hinaus leistet der AN vorbeugende Maßnahmen (vorbeugende Pflege) zur Behebung von Fehlern, welche dem AN unabhängig von Fehlermeldungen bekannt werden. Zusätzlich ist der AN verantwortlich die Wiederherstellung der Betriebsbereitschaft sicherzustellen. Die Qualitätssicherung richtet sich nach dem aktuellen, branchenüblichen Stand der Technik.

Der Leistungsumfang des AN umfasst auch:

- Anbieterbedingte Updates der Laufzeitumgebungen (Betriebssysteme iOS, Android; (viertel-) jährliche größere Updates der mobilen Betriebssysteme iOS und Android, Zwischenupdates und jährliche Major-Updates)
- Änderungen der Appstore-Richtlinien
- Änderungen in der Infrastruktur der Betriebssysteme
- Regelmäßiges Monitoring der Softwareumgebung, wie z. B. neue Usergeräte, neue Betriebssysteme und damit zusammenhängende Funktionsänderungen
- Sicherheitskritische Updates der Software-Bibliotheken und Frameworks sowie Compliance-Vorgaben von staatlichen Stellen (z. B. BSI) und Aufsichtsbehörden (z. B. BAS)
- Proaktive Beratung der TK hinsichtlich notwendiger oder empfohlener Anpassungen. Diese Beratung erfolgt so frühzeitig, dass im Rahmen des Änderungsdienstes negative Auswirkungen auf die Benutzbarkeit des Produktes vermieden werden können, sofern die Informationen zu Anpassungen auch von Dritten dem AN rechtzeitig zur Verfügung stehen.
- Weiterhin übernimmt der AN eigenständig Maßnahmen, um stets den Betrieb im Rahmen der zugesicherten SLAs zu gewährleisten. Dazu gehören insbesondere die Modernisierung und Anpassungen an der Software-Architektur und Implementierung der Gesamtlösung, insbesondere im Hinblick auf Performance bzw. steigender Last.

Der AN ist darüber hinaus verpflichtet, eine hohe Quellcodequalität zu gewährleisten. Hierzu gehört insbesondere:

- Einsatz von Verfahren zur Strukturverbesserung von Quellcode, z. B. Durchführung von Refactoring
- Code-Reviews zur regelmäßigen Prüfung der Codequalität
- Führen von Software-Metriken als Teilmaßnahme der Qualitätssicherung
- Komplexitätsmetriken

Sollte sich bei der Inbetriebnahme von Aktualisierungen des AN ein unvorhergesehenes anderes Verhalten der implementierten Lösung einstellen und nicht sofort beseitigt werden können, müssen Maßnahmen zur temporären Umgehung durch den AN beschrieben und in Abstimmung mit der TK umgesetzt werden.

4.2. Monatsbericht

Der AN verpflichtet sich, der TK regelhaft Daten (monatlich) zu liefern. Dazu gehören mindestens alle Kennzahlen, die auch Dritten (z. B. gematik) regelhaft geliefert werden. Darüber hinaus stellt der AN sicher, dass die in den folgenden aufgeführten Kennzahlen monatlich aktualisiert werden und die Daten aggregiert sowie anonymisiert bereitgestellt werden, um jeden Personenbezug auszuschließen. Die Daten werden über eine zu definierende Schnittstelle bereitgestellt, wenn die Möglichkeit zur Datenerhebung besteht.

1. Nutzerstatistiken Versicherte
   IDP:
   - Anzahl der angelegten GesundheitsIDs
   - Anzahl der erfolgreichen Identifikationen
   - Anzal der Autorisierungen
   - Anzahl der aktiven Nutzer (mind. 1 Nutzer-Aktivität in dem betrachteten Monat)

   ePA Desktop FdV:
   - Anzahl der aktiven Nutzer (mind. 1 Nutzer-Aktivität in dem betrachteten Monat)
   - Häufigkeit der Aktivität pro Nutzer (z. B. durchschnittliche Anzahl der Logins pro Tag/Woche/Monat).

2. Performance-Kennzahlen
   IDP:
   - Fehlerquoten bei der Nutzung (Fehlgeschlagene Identifikationen, fehlgeschlagene Autorisierungen)

   ePA Desktop FdV:
   - Fehlerquoten bei der Nutzung der ePA (Anzahl der Fehlermeldungen je Anwendungsfall)

4.3. Release-Management

Grundsätzlich werden alle Veröffentlichungen des sek. IDP und des ePA Desktop FdV in einem gemeinsamen Lieferplan (auch als Release-Plan bezeichnet) organisiert.

Lieferzeitpunkte beziehen sich jeweils auf ein Produkt unter allen weiter oben angegebenen Operating Systems. Darin aufgeführt sind u. a. auch die verbindlichen Zeitpunkte der Backend-Deployments auf den verschiedenen Umgebungen (RU DEV, RU, TU und PU).

Die TK stimmt mit dem AN diesen Lieferplan in gegenseitigem Einvernehmen ab.

4.3.1. Release-Typen

Release Typ – Initiale Bereitstellung

Das Release *Initiale Bereitstellung* beschreibt die Auslieferung der ersten Version zum Go-Live in PU nach Zuschlag der Ausschreibung. Zum Zeitpunkt der Ausschreibung geht die TK von einem Go-Live in PU sechs Monate nach Vertragsabschluss aus.

Release Typ – Major

Ein *Major* Release ergibt sich, wenn anhand des gematik Produkttypsteckbriefs sich an der ersten oder zweiten Stelle Änderungen zur Vorversion ergeben. Grundlage dafür sind die Spezifikations-Veröffentlichungen der gematik.

Release Typ – Maintenance

Ein *Maintenance* Release beinhaltet unterjährige oder turnusgemäße Changes der Gematik (derzeit je Quartal), neue Funktionen und/oder Bugfixes:

- Für neue, von der TK gewünschte Funktionen, muss der AN nach Anfrage durch die TK innerhalb von zehn Werktagen eine erste Einschätzung zur Umsetzbarkeit der neuen Funktionen abgeben und, sofern der AN grundsätzlich in der Lage ist die Anforderungen umzusetzen, muss er innerhalb von zwanzig Werktagen ein Angebot, inklusive Preis und Lieferzeitpunkt, vorlegen.
- Die notwendigen Bugfixes werden zwischen der TK und dem AN abgestimmt (vgl. Kapitel 4.5)

Es ist mindestens ein *Maintenance* Release je Quartal auszuliefern. Die Lieferzeitpunkte sind vornehmlich in der Mitte des Quartals anzusetzen und zwischen TK und AN im Einvernehmen abzustimmen. Es müssen stets zwei zukünftige *Maintenance* Releases verbindlich terminiert sein.

4.3.2. Release-Zeiträume

Folgende Zeiträume sind, bezogen auf den sek. IDP, einzuhalten:

	Initiale Bereitstellung	Major	Maintenance
Lieferplan	8 Wochen nach Zuschlag	4 Wochen nach Spec-Veröffentlichung	Mindestens die zwei folgenden Maintenance Releases sind jederzeit zeitlich benannt
Schnittstellen-beschreibung	8 Wochen nach Zuschlag	6 Wochen nach Spec-Veröffentlichung	5 Wochen vor Final Release (falls zutreffend)
Vorab-Release	12 Wochen nach Zuschlag	-	-
Beta-Release	18 Wochen nach Zuschlag	2 Wochen vor Final Release	2 Wochen vor Final Release
Final-Release	20 Wochen nach Zuschlag	2 Wochen vor gematik PU-Termin	Mitte eines Quartals

Folgende Zeiträume sind, bezogen auf das ePA Desktop FdV, einzuhalten:

	Initiale Bereitstellung	Major	Maintenance
Lieferplan	8 Wochen nach Zuschlag	4 Wochen nach Spec-Veröffentlichung	Mindestens die zwei folgenden Maintenance Releases sind jederzeit zeitlich benannt
Schnittstellenbeschreibung	-	-	-
Vorab-Release	12 Wochen nach Zuschlag	-	-
Beta-Release	18 Wochen nach Zuschlag	2 Wochen vor Final Release	2 Wochen vor Final Release
Final-Release	20 Wochen nach Zuschlag	2 Wochen vor gematik PU-Termin	Mitte eines Quartals

Folgende Zeiträume sind, bezogen auf den optionalen SDK-Abruf für das Authenticator Modul (vgl. Kapitel 2.3.2.9), einzuhalten:

	Initiale Bereitstellung	Major	Maintenance
Lieferplan	4 Wochen nach Abruf der Option	4 Wochen nach Spec-Veröffentlichung	Mindestens die zwei folgenden Maintenance Releases sind jederzeit zeitlich benannt
Schnittstellenbeschreibung	16 Wochen nach Abruf der Option	6 Wochen nach Spec-Veröffentlichung	5 Wochen vor Final Release (falls zutreffend)
Vorab-Release	24 Wochen nach Abruf der Option	Mind. 4x im 3 Wochenabstand vor Beta-Release-Termin	Mind. 1x 3 Wochen vor Final Release, falls Schnittstellenänderungen
Beta-Release	30 Wochen nach Abruf der Option	16 Wochen vor gematik PU-Termin	2 Wochen vor Final Release bei Schnittstellenänderungen
Final-Release	36 Wochen nach Abruf der Option	2 Wochen vor gematik PU-Termin	Mitte eines Quartals

Grundsätzlich werden folgende Qualitätsstufen im Release-Plan behandelt:

1. **Lieferplan**
   Abgestimmter Lieferplan, der alle in der o.g. Tabelle aufgeführten Zeiträume berücksichtigt.
2. **Schnittstellenbeschreibung**
   Abgestimmte Schnittstellenbeschreibungen auf der Basis von OpenAPI-Beschreibungen. Für Asynchrone Schnittstellen (wenn zutreffend) ist die Basis AsyncAPI. Jeweils in der aktuellen Version.
3. **Vorab-Release (Preview)**
   Abgestimmter, aber nicht vollständig getesteter Arbeitsstand mit Funktionseinschränkungen, inkl. Dokumentation. Der fachliche Scope wird zwischen AN und TK abgestimmt.
4. **Beta-Release**
   Getestete Version mit stabilen APIs aller Funktionen, inkl. Dokumentation.
5. **Final-Release (Stable)**
   Vollständig qualitätsgesicherte Version inkl. vollständiger Dokumentation (s.u.)

Der Release-Plan ergibt sich aus der oben dargestellten Matrix. Abweichungen vom Release-Plan in Umfang oder Zeitpunkt müssen im Einvernehmen mit der TK abgestimmt werden.

4.3.3. Release-Artefakte

Zu den jeweiligen Releases gehören folgende Artefakte:

Schnittstellenbeschreibungen

Es ist eine vollständige und nachvollziehbare Schnittstellenbeschreibung der bereitzustellenden API zu erstellen und zu liefern. Diese hat mindestens folgende Inhalte und Anforderungen zu erfüllen:

1. Allgemeine Beschreibung
    a. Darstellung des Zwecks und des Funktionsumfangs der API
    b. Übersicht der Architektur und eingesetzter Technologien
2. Technische Spezifikation auf Basis des OpenAPI Standards bzw. sofern zutreffend AsyncAPI Standards
    a. Vollständige Auflistung sämtlicher Endpunkte inkl. URL-Struktur und unterstützter Methoden
    b. Beschreibung der Request- und Response- Struktur
    c. Definition aller Datentypen, Pflicht- und optionalen Felder
    d. Auflistung und Erläuterung sämtlicher Rückgabecodes und Fehlermeldungen
    e. Darstellung der eingesetzten Authentifizierungs- und Autorisierungsverfahren
    f. Beschreibung der Sicherheitsmaßnahmen (u. a. Verschlüsselung, Transportprotokolle)
3. Datenmodell & Referenzen auf Basis des OpenAPI Standards bzw. sofern zutreffend AsyncAPI Standards
    a. Dokumentation der zugrunde liegenden Datenobjekte und deren Relation
    b. Bereitstellung von Referenzdatensätzen und Beispieldaten
    c. Darstellung des Versionierungskonzepts der API
4. Integrationsszenarien
    a. Beschreibung relevanter Anwendungsfälle und Abläufe
    b. Darstellung in Form von Sequenz- oder Flussdiagrammen (soweit erforderlich)
    c. Erläuterung von Abhängigkeiten zu anderen Systemen oder Schnittstellen
5. Nicht-funktionale Anforderungen
    a. Angabe von Performance-Vorgaben (z. B. Antwortzeiten, Durchsatz, Rate-Limits)
    b. Beschreibung der Verfügbarkeits- und Monitoring Anforderungen
    c. Vorgaben zu Logging- und Audit-Funktionalitäten
6. Dokumentation & Hilfsmittel
    a. Bereitstellung einer vollständigen, maschinen- und menschenlesbaren API-Dokumentation (z. B. Swagger)
    b. Bereitstellung von Beispielen (z. B. Curl, Postman Collections)
    c. Dokumentation der Änderungs- und Versionshistorie
    d. Eine Liste der verwendeten Drittbibliotheken inkl. einer Beschreibung des Verwendungsgrunds

Vorab-Release (Preview)

1. RU oder RU DEV
    a. Bereitstellung eines Backends mit abgestimmtem Funktionsumfang zur Integration durch die TK. Backend-Schnittstellen, die zu diesem Zeitpunkt noch nicht funktional sind, werden gemockt zur Verfügung gestellt.
    b. Zugang für den Auftraggeber (z. B. über URL mit gesichertem Zugang)
    c. Nachvollziehbare Versionierung
2. Funktions- und Testnachweise
    a. Übersicht der im Preview enthaltenen Funktionen (Change- und Feature-Liste)
    b. Beschreibungen etwaiger Einschränkungen gegenüber dem Stable Release (u. a. noch fehlende Features oder Ausprägungen eines Features)
    c. Beispielhafte Testdaten zur Verifikation der Funktionalität(en)
3. Begleitende Dokumentation
    a. Kurze Preview-Dokumentation mit Hinweisen zu:
        i. enthaltenen Features
        ii. Bekannte Einschränkungen / offene Punkte
        iii. Bekannte Fehler (Bug-Liste)
    b. Release Notes zum Preview-Stand

Beta-Release

Ein Beta-Release ist im Sinne des Anforderungsmanagement voll funktionsfähig und größtenteils qualitätsgesichert. In Fällen, die mit der TK abzustimmen sind, ist es zulassungsrelevant und - daher die an Zulassungen gültigen Kriterien erfüllen.

1. RU oder RU DEV
    c. Das Backend muss voll funktionsfähig sein, deployt und lauffähig sein
    d. Zugang für den Auftraggeber (z. B. über URL mit gesichertem Zugang)
    e. Signierte und versionierte Release-Kennzeichnung
4. Funktions- und Testnachweise
    a. Übersicht der in der Beta enthaltenen Funktionen (Change- und Feature-Liste)
    b. Beschreibungen etwaiger Einschränkungen gegenüber dem Stable Release (u.a. bekannte Bugs)
    c. Frei von zulassungsverhindernden Bugs
    d. Beispielhafte Testdaten zur Verifikation der Funktionalität(en)
    e. Feature-, Regressions-, Smoke-Test-Berichte
5. Begleitende Dokumentation
    a. Beta-Dokumentation mit Hinweisen zu:
        i. enthaltenen Features
        ii. Bekannte Einschränkungen / offene Punkte
        iii. Bekannte Fehler (Bug-Liste)
    b. Release Notes zum Beta-Stand
    c. Abnahme-Walkthrough-Angebot durch AN

Final-Release

Zu einem Final-Release gehören folgende Artefakte:

- Vollständige Dokumentation der APIs (Dokumentation mittels OpenAPI oder AsyncAPI)
- Release-Notes, bestehend aus
  - Technische Zusammenfassung, verständlich für TK-Entwickler
  - Kurzbeschreibung als Report (Management Summary)
- Impact Assessment Report zur Einschätzung der Notwendigkeit einer Begutachtung
- Hinweispflicht auf kritische Veränderungen an zentralen Software-Komponenten und Schnittstellen
- Testplan inkl. Testergebnisse & Regressionstestergebnisse
- Abnahme-Walkthrough-Angebot durch AN

4.4. Testing

Jede Software-Auslieferung (ausgenommen RU-DEV) muss mit einer vollumfänglichen nachvollziehbaren Test-Dokumentation (Methodik inkl. Test-Abdeckung) geliefert werden, inkl.:

- „Findings“ (Auflistung aller Fehler und Auffälligkeiten im Test, bspw. Software-Verhalten abseits der Spezifikationen)
- Daraus resultierender Maßnahmen oder Umgehungslösungen, die das zuvor entdeckte „Finding“ in seiner Auswirkung in Hinsicht auf seine Funktion korrigieren oder abmildern.
- Auflistung aller Komponenten und Schnittstellen, die nicht getestet wurden inkl. einer Darlegung, weshalb kein Test erfolgen konnte
- Risiko-Abschätzungen („Impact-Analysen“) der einzelnen „Findings“ und nicht getesteter Komponenten und Schnittstellen zu weiteren Schnittstellen, Abhängigkeiten sowie zum Gesamtprodukt

Der AN entwickelt während der Vertragslaufzeit zusammen mit der TK ein Konzept für automatisierte Contract-Tests, um Schnittstellenänderungen kontrolliert umzusetzen. Ziel ist die Sicherstellung, dass Änderungen an API-Endpunkten, Datenstrukturen oder Rückgabeformaten keine unbeabsichtigten Seiteneffekte erzeugen. Gemeinsam werden geeignete Tools ausgewählt und in die bestehende Test- und CI/CD-Umgebung integriert.

4.5. Fehleranalyse und -behebung

Der AN muss dazu in der Lage sein, in den Frontend-Anwendungen eine Fehleranalyse zu betreiben. In Produktion auftretende Fehler sind proaktiv durch den AN zu analysieren. Analyse-Ergebnisse werden der TK in einem branchenüblichen Report wöchentlich zur Verfügung gestellt. Werden für die Analyse Frontend-Logs erhoben, sind die geltenden Datenschutzvorgaben gemäß der gematik Spezifikation zu berücksichtigen. Außerdem stellt der AN der TK eine Möglichkeit bereit, Fehler eigenständig aufzunehmen und an den AN zur Behebung zu übergeben.

Der AN verpflichtet sich, innerhalb einer unten definierten Reaktionszeit die Fehlerbehebung vorzunehmen.

Die Kritikalität der Fehler wird durch die TK wie folgt bewertet:

Level	Beschreibung	Zeitraum innerhalb dessen mit einer Behebung des Fehlers begonnen werden muss	Ziel-Release

Hotfix	• Datenschutzvorfall
	• Features können nicht genutzt werden (fehlende Hoheit über die eigenen Daten - kein Workaround möglich)
	• Zulassungsverhindernd, weil:
	  ○ es einen sicherheitstechnisch kritischen Fehler betrifft (z. B. nicht zulässige Authentifizierung und Autorisierung, Angriffsvektoren nicht geblockt) oder
	  ○ eine wesentliche Abweichung der durch gematik spezifizierten Anforderung (z. B weil der Use Case/Flow nicht ausführbar ist) vorliegt
	• Fehler führt nicht nachvollziehbar zur Dateninkonsistenz, die nicht durch operative Eingriffe behoben werden kann
	• Fehler führt nachvollziehbar zu einer Dateninkonsistenz, die nicht durch operative Eingriffe behoben werden kann
		4h, auch außerhalb der Service-Zeiten	Bereitstellung unverzügliches Hotfix-Release

High	• Happy path Use Case nicht oder nur über Workaround durchführbar, jedoch nicht zulassungsverhindernd • Signifikanter Fehler in der Corporate Identity Umsetzung (falsche Farben, falsche Corporate Identity Icons) • Dem Flow widersprechende Texte	3 Werktage	Nächstes Final-Release
Medium	• Abweichung vom festgelegten Design / UI • Textfehler (Auffällige Typos die auch den Sinn des Wortes verändern oder grammatikalisch schwerwiegend sind, mehrere Typos auf einem Screen, nicht kundenspezifisch konfigurierbar) • Fehlermeldungen zu unspezifisch, jedoch Fehlermeldung als gewünschter Bestandteil des Flows • Edge Cases (Negativ Test cases) die zu Fehlermeldungen führen (jedoch nur unter bestimmten Konstellationen auftreten, die nicht dem Standard-Flow /Happy Path oder Standardfehlerfall entsprechen (siehe hierbei auch: Fehlermeldungen oben) • TK-individuelle Farbschemata, Icons, etc., die nicht unter der Corporate Identity der Standardanwendungen der TK fallen • Accessibility Tickets (nur wenn im Vertrag gefordert ist)	10 Werktage	Übernächstes Final-Release oder nach Absprache
Low	• Accessibility Ticket, wenn nicht im Vertrag gefordert • Einzelner Rechtschreibefehler auf einem Screen	15 Werktage	Übernächstes Final-Release oder nach Absprache

Fehler werden gemäß einer mit der TK abzustimmenden Bug-Matrix kategorisiert und bearbeitet. Die TK hat das einseitige Stimmrecht einen Fehler mit Klassifizierung „Hotfix“ gemäß vorstehender Tabelle festzulegen.
Fehler mit der Kritikalität „Hotfix“ werden in einem dedizierten Hotfix-Release ausgeliefert. Der AN verpflichtet sich, dafür Sorge zu tragen, dass Hotfix-Releases innerhalb von 24 Stunden ausgeliefert werden können.

Alle Fehler mit Kritikalität High, Medium oder Low werden gemäß o.a. Tabelle in entsprechende Final-Releases in den Release-Plan aufgenommen.

5. Allgemeine technische Anforderungen

Neben den o.g. Vorgaben der gematik und den individuellen Vorgaben der TK gelten zusätzlich die allgemeinen technischen Vorgaben der TK gemäß Anlage „AB_Richtlinie_Pflichtenheft_IDP“. Falls eine allgemeine technische Anforderung in einem direkten Widerspruch zu den o.g. Vorgaben stehen sollte, so wäre die Definition aus diesem Dokument führend.

6. Zusatzanforderungen Datenschutz

Der AN akzeptiert das TK-Dokument zur Auftragsvereinbarung nach Art. 28 DSGVO i.V.m. § 80 SGB X im vollen Umfang. Geringfügige inhaltliche/redaktionelle Anpassungen können an dem bereitgestellten Dokument erfolgen, unterliegen aber dem beidseitigen Einvernehmen. Fremde Dokumente werden grundsätzlich nicht akzeptiert.

Sollte es zu einer Datenschutzverletzung kommen, so erfolgt durch den AN eine unverzügliche Meldung nach Art. 33 Abs. 1 DSGVO an die TK und zwar so, dass die TK die 72 Stunden Regelung nach Art. 33 Abs. 1 S. 2 DSGVO gegenüber ihren eigenen Aufsichtsbehörden einhalten kann. Die Erstmeldung an die TK muss für Dritte (z. B. weitere Fachbereiche innerhalb der TK und Behörden) in ausführlicher und nachvollziehbarer Form bereitgestellt werden. Die eventuell aus der Datenschutzverletzung resultierende(n) Folgemeldung(en) müssen die Erstmeldung in nachvollziehbarer Form ergänzen und den Vorfall weiterhin in ausführlicher Form ergänzen, bis dieser abgeschlossen ist. Dies gilt auch für die schon ergriffenen oder geplanten Maßnahmen zur Fehlerbehebung.

7.TK-Projektanforderungen

7.1. Projektleitung

Der AN ist angehalten auf besondere betriebliche Belange der TK im Zusammenhang mit der Tätigkeit, die sich aus dem Vertragsverhältnis ergeben, z. B. release-bezogene Zielvorgaben und fachliche Vorgaben, Rücksicht zu nehmen, soweit diese zur ordnungsgemäßen Vertragsdurchführung erforderlich sind.
Der AN wird einen Projektleiter einsetzen, der ermächtigt ist, kurzfristig verbindliche Entscheidungen bezüglich der Projektdurchführung und Entscheidungen über vertragliche Angelegenheiten für den AN zu treffen. Der Projektleiter ist für die Organisation der Ressourcen im Rahmen der Leistungserbringung verantwortlich.
Sofern Unterstützungsleistungen angefordert werden (vgl. Kapitel 7.4), ist der Projektleiter der übergeordnete Ansprechpartner für Steuerung und Koordination der Integrationsphase, Annahme von Anforderungen, Priorisierung und Eskalationsmanagement.
Der Projektleiter ist vom AN zu benennen. Der AN ist ferner angehalten die benannte Person langfristig in der Rolle zu halten. Sollte der Projektleiter vom AN gewechselt werden, so hat dies nach Rücksprache mit der TK zu erfolgen.

7.2. Personelle Bereitstellung durch den AN

Um die in den vorherigen Kapiteln beschriebenen Leistungen zu erfüllen, stellt der AN geeignetes Personal bereit. Neben dem Projektleiter werden der TK feste Ansprechpersonen genannt, um die notwendigen Abstimmungen hinsichtlich initialer Bereitstellung, Betrieb, Wartung und Pflege vorzunehmen.

7.3. Kommunikation

Austausch- und Steuerungsformate
Während der gesamten Vertragslaufzeit wird ein regelmäßiger Informationsaustausch zwischen der TK und dem AN etabliert:

- **Wöchentlicher operativer Jour fixe:**
  Regelmäßiger Abstimmungstermin (z. B. 60 Minuten, remote via MS Teams o.ä.) mit Beteiligung der technischen Leads beider Seiten, Ziel: Abstimmung offener Punkte, Fortschrittskontrolle, Koordination von Test- und Release-Aktivitäten.
- **Zweiwöchentlicher Management-Termin:**
  Austausch auf Leitungsebene (Projektleitung / Client Manager), Ziel: Status, Risiken, Kapazitätsplanung, Prioritäten. Grundsätzlich findet der Austausch remote via MS Teams und 4x pro Jahr bei der TK in der Unternehmenszentrale statt)
- **Ad-hoc-Workshops:**
  Nach Bedarf zur Klärung komplexer Themen

7.4. Zusätzliche personelle Unterstützungsleistungen bei Integration und Migration

Gegenstand der Regelung

Neben der Bereitstellung der beschriebenen Leistungen bietet der Anbieter auf Abruf Unterstützungsleistungen durch qualifiziertes Personal an, um die Integration des Systems in die IT-Umgebung der TK sicherzustellen. Diese Unterstützungsleistung **kann** durch die TK zu folgenden Zeitpunkten in Anspruch genommen werden:

- bis zum ersten Go-Live (vgl. Kapitel 7.5)
- bei Abruf der Option eines SDK bis zum ersten Go-Live (vgl. Kapitel 2.3.2.9)

Abrufbare Rollen und typischer Einsatzbereich

- Backend-Entwickler: Unterstützung bei der Implementierung von Schnittstellen, Anpassung von APIs, Fehleranalyse und Performanceoptimierung.
- Frontend-Entwickler: Unterstützung bei der Anbindung der App-Frontend-Komponenten an die Backend-APIs.
- Solution Architect / Integrationsarchitekt: Unterstützung bei Architekturentscheidungen, Sicherheitskonzepten und Infrastrukturintegration.

Abruf, Verfügbarkeit und Vergütung

- Der Auftraggeber kann die genannten Rollen nach Bedarf abrufen (nach Aufwand, mit Stundensätzen gemäß Preisblatt).
- Der Auftragnehmer stellt sicher, dass qualifiziertes Personal mit projektbezogenem Know-how innerhalb von max. 10 Arbeitstagen nach Abruf zur Verfügung steht.

7.5. Meilensteine

Im folgenden Absatz sind Meilensteine definiert. Die Meilensteine stellen Teilabschlüsse des Gesamtprojekts dar. Die Meilensteine orientieren sich an den definierten Lieferzeitpunkten für die initiale Bereitstellung (**vgl. Kapitel 4.3.2**)

7.5.1. Meilensteine sek. IDP

Der AN stellt sicher, dass folgende Meilensteine bis zum angegebenen Zeitraum vollständig erfüllt werden:

Meilenstein 1 (Schnittstellenbeschreibung sek. IDP)
8 Wochen nach Zuschlag
Der AN muss der TK die zum Zeitpunkt aktuelle technische und fachliche Dokumentation der Produkte bereitstellen:

- IDP-Backend: Schnittstellen zur Anbindung an das Kassenbackend
- IDP-Frontend: Detaillierte Beschreibung des Funktionsumfangs und der fachlichen Abläufe

Meilenstein 2 (Vorab-Release sek. IDP)
12 Wochen nach Zuschlag
Der AN muss das Backend und Frontend mit abgestimmtem Funktionsumfang bereitstellen. Noch nicht vorgenommene Produktanpassungen (vgl. Kapitel 2.3.2) sind der TK mitzuteilen.

Meilenstein 3 (Beta-Release sek. IDP)
18 Wochen nach Zuschlag
Der AN muss die notwendigen Produktanpassungen (vgl. Kapitel 2.3.2) vorgenommen haben, sodass die Anforderungen, die aus den Ausschreibungs-Dokumenten der TK hervorgehen, in der RU DEV erfüllt werden. Der sek. IDP der TK ist Teil der Föderation und durch TI-Fachdienste in der RU DEV aufrufbar. Die sek. IDP Backend-Anbindung an die TK (inklusive Anbindung des Signaturdienstes, der nicht Teil der Föderation ist) ist abgeschlossen.

Meilenstein 4 (Final Release sek. IDP)
20 Wochen nach Zuschlag
Das final Release wird der TK für das IDP-Frontend zur Veröffentlichung in den jeweiligen Stores bereitgestellt.

Meilenstein 5 (Zulassung und ggf. Aufhebung der Nebenbestimmungen)
Der AN muss die gültige gematik Zulassung für den produktiven Betrieb der im Leistungsgegenstand definierten Produkte vorweisen. Alle Nebenbestimmungen der gematik, die an eine vorläufige Zulassung gekoppelt sind, wurden aufgelöst.

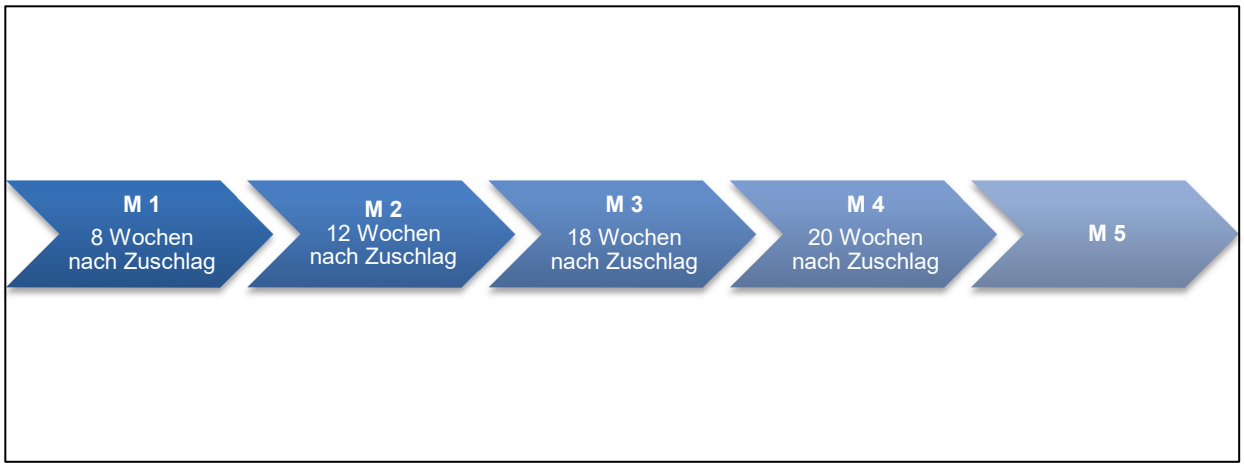

Abbildung 3: Meilensteine

7.5.2.Meilensteine ePA Desktop FdV

Der AN stellt sicher, dass folgende Meilensteine bis zum angegebenen Zeitraum vollständig erfüllt werden:

Meilenstein 1 (Schnittstellenbeschreibung ePA Desktop FdV)
8 Wochen nach Zuschlag
Der AN muss der TK die zum Zeitpunkt aktuelle technische und fachliche Dokumentation der Produkte bereitstellen:

- ePA Desktop FdV: Detaillierte Beschreibung des Funktionsumfangs und der fachlichen Abläufe

Meilenstein 2 (Vorab-Release ePA Desktop FdV)
12 Wochen nach Zuschlag
Der AN muss das Frontend mit abgestimmtem Funktionsumfang bereitstellen. Noch nicht vorgenommene Produktanpassungen (vgl. Kapitel 2.4.2) sind der TK mitzuteilen.

Meilenstein 3 (Beta-Release ePA Desktop FdV)
18 Wochen nach Zuschlag
Der AN muss die notwendigen Produktanpassungen (vgl. Kapitel 2.4.2) vorgenommen haben, sodass die Anforderungen, die aus den Ausschreibungs-Dokumenten der TK hervorgehen, in der RU DEV erfüllt werden.

Meilenstein 4 (Final Release ePA Desktop FdV)
20 Wochen nach Zuschlag
Das final Release wird der TK für das ePA Desktop FdV zur Veröffentlichung in den jeweiligen Stores bereitgestellt.

Meilenstein 5 (Zulassung und ggf. Aufhebung der Nebenbestimmungen)
Der AN muss die gültige gematik Zulassung für den produktiven Betrieb der im Leistungsgegenstand definierten Produkte vorweisen. Alle Nebenbestimmungen der gematik, die an eine vorläufige Zulassung gekoppelt sind, wurden aufgelöst.

7.5.3. Meilensteine bei Abruf der Option SDK

Der AN stellt sicher, dass folgende Meilensteine bis zum angegebenen Zeitraum vollständig erfüllt werden:

Meilenstein 1 (Schnittstellenbeschreibung SDK)
16 Wochen nach Zuschlag
Der AN muss der TK die zum Zeitpunkt aktuelle technische und fachliche Dokumentation der Produkte bereitstellen:

- Headless SDK: Detaillierte Beschreibung des Funktionsumfangs und der technischen Abläufe

Meilenstein 2 (Vorab-Release SDK)
24 Wochen nach Zuschlag
Der AN muss das SDK mit abgestimmtem Funktionsumfang bereitstellen. Noch nicht vorgenommene Produktanpassungen (vgl. Kapitel 2.3.2.9) sind der TK mitzuteilen.

Meilenstein 3 (Beta-Release SDK)
30 Wochen nach Zuschlag
Der AN muss die notwendigen Produktanpassungen (vgl. Kapitel 2.3.2.9) vorgenommen haben, sodass die Anforderungen, die aus den Ausschreibungs-Dokumenten der TK hervorgehen, in der RU DEV erfüllt werden.

Meilenstein 4 (Final-Release SDK)
36 Wochen nach Zuschlag
Das Final-Release des SDK wird der TK bereitgestellt.

Meilenstein 5 (Zulassung und ggf. Aufhebung der Nebenbestimmungen)
Der AN muss die gültige gematik Zulassung für den produktiven Betrieb der im Leistungsgegenstand definierten Produkte vorweisen. Alle Nebenbestimmungen der gematik, die an eine vorläufige Zulassung gekoppelt sind, wurden aufgelöst.