Glossar
für die elektronische Patientenakte (ePA)

Begriff	Beschreibung
Ad-hoc-Berechtigung (ePA)	Hierbei handelt es sich um die Berechtigungen, die der Versicherte, einer Leistungserbringerinstitution (LEI) z. B. seinem Hausarzt, unter Verwendung seiner eGK und PIN direkt vor Ort erteilen kann.
Aktensystem	Das ePA-Aktensystem ist ein Produkttyp der Fachanwendung ePA. Es stellt sicher, dass nur authentifizierte und autorisierte Nutzer mit dem ePA-Aktensystem interagieren. In einer Komponente zur Dokumentenverwaltung verwaltet das ePA-Aktensystem die Dokumente zu einem Aktenkonto eines Versicherten.
Alternative Versichertenidentität (al.vi)	Mit Hilfe einer alternativen Versichertenidentität kann sich ein Versicherter ohne eGK am ePA-Aktensystem anmelden. Eine Bestätigung der Identität wird nach erfolgter Zwei-Faktor-Authentisierung am Frontend des Versicherten (FdV) beim Signaturdienst (SGD) erfragt und von diesem an das Frontend zurückgegeben (vergleichbar mit einer Fernsignatur).
Anbieterwechsel	Bei einem Anbieterwechsel ändert sich der Aktenanbieter (beispielsweise ein Wechsel von BITMARCK zur IBM). Der Versicherte kann mit ePA Stufe 1.1 seine Akte noch nicht zum neuen Anbieter umziehen lassen. Das geht erst ab 01.01.2022. Bis dahin kann der Versicherte beim Anbieterwechsel die Dokumente aus seiner bisherigen Akte lokal zwischenspeichern und danach in die neue Akte einstellen. Die alte Akte wird beim bisherigen Anbieter gelöscht.
Authentifizierung	Authentifizierung ist die Überprüfung der Identität. Beispiel: Das System prüft die Richtigkeit und Gültigkeit der Signatur Technischer Prozess (ePA): Rechnerische Prüfung der Signatur, Prüfung des Datums Gültigkeit bis des Zertifikats gegen das Tagesdatum, Prüfung des Zertifikatsstatus gegen den OCSP-Responder der eGK-Zertifikate. Übergabe eines Authentisierungs-Token an das Frontend.
Authentifizierung (1FA)	Ein-Faktor-Authentifizierung
Authentifizierung (2FA)	Zwei-Faktor-Authentifizierung
Authentisierung	Authentisierung ist der Nachweis einer eindeutigen Identität. Beispiel: Ein Versicherter authentisiert sich durch Stecken der eGK und Eingabe der PIN Technischer Prozess (ePA): Zum Beispiel Challenge/Response. Das System übergibt beim Wunsch nach Zugriff eine Challenge an das Frontend. Das Frontend benutzt das AUT-Zertifikat der eGK. Durch die PIN-Eingabe wird der private Schlüssel für das AUT-Zertifikat freigeschaltet. Mit dem privaten Schlüssel werden dann die Challenge und das Zertifikat des Versicherten signiert. Die signierte Challenge und das signierte Zertifikat werden als Response an das System übergeben.

Autorisierung	Autorisierung ist die Prüfung/Vergabe von Rechten. Beispiel: Das System prüft, ob für den Besitzer eines Authentisierungs-Tokens für die Nutzung der ePA eine Berechtigung vorliegt. Technischer Prozess (ePA): Das System prüft, ob für den Besitzer eines Authorisierungs-Tokens ein verschlüsseltes Schlüssel-Paket vorhanden ist und übergibt dieses zusammen mit einem Autorisierungs-Token an das Frontend.
BfDI	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Das Bundesamt für Sicherheit in der Informationstechnik ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat mit Sitz in Bonn, die für Fragen der IT-Sicherheit zuständig ist.
Bundesamt für Soziale Sicherung (BAS)	Zum 1. Januar 2020 ist das im Jahr 1956 gegründete Bundesversicherungsamt (BVA) in Bundesamt für Soziale Sicherung (BAS) umbenannt worden. Das BAS führt die Aufsicht über die Träger und Einrichtungen der gesetzlichen Kranken-, Pflege-, Renten- und Unfallversicherung, deren Zuständigkeitsbereich sich über mehr als drei Bundesländer erstreckt. Zudem nimmt das BAS wichtige Verwaltungsaufgaben im Bereich der Sozialversicherung wahr. Zu diesen Aufgaben gehören u. a. die Verwaltung des Gesundheitsfonds, die Durchführung des Risikostrukturausgleichs in der Krankenversicherung, die Zulassung von Behandlungsprogrammen für chronisch Kranke sowie die Verwaltung des Ausgleichsfonds in der sozialen Pflegeversicherung.
Business Service Manager (BSM)	Der BSM wird eingesetzt, wenn ein Nutzer einen Fehler, über die ePA-App, meldet und Details zu seinem eingesetzten Smartphone benötigt werden. So kann etwa das benutzte Hardware Modell mit exaktem Softwarestand bis hin zur aktuellen Akku-Kapazität ermittelt werden.
Captcha	Ein Captcha wird verwendet, um festzustellen, ob ein Mensch oder eine Maschine (Roboterprogramm, kurz Bot) einbezogen ist. In der Regel dient dies zur Prüfung, von wem Eingaben in Internetformulare erfolgt sind, weil Roboter hier oft missbräuchlich eingesetzt werden. Captchas dienen also dem Schutz der Betreiber-Ressourcen, nicht dem Schutz des Benutzers oder dessen Daten. Im Unterschied zum klassischen Turing-Test, bei dem Menschen die Frage klären möchten ob sie mit einem Mensch oder einer Maschine interagieren, dienen Captchas dazu, dass eine Maschine diese Frage klären soll.
Change Request (CR)	Änderungsanforderung
Data Universal Numbering System (DUNS / D-U-N-S)	Die D-U-N-S Nummer ist eine neunstellige Zahl, anhand derer sich Unternehmen auf Basis des Standorts eindeutig identifizieren lassen. Sie wird von Dun & Bradstreet (D&B) zugewiesen und verwaltet und im geschäftlichen Bereich als standardisierte Kennziffer genutzt.
DiGA	Digitale Gesundheitsanwendungen
DiGAV	Digitale-Gesundheitsanwendungen-Verordnung
Dokumentenverwaltung	Die ePA-Komponente Dokumentenverwaltung des ePA-Aktensystems, dient dem sicheren Speichern und Auffinden von Dokumenten des Versicherten aus seiner persönlichen Akte, durch berechtigte Nutzer. Diese sind der Versicherte selbst oder von ihm benannte Vertreter sowie Leistungserbringerinstitutionen.
eGS	Elektronische Gesundheitsservices

eIDAS	electronic IDentification, Authentication and trust Services
Elektronische Patientenakte (ePA)	Gesetzlich Versicherte können ab dem 01.01.2021 – auf freiwilliger Basis – ihre gesundheitsbezogenen Dokumente mit einer elektronischen Patientenakte (ePA) ihrer Krankenkasse künftig lebenslang sicher verwalten. Die darin enthaltenen Informationen stehen ihnen selbst sowie Leistungserbringern zur Verfügung – sofern der Versicherte zuvor die jeweiligen Leistungserbringerinstitutionen dafür berechtigt hat. Mit Inkrafttreten des Terminservice- und Versorgungsgesetzes (TSVG) werden die gesetzlichen Krankenkassen verpflichtet, ihren Versicherten spätestens ab dem 1. Januar 2021 eine von der Gesellschaft für Telematik mbH (gematik) zugelassene elektronische Patientenakte (ePA) anzubieten. Weiterhin haben die die gesetzlich Versicherte zudem einen Rechtsanspruch auf die Nutzung ihrer ePA. Alle Leistungserbringer sind verpflichtet, ihren Patienten die Daten, die über diese erhoben wurden, in deren ePA bereitzustellen, sofern der Patient es wünscht. Das wird die Rechte und Partizipationsmöglichkeiten des Versicherten deutlich stärken. Die ePA ist eine versichertengeführte Akte.
eMP	Elektronischer Medikationsplan
ePA Versicherten Helpdesk (ePA VHD)	Der Versicherten Helpdesk ist die erste Anlaufstelle für die Versicherten bei allen Fragen rund um die ePA. Der ePA VHD wird dem Versicherten durch seine zuständige Krankenkasse oder einen, von ihr beauftragten, Dienstleister bereitgestellt.
ePA-Aktensystem	Das ePA-Aktensystem ist ein Produkttyp der Fachanwendung ePA. Es stellt sicher, dass nur authentifizierte und autorisierte Nutzer mit dem ePA-Aktensystem interagieren. In einer Komponente zur Dokumentenverwaltung verwaltet das ePA-Aktensystem die Dokumente zu einem Aktenkonto eines Versicherten.
ePA-Modul Frontend des Versicherten (FdV-Modul)	Das ePA-Modul Frontend des Versicherten ist als Komponente im Frontend des Versicherten integriert und führt die dezentrale Fachlogik der Fachanwendung ePA aus. Es ermöglicht dem Versicherten die Nutzung des ePA-Aktensystems.
Fachanwendungsspezifischer Dienst (FAD)	Ein fachanwendungsspezifischer Dienst ist ein System, das an die TI-Plattform angeschlossen ist und im Rahmen fachlicher Anwendungsfälle als Provider auftritt. Der fachanwendungsspezifische Dienst nutzt Infrastruktur- und Netzwerkdienste der TI-Plattform. Fachanwendungsspezifische Dienste stellen die Integrationsschicht für Backendsysteme und Bestandsnetze (Existing Application Zone) dar.
FdV	Frontend des Versicherten
Feldtest	Das wesentliche Ziel eines Feldtests ist der Nachweis der Funktionalität und Interoperabilität der verschiedenen ePA-Komponenten (Konnektor, Aktensystem, FdV) in der Produktivumgebung. Da die Durchführung des Feldtests mehrere Monate in Anspruch nimmt und eine fristgerechte Umsetzung der ePA zum 01.01.2021 somit nicht sichergestellt werden konnte, wurde entschieden anstatt des Feldtests eine kontrollierte Inbetriebnahme in der Produktivumgebung durch den Anbieter der ePA-Aktensysteme durchzuführen. Siehe Kontrollierte Inbetriebnahme.
Graphical User Interface (GUI)	Grafische Benutzeroberfläche
Health Care Provider (HCPO)	Leistungserbringerinstitution

Heilberufsausweis (HBA)	Der Heilberufsausweis (HBA) ist ein personenbezogener Ausweis für Personen, die einen Heilberuf ausüben, wie z. B. Ärzte oder Apotheker. Dieser Ausweis hat das Format einer Scheckkarte und ist mit einem Lichtbild und einem Mikroprozessorchip ausgestattet. Der HBA ermöglicht eine Authentifizierung gegenüber der Telematikinfrastruktur (TI), Verschlüsselung und enthält zudem eine qualifizierte elektronische Signatur (QES) des Arztes, bzw. Apothekers. Mit dem HBA kann auf die Patientendaten der eGK zugegriffen werden, sofern der Patient diese freigegeben hat. Durch den elektronischen Ausweis werden zusätzliche Anwendungen, wie z. B. das elektronische Rezept erst möglich. Die Ausgabe erfolgt in der Regel durch die entsprechende Kammer, wie z. B. Landesärzte-, bzw. Landesapothekerkammer.
Identity Access Management (IAM)	Die Einführung eines Identity and Accessmanagements (IAM) stellt die solide Basis für die Online Produkte / Anwendungen der Krankenkasse dar zur sicheren Identifizierung und Authentifizierung des Versicherten. Bei Bedarf werden zusätzliche Authentifizierungsfaktoren je nach anzuzeigenden Daten und deren Schutzniveau genutzt. An einer zentralen Stelle werden die Versicherten als Online Benutzer gepflegt und können mit Standard Verfahren wie OAuth2 (Open Authorization) / OpenID Connect für Single-Sign-On in bestehenden Anwendungen eingebunden werden. Damit werden die Anforderungen des § 217f SGB V aber auch der gematik im Kontext ePA erfüllt. Bei den Standard Authentifizierungsverfahren ist der Standard OpenID Connect dem reinen OAuth2 vorzuziehen, da hier mehr und genauer die jeweiligen Prozesse beschrieben sind und somit Probleme bei der Einbindung vermieden werden. Das ePA IAM bietet flexible Möglichkeiten der Nutzung von Erstregistrierungsmodulen, um den Versicherten einwandfrei zu identifizieren.
IDP	Identity Provider
Integrated Circuit Card Serial Number (ICCSN)	Eindeutige Identifikationsnummer einer eGK. Die ICCSN hat als Bestandteile das Branchenkennzeichen, das Länderkennzeichen, den Kartenherausgeberschlüssel und eine fortlaufende Nummer. Die ICCSN einer eGK wird automatisch vom Kartenapplikationsmanagementsystem erzeugt. Sie wird auf dem Chip der eGK gespeichert und ist in der Regel auf der Rückseite der Karte aufgedruckt.
Integrating the Healthcare Enterprise (IHE)	Initiative von Anwendern und Herstellern mit dem Ziel, den Datenaustausch zwischen IT-Systemen im Gesundheitswesen zu standardisieren und zu harmonisieren.
KIM	Kommunikation im Medizinwesen
Klickdummy	Ein Klickdummy ist ein klickbarer Prototyp, der im Zuge einer Web- oder Softwareentwicklung – also bspw. beim Entwurf von Websites oder der Programmierung von Webanwendungen – frühzeitiges Feedback der Anwender ermöglicht.
Kontrollierte Inbetriebnahme	Die kontrollierte Inbetriebnahme ersetzt den bisher geplanten Feldtest für die ePA. Die Anbieter der ePA-Aktensysteme werden in der Produktivumgebung die kontrollierte Inbetriebnahme durchführen. Dabei sollen grundsätzlich die Funktionen von „Lesen aus der Akte“ und „Schreiben in die Akte“ über den Versicherten bzw. seine ePA-App und die Leistungserbringer sichergestellt werden. Hat der Anbieter einen schriftlichen Nachweis über eines der beiden Verfahren erbracht, kann das ePA-Aktensystem bundesweit angeboten werden.
Krankenkassenwechsel	Bei einem Kassenwechsel bleibt der Aktenanbieter (beispielsweise BITMARCK) gleich. Der Versicherte nutzt weiterhin die Akte beim gleichen Anbieter.

Krankenversichertennummer (KVNR)	Mit Einführung der eGK wurde aus der bisher kassenindividuell festgelegten KVNR eine kassenübergreifend gültige KVNR. Ein Versicherter behält diese zukünftig sein Leben lang. Basis für die KVNR ist die Rentenversicherungsnummer (RVNR). Die RVNR wird von der „Datenstelle der Deutschen Rentenversicherung" (DSRV) vergeben. Die Vergabe der KVNR (bundeseinheitlicher krankenkassenübergreifender Nummernkreis) erfolgt durch die „Vertrauensstelle Krankenversichertennummer" (ITSG). Das Verfahren zur Vergabe einer KVNR wird über die Kasse gesteuert. Der Versicherte liefert nur die dafür notwendigen Daten.
KTR	Kostenträger
KVS	Kontoverwaltungssystem
Leistungserbringer (LE)	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. Leistungserbringer werden im deutschen Gesundheitssystem alle Personen und Organisationen genannt, die Leistungen für die Versicherten der Krankenkassen erbringen. Alle Leistungserbringer müssen über ein Institutionskennzeichen (IK) verfügen. Dieses IK ist Bedingung für die Abrechnung von erbrachten Leistungen mit den Krankenkassen. Zu den Leistungserbringern zählen beispielsweise Ärzte und Physiotherapeuten.
Leistungserbringerinstitution (LEI)	Die in organisatorischen Einheiten oder juristischen Personen zusammengefassten Leistungserbringer (z.B. Arztpraxen, Krankenhäuser).
Letter of Intent (LoI)	Durch diese Absichtserklärung werden im Rechtswesen Willenserklärungen von Verhandlungspartnern verstanden, die das Interesse an Verhandlungen oder am Abschluss eines Vertrags bekunden sollen. Die Erklärungen werden von einem oder von mehreren Verhandlungspartnern abgegeben.
Minimum Viable Product (MVP)	MVP ist die erste minimal funktionsfähige Ausführung eines Produkts bzw. einer Software.
MIO	Medizinisches Informations Objekt
Mockup	Ein Mockup ist ein digital gestalteter Entwurf von einer Website und / oder App. Mockups dienen der Visualisierung. Sie beinhalten Navigationsstruktur, Site- und Design-Elemente im Detail.
NFC	Near Field Communication
NFDM	Notfalldatenmanagement
nPA	Elektronischer Personalausweis
OGS	Online Geschäftsstelle
OMS	Output Management System
Open Authorization 2.0 (OAuth2)	OAuth2 = Die Abkürzung OAuth steht für Open Authorization und ist ein offenes Protokoll, das eine sichere Autorisierung von Webservices oder mobilen Anwendungen ermöglicht, ohne Drittanbietern Passwörter offenlegen zu müssen. Das Protokoll verwendet eine tokenbasierte Autorisierung und Authentifizierung. Der Prozess zum Erhalt eines Tokens nennt sich Flow. Das Open Authorization-Framework 2.0 wurde im Jahr 2012 im RFC 6749 verabschiedet. Kurz gesagt: OAuth 2.0 bildet das Autorisierungsprotokoll und ist nicht dafür vorgesehen Identitätsinformationen weiter zu geben. Es beantwortet also die Frage „Was darf ich?“ als Nutzer und beschäftigt sich mit den Berechtigungen eines Users.

OpenID Connect (OIDC)	OpenID Connect (OIDC) = OpenID basiert auf einem dezentralen Konzept und nutzt URL-basierte Identitäten (IDs) für die Anmeldung bei Web-Diensten. Mit Hilfe dieser Identitäten ist es möglich, sich bei mehreren Diensten ohne erneute Eingabe von Usernamen und Passwort anzumelden. Das Konzept unterstützt damit Single-Sign-on. Im Jahr 2014 verabschiedete die OpenID Foundation eine komplett überarbeitete Version des Protokolls mit der Bezeichnung OpenID Connect. Um für eine bessere Unterstützung von mobilen Anwendungen und für mehr Interoperabilität zu sorgen, nutzt die neue Version das so genannte OAuth 2.0-Framework. Ziel des neuen Protokolls ist eine breitere Akzeptanz und mehr Möglichkeiten für Single-Sign-on-Verfahren im Netz zu schaffen. Kurz gesagt: OpenID Connect macht die Authentifizierung und stellt die Frage „Wer bin ich?“. Das Protokoll bildet dazu mit Hilfe von ID Tokens die Identität des Nutzers ab. OpenID Connect bildet damit die Erweiterung von OAuth 2.0 um Authentifizierungsaspekte.
Patientendaten-Schutzgesetz (PDSG)	Mit dem Patientendaten-Schutzgesetz werden digitale Angebote wie die elektronische Patientenakte nutzbar und sensible Gesundheitsdaten gleichzeitig bestmöglich geschützt.
Persönliche Identifikationsnummer (PIN)	Die Freischaltung des Zugriffs auf Anwendungsdaten einer eGK sowie der personenbezogenen Schlüssel erfolgt durch die Eingabe persönlicher Geheimnummern (PINs). PINs sind Kernbestandteile einer jeden eGK. Sie haben eine Länge von 6-8 Ziffern. Sie sind ausschließlich für den Karteninhaber bestimmt und dürfen zur Sicherstellung der Datenvertraulichkeit nur ihm selbst bekannt sein.
Public Key Infrastructur (PKI)	Eine PKI ist ein System, welches es ermöglicht Zertifikate für öffentliche Schlüssel auszustellen, zu verteilen und zu prüfen. Die Zertifikate werden dazu genutzt die öffentlichen Schlüssel, die in allgemein zugänglichen Verzeichnissen bereitgestellt werden, eindeutig ihren Besitzern zuzuordnen.
RISE	Research Industrial Systems Engineering
SDK	Software Development Kit
Secure Module Card (SMC)	SMC = Secure Module Card (elektronischer Ausweis) Die Secure Module Card (SMC) ist ein institutionsbezogener Ausweis, mit dem sich Institutionen der Leistungserbringer, z. B. Arztpraxen oder Krankenhäuser, gegenüber der Telematikinfrastruktur (TI) ausweisen. Dieser Ausweis ist für den Zugriff auf die Daten der eGK erforderlich, sofern der Patient diese freigegeben hat. Er hat das Format einer SIM-Karte (identisch einer Handykarte) und ist mit einem Mikroprozessorchip ausgestattet. Die Ausgabe erfolgt durch jeweils festgelegte Stellen, z. B. die Kassenärztlichen Vereinigungen (KV) für Arztpraxen oder die Deutsche Krankenhausgesellschaft (DKG) für Krankenhäuser. Diese Organisationen stellen sicher, dass die SMC nur an berechtigte Institutionen ausgegeben wird. Man unterscheidet zwischen der SMC-A- und der SMC-B-Karte. Die SMC-A-Karte enthält die Schlüssel, um auf die eGK zuzugreifen. Sie ist im Kartenterminal eingesetzt. Die SMC-B-Karte enthält alle Funktionen der SMC-A-Karte und dient darüber hinaus zur Identifikation der Institution gegenüber der Telematikinfrastruktur (TI). Sie kann im Konnektor oder in ein durch den Konnektor nutzbares Kartenterminal gesteckt sein.
SGD1	Schlüsselgenerierungsdienst Typ 1
SGD2	Schlüsselgenerierungsdienst Typ 2
SigD	Signaturdienst
SIGU	Sicherheitsgutachten

SSO	Single Sign On
Stacktrace	Ein Stack-Trace ist ein Bericht, der Informationen über Programmunterprogramme bereitstellt. Es wird häufig für bestimmte Arten des Debuggens verwendet, bei dem ein Stack-Trace Softwareingenieuren dabei helfen kann, herauszufinden, wo ein Problem liegt oder wie verschiedene Subroutinen während der Ausführung zusammenarbeiten.
SÜV	Sichere Übermittlungsverfahren
SZZP	Sicherer zentraler Zugangspunkt zur TI
TAGS	Dieser Begriff wird in der Informatik zur Markierung oder Kennzeichnung bestimmter Werte benutzt.
TeS	Telematik Services
TI	Telematikinfrastruktur
TSP	Trust Service Provider
UEePA	Übergangsregelung ePA
Universally Unique Identifier (UUID)	Der Universally Unique Identifier, kurz UUID, ist ein Standard für Identifikationsnummern. Immer dann, wenn Informationen zweifelsfrei auseinandergehalten werden müssen, kann eine einzigartige ID helfen. Im Kontext der ePA ist die UserId eine UUID und wird pro App Session neu generiert.
VAU	Vertrauenswürdige Ausführungsumgebung
Verzeichnisdienst (VZD)	Der VZD ist ein zentraler Dienst der TI-Plattform. Er beinhaltet die Speicherung aller Einträge von Leistungserbringern und Institutionen mit allen definierten Attributen, die in das Verzeichnis aufgenommen werden sollen und die Fachdaten durch fachanwendungsspezifische Dienste. Anhand einer Suchanfrage können Clients und fachanwendungsspezifische Dienste Basis- und Fachdaten abfragen (z. B. X.509-Zertifikate). Ferner können Einträge des Verzeichnisses durch berechtigte fachanwendungsspezifische Dienste geändert, hinzugefügt und gelöscht werden.
VHD	Versicherten-Help-Desk
VIP–Kennzeichen	Die Bezeichnung VIP-Kennzeichen ist hier nur als Oberbegriff für eine Kennzeichnung zu sehen, die wie folgt lauten kann: 0 = keine geschützte Person 1 = geschützte Person 6 = besonders geschützte Person 7 = VIP Umgangssprachlich hat sich im BITMARCK-System der Oberbegriff für eine solche Kennzeichnung mit „VIP-Kennzeichen“ manifestiert. Gemeint ist hier jedoch die oben genannte grundsätzliche Kennzeichnung aller vorhandenen Kennzeichen.