

Einführung der Gesundheitskarte

Glossar

Version: 1.7.0
Stand: 30.03.2007
Status: freigegeben

Dokumentinformationen

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.64	31.08.05	Alle	Aktualisierter Stand zu Meilenstein 4	gematik, IQS
0.0.9	07.02.06	Alle	Dokument wurde neu strukturiert und um weitere Glossarbegriffe ergänzt	gematik, IQS
1.0.0	28.03.06	3	Ergänzung der Abkürzungen, Überarbeitung des Glossars (Erläuterungen, Begriffe)	gematik, IQS
1.1.0	17.05.06	3	Ergänzung der Abkürzungen, Begriffe, Inhaltsverzeichnis	gematik
1.2.0	02.06.06	3	Ergänzungen, insbesondere Netzwerk-Begriffe	gematik
1.3.0	14.06.06	3	Ergänzungen Begriffe der Gesamtarchitektur, Einarbeitung Kommentare von extern	gematik
1.4.0	21.07.06	3	Ergänzung Begriffe Betrieb, Abkürzungen AG2, Kommentare	gematik
1.4.3	19.10.06		Anwendungsfall, Einarbeiten von ITIL-Begriffen, Ergänzung Begriffe Netzwerksicherheit	gematik, IQS
1.5.0	31.10.06		Freigabe	gematik
1.5.1	20.11.06	3	Überarbeitung Akkreditierung	gematik, IQS
1.5.2	23.01.07	3	Änderung Begriffe Anwendungsfall, Use Case, Akteure, Aktion	gematik, IQS
1.5.3	12.02.07	3	Änderung/Ergänzung zu Begriffen des Anforderungsmanagements (Anforderungsmeldung, Quittung der Anforderungsmeldung, Anforderung, Auftragsanforderung, Umsetzungs-, Eingangs-, Ausgangs-, Status im Anforderungsmanagement, Change Request, Release und Releasedefinition)	gematik, IQS
1.6.0	12.02.07		freigegeben	gematik
1.6.1	14.03.07	3	Änderung/Ergänzung zu Begriffen des Anforderungsmanagements (Anforderungsmeldung, Ausgangs-, Auftrags-, Umsetzungs-, Sicherheits-, funktionale- und nicht-funktionale-, Leistungs-, Eingangs- und Änderungsanforderung, Anforderung, Releasedefinition, Quittung der Anforderungsmeldung, Benutzbarkeit und Benutzerfreundlichkeit)	gematik, IQS
1.7.0	30.03.07		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen	2
Inhaltsverzeichnis.....	3
1 Zusammenfassung	4
2 Einführung.....	5
2.1 Zielsetzung und Einordnung des Dokumentes	5
2.2 Zielgruppe.....	5
2.3 Geltungsbereich.....	5
2.4 Arbeitsgrundlagen	5
2.5 Abgrenzung des Dokumentes	5
2.6 Notation.....	5
3 Glossar.....	6
Anhang	74
A1 – Abkürzungen	74
A2 - Glossar	74
A3 - Abbildungsverzeichnis.....	74
A4 - Tabellenverzeichnis	74
A5 - Referenzierte Dokumente.....	74

1 Zusammenfassung

Das vorliegende Glossar enthält die Definitionen und Erläuterungen der Begriffe und Abkürzungen, welche in den Ergebnisdokumenten des Projektes zur Einführung der elektronischen Gesundheitskarte verwendet werden.

Es wird als zentrales Verzeichnis geführt, eine Erläuterung der Begriffe in den Einzeldokumenten ist in der Regel nicht vorgesehen.

Zum Verständnis der Erläuterungen ist zu berücksichtigen, dass sich Definition und Verwendung der Begriffe am Kontext der Telematik im Gesundheitswesen und speziell an der Einführung der Gesundheitskarte orientieren.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Das Dokument definiert die im Projekt zur Einführung der Gesundheitskarte verwendeten Fachbegriffe. Es soll zu einem gemeinsamen Verständnis zu diesen Begriffen beitragen.

2.2 Zielgruppe

Das Dokument dient den Lesern der Ergebnisdokumente zur Klärung begrifflicher Divergenzen. Gleichzeitig wird es innerhalb des Projektes zur Vereinheitlichung der Fachausdrücke herangezogen.

2.3 Geltungsbereich

Die Begriffe sind innerhalb des Projektes zur Einführung der Gesundheitskarte verbindlich anzuwenden.

2.4 Arbeitsgrundlagen

Die Begriffe werden im Rahmen der Projektarbeit in Form einer Excel-Tabelle definiert und gepflegt. Das vorliegende Dokument gibt den zur Veröffentlichung bestimmten Auszug aus diesem Bestand wieder.

2.5 Abgrenzung des Dokumentes

Das Dokument hat nicht das Ziel, Verfahren und Spezifikationen zu ersetzen. Begriffe werden daher nur insoweit erläutert, als es zu ihrem Verständnis und ihrer Abgrenzung erforderlich ist.

2.6 Notation

Begriffe und Abkürzungen sind in der linken Spalte erläutert. Der englische Fachbegriff (auch die englische Übersetzung einer Abkürzung) wird in Spalte 2 angeführt. Zu den Begriffen bestehende Abkürzungen sind in der Spalte 2 in Klammern gesetzt.

Die Definition eines Begriffes wie auch die deutsche Übersetzung einer Abkürzung sind in der dritten Spalte eingetragen. Hier finden sich auch Hinweise auf wesentliche Synonyme.

Kursiv geschriebene Begriffe in der Definition sind ihrerseits im Glossar definiert.

3 Glossar

Begriff	Englisch, (Abk.)	Definition (Synonym)
1st Level Support		Erste öffentliche Ansprechpartner im Support
2nd / 3rd Level Support		Nachgelagerte Supportabteilungen zur Lösung tiefergehender Probleme
3DES	Triple-DES	Betriebsmodus des <i>DES</i> , der gegenwärtig noch sicher ist. Dabei wird <i>DES</i> dreimal hintereinander angewendet.
A		
AB		<ol style="list-style-type: none"> 1. Betriebliche <i>Anforderung</i> 2. Architekturboard
ABDA		Bundesvereinigung Deutscher Apothekerverbände
Ablaufdatum	expiration date	Datum, ab dem eine zugesicherte Leistung nicht mehr verfügbar ist (Synonym: gültig bis).
Abnahmetest	acceptance trial	Test eines Produktes, in dem geprüft wird, ob das Produkt die Anforderungen der <i>Spezifikation</i> erfüllt.
ABS		Acrylnitril-Butadien-Styrol
Access Controll Information	(ACI)	ACI bezeichnet Datensätze, in denen Informationen über Zugangsberechtigungen verschiedener Identitäten abgelegt sind
ACI	Access Controll Information	
Administrative Hoheit		Verantwortlichkeit für das zweckorientiert und gesetzeskonforme Funktionieren eines <i>Systems</i>
Administrator		Fachpersonal zum Aufbau und Betrieb der <i>Telematikinfrastruktur</i> und der vorhandenen <i>Primär-</i> und <i>Back-End-Systeme</i> .
ADSL	Asymmetric Digital Subscriber Line	Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über eine normale Telefonleitung.
ADT		Abrechnungsdatenträger (Standard der KBV)
AE		Architekturentscheidung
AES	Advanced Encryption Standard	Standard für ein symmetrisches Kryptosystem
AF		Funktionale <i>Anforderung</i>
AHB		Anschlussheilbehandlung
AID	Application Identifier	Kennung zur Identifikation einer Software
AkdÄ		Arzneimittelkommission der deutschen Ärzteschaft

Begriff	Englisch, (Abk.)	Definition (Synonym)
Akkreditierung	accreditation	<p>Prozess der Überprüfung bzw. Bescheinigung der erfolgreichen Überprüfung bzgl. der Erfüllung einer besonderen Eigenschaft.</p> <p>Die Akkreditierung ist gemäß § 2 Nr. 15 des Signaturgesetzes ein freiwilliges „Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.“</p> <p>Die Akkreditierung von Telematik-Services ermöglicht die gegenseitige Authentisierung der Dienste innerhalb der Telematikinfrastruktur.</p>
Akkreditierungsstelle	accreditation body	Die Akkreditierungsstelle ist eine Organisation oder Institution, welche Akkreditierungen durchführt. Die Befugnis leitet sich im Allgemeinen von hoheitlichen Stellen ab.
Akteur	actor	<p>Ein Akteur ist eine gewöhnlich außerhalb des betrachteten bzw. zu realisierenden <i>Systems</i> liegende Einheit, die an der in einem <i>Anwendungsfall</i> beschriebenen Interaktion mit dem <i>System</i> beteiligt ist.</p> <p>Ein Akteur kann ein Mensch sein, z. B. ein <i>Benutzer</i>, ebenso aber auch ein anderes technisches <i>System</i>. [Oestereich]</p> <p>Akteure sind beispielsweise die Anwender des <i>Systems</i>. Bei den Akteuren werden jedoch nicht die konkreten beteiligten Personen unterschieden, sondern ihre <i>Rollen</i>, die sie im Kontext des <i>Anwendungsfalls</i> einnehmen.</p>
Aktion		Eine Aktion stellt die fundamentale Einheit ausführbarer Funktionalität dar, die im Modell nicht weiter zerlegt wird und somit atomar ist. Die Aktionen innerhalb der einzelnen <i>Anwendungsfälle</i> werden in den <i>Fachkonzepten</i> der gematik aus fachlicher Sicht beschrieben. Dabei werden nur diejenigen Aktionen definiert, die von den <i>Akteuren</i> in Verbindung mit einem <i>Informationsobjekt</i> ausgeführt werden.
Aktualitätsprüfung	currency check	Die von einem autorisierten und authentifizierten <i>Leistungserbringer</i> angestoßene Prüfung mit dem Ziel, den <i>Versicherten</i> betreffende Daten zu prüfen, ob diese noch aktuell sind oder ggf. zu aktualisieren sind (aktueller <i>Use Case</i> : VSD auf der eGK auf Aktualität prüfen).
AlgRef.		Algorithmus Referenz
AM	Access Mode	Zugriffsmodus
AMDD		Arzneimitteldokumentationsdienst
AMDOK		<i>Arzneimitteldokumentation</i>
AMS	Application Management System	<i>Anwendungsmanagementsystem</i> , siehe auch CAMS
AMTS		Arzneimitteltherapiesicherheit (-sprüfung)
AN		Nicht-funktionale <i>Anforderung</i>

Begriff	Englisch, (Abk.)	Definition (Synonym)
Änderungsanforderung	Change request	Schriftlich formalisierte Darstellung eines Änderungsbedarfs an Ergebnistypen eines abgestimmten Release und/oder einer abgestimmten veröffentlichten Version. Change Requests sind immer entscheidungs- und bewertungsrelevant.
AnF		Funktionale Annahme
Anforderung	requirement	<p>Vor der Entwicklung von Produkten werden die Eigenschaften festgelegt, welche das Produkt erfüllen muss. Dabei wird nach fachlichen (welche Funktion muss das Produkt erfüllen), technischen (wie muss die Funktion umgesetzt werden), betrieblichen (was muss die das Produkt leisten) Aspekten und solchen der Sicherheit differenziert.</p> <p>Im Rahmen des Projektes zur Einführung der Gesundheitskarte gilt aus Sicht des Anforderungsmanagements:</p> <p>Beschreibung einer gewünschten Eigenschaft des Produktes „Telematikinfrastruktur“, die ausschließlich auf folgende konzeptionelle Ergebnistypen inhaltlich wirkt:</p> <ul style="list-style-type: none"> * Fachkonzept * Facharchitektur, Gesamtarchitektur * Spezifikation * Releasedefinition <p>Anforderungen werden klassifiziert und aus speziellen Sichten gruppiert.</p> <p>Abgegrenzte Begriffe, die nicht dieser Definition unterliegen:</p> <ul style="list-style-type: none"> * Testanforderung: Anforderungen an den Test der Telematikinfrastruktur * Betriebsanforderung , Incident-Meldung: Anforderungen an den Betrieb der Telematikinfrastruktur * Sicherheitsanforderung: Sicherheitsanforderungen mit Geheimhaltung * Risikobetrachtungen
Anforderungsmeldung	Demand note	<p>Schriftlich formalisierte Darstellung einer Anforderungsidee als ausschließliches Kommunikationsmittel für den Entscheidungs- und Bewertungsprozess von Anforderungen.</p> <p>Datenhaushalt:</p> <ul style="list-style-type: none"> * Anforderungssteller (Name, Organisationseinheit, E-Mail, Telefon) * Erstellungsdatum * Bezug (optional) * Anforderungstext * Anforderungserläuterung (optional) * Dringlichkeit, Zusammenhänge (optional)
Anmeldename	login, login name	Benutzername, mit dem sich ein Benutzer gegenüber einem IT-System anmelden kann.
AnN		Nicht-funktionale Annahme
AnS		Annahme zur Sicherheit
ANSI	American National Standards Institute	Amerikanisches Normungsinstitut, mehrere seiner Standards wurden in internationale Normen übernommen (ANSI-ASCII, DES, X.9.31 (RSA). X9.53 (3DES), X9.62 (ECDSA))

Begriff	Englisch, (Abk.)	Definition (Synonym)
Anwendung	application	Einsatzbereich bzw. Nutzung der eGK. Über § 291a SGB V festgelegte Anwendungen sind z.B. eRezept oder freiwillige Anwendungen. Zu den Anwendungen auf der eGK gehören, Bereiche mit anwendungsspezifischen Daten und zugehörigen Zugriffsschutzregeln, hier jedoch kein ausführbarer Code. Synonym: Applikation
Anwendungsfall	Use Case	Ein Anwendungsfall (engl. Use Case) spezifiziert eine abgeschlossene Menge von <i>Aktionen</i> eines oder mehrerer <i>Akteure</i> , die von einem <i>System</i> bereitgestellt werden und einen erkennbaren fachlichen Nutzen für einen oder mehrere <i>Akteure</i> erbringen. Ein Anwendungsfall beschreibt immer nur genau einen Ablauf oder einen <i>Prozess</i> . Dabei sind neben dem Regelprozess (bestehendes oder gewünschtes Verhalten) auch die alternativen Pfade (Fehlverhalten, Sonderfälle) zu beschreiben. Die beschriebenen Abläufe dürfen jedoch nicht zu komplex werden. In den <i>Fachkonzepten</i> der gematik werden rein fachliche Anwendungsfälle beschrieben. Zur besseren Abgrenzung von den fachlichen Anwendungsfällen wird in den technisch ausgerichteten Dokumenten (<i>Facharchitekturen</i> , <i>Spezifikationen</i>) der Begriff "Use Case" für die technischen Anwendungsfälle (Technischer Use Case = <i>TUC</i>) verwendet.
Anwendungsgateway		Anwendungsgateways sind Infrastruktur-Bestandteile, die spezifische Protokoll-Anfragen entgegen nehmen, diese auf syntaktische Korrektheit sowie Sicherheitsrisiken und potentiell Berechtigungen hin überprüfen und an eine Backend-Anwendung weiterleiten. Hierdurch wird ein direkter Zugriff aus einer unsicheren Zone auf eine schützenswerte Anwendung verhindert und somit ein erhöhtes Sicherheitsniveau erreicht
Anwendungsmanagement	application management	Betreuung von <i>Systemen</i> und <i>Anwendungen</i> , um einen reibungslosen Betrieb aufrecht zu erhalten. Beschreibt im Zusammenhang mit der eGK das interne Management bzw. die Administration der zur Verfügung gestellten Anwendungen innerhalb des <i>Kartenmanagements</i> im Gegensatz zum Begriff <i>Kartenanwendungsmanagement</i> . Synonym: Applikationsmanagement
Anwendungsmanagementsystem	application management system (AMS)	<i>System</i> für das <i>Anwendungsmanagement</i> . Synonym: Applikationsmanagementsystem
API	Application Programming Interface	Ein Application Programming Interface ist eine dokumentierte Software-Schnittstelle, mit deren Hilfe ein Software-System bestimmte Funktionen eines anderen Software-Systems nutzen kann.
Apothekenteil		Apothekenteil (des <i>eRezeptes</i>): Teilbereich des Datensatzes <i>eRezept</i> , der nach Einlösung einer elektronischen Verordnung in der Apotheke zu dem Datensatz <i>eRezept</i> hinzugefügt wird. Dieser Teil enthält z.B. die Dispensierdaten und die <i>Signatur</i> des Apothekers.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Applikationsform		Darreichungsform eines Arzneimittels oder einer Rezeptur. Eine normative Liste der Benennungen und Abkürzungen ist in der Datensatzbeschreibung <i>eRezept</i> enthalten (Beispiel: Tablette, Tab.).
Approbierter Heilberufler		Eine natürliche Person (<i>Arzt</i> , Apotheker, Zahnarzt) mit gültiger Approbation (Zulassung der Ärzte-, Zahnärzte- oder Apothekerkammer), die sie berechtigt entsprechende Heilbehandlungen durchzuführen.
Arbitration		Konfliktlösungsverfahren, bei dem ein neutraler Dritter den Vorsitz hat (Schlichtung).
Architektur	architecture	Eine Architektur beschreibt den prinzipiellen Aufbau eines <i>Systems</i> , seine Zerlegung in Bausteine, die Festlegung ihrer Aufgaben und die Beschreibung des Zusammenwirkens der Bausteine. Dazu gehört auch die Festlegung, welche Aufgaben eine IT-Infrastruktur übernimmt.
Architektursichten		Beschreibt einen technisch orientierten Blickwinkel aus Sicht definierter Systemanforderungen. Im Rahmen der hier entwickelten Referenzarchitektur werden die fünf Sichtweisen des RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) verwendet: <i>Enterprise View</i> , <i>Computational View</i> , <i>Information View</i> , <i>Engineering View</i> und <i>Technology View</i> .
ARR	Access Rule Reference	
Arzneimittel-Dokumentation		Dokumentation der durch einen <i>Leistungserbringer</i> verordneten, dispensierten und applizierten Arzneimittel. Die Dokumentation erfolgt zu einem <i>Versicherten</i> als freiwillige <i>Anwendung</i> in einer einheitlichen elektronischen Datenstruktur mit dem Ziel, die versorgenden <i>Ärzte</i> und Apotheker über die aktuelle Medikation des <i>Patienten</i> zu informieren und eine automatische Erkennung von Arzneimittelrisiken und Nebenwirkungen durch die Fachinformationssysteme von <i>Arzt</i> und Apotheker zu ermöglichen.
Arzt	doctor, physician	Unter dem Begriff wird aus dem Akteursmodell zusammengefasst ein Arzt, eine Ärztin, ein Zahnarzt oder eine Zahnärztin mit Approbation verstanden.
Arztbrief		Signierte papiergebundene oder elektronische Dokumentation eines <i>Arztes</i> oder Zahnarztes mit partiell vertraglich vorgegebenen Bestandteilen zu einem <i>Versicherten</i> und dessen Krankheitsgeschehen mit dem Ziel, dass ein anderer <i>Leistungserbringer</i> darüber informiert wird. Beispiele: Krankenhausentlassbrief oder Unfallbericht.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Ärztliche Verordnung		Signierte Verschreibung von Leistungen im Sinne des § 291 a und §73 Abs. 2 SGB V durch einen <i>Arzt</i> für medizinische Rehabilitation, Arznei-, Verband-, Heil- und Hilfsmittel, Krankentransporte, Krankenhausbehandlung oder Behandlung in Vorsorge- oder Rehabilitationseinrichtungen, häuslicher Krankenpflege oder Sozialtherapie.
Arztpraxispersonal		Personal der <i>Arzt-</i> oder <i>Zahnarztpraxis</i> oder des Krankenhauses, welches auf Weisung des <i>Arztes</i> oder <i>Zahnarztes</i> im Rahmen des <i>SGB V</i> handelt. Beispiel: <i>Arztthelferin</i> .
Arztteil		Teil des Datensatzes <i>eRezept</i> , der vom <i>Arzt</i> erstellt wird. Enthält z.B. Daten des <i>Versicherten</i> und des <i>Arztes</i> , die <i>Verordnung</i> und die <i>Signatur</i> des <i>Arztes</i> .
AS		Sicherheitsanforderung
ASN.1	Abstract Syntax Notation One	Notation für Datenformate
AT	Authentication Template	
ATR	Answer to Reset	
Attribut	attribute	Ein Attribut ist ein beschreibendes Merkmal und definiert eine Eigenschaft eines <i>Informationsobjekts</i> . Beispielsweise kann das <i>Zertifikat</i> einer <i>elektronischen Signatur</i> ein Attribut enthalten, aus dem hervorgeht, dass der Zertifikatsinhaber ein <i>Arzt</i> ist.
Attributbestätigungsinstanz		Eine Attributbestätigungsinstanz ist Teil einer <i>PKI</i> und bescheinigt, dass der Antragsteller für ein <i>Zertifikat</i> eine bestimmte Eigenschaft besitzt, so dass diese als <i>Attribut</i> in das beantragte <i>Zertifikat</i> aufgenommen werden kann.
Attributzertifikat		Ein Attributzertifikat ist ein <i>Zertifikat</i> , das selbst keinen <i>öffentlichen Schlüssel</i> enthält sondern lediglich in eindeutiger Weise auf ein <i>Public-Key-Zertifikat</i> verweist. Es wird verwendet, um dem referenzierten <i>Public-Key-Zertifikat</i> weitere <i>Attribute</i> zuzuweisen.
Auftragsanforderung	order requirement initial requirement	Klassifizierung von Anforderung Anforderungen, die im Sinne einer Weisung (verbindlich, bewertungsrelevant) oder im Sinne eines Auftrages (unverbindlich, entscheidungs- und bewertungsrelevant) an die gematik gehen.
Augenschein und Augenscheinsbeweis		Augenschein ist jede unmittelbare sinnliche Wahrnehmung durch eine für ein Gericht oder eine Behörde tätige Person mit dem Ziel, beweis erhebliche Tatsachen festzustellen (z. B. durch Sehen, Hören, Riechen). Der Beweis durch Augenschein (Augenscheinsbeweis), der im Zivilprozessrecht in §§ 371 ff geregelt ist, umfasst alle Beweismittel, die nicht als Zeugen-, Urkunden-, oder Sachverständigenbeweis gesetzlich besonders geregelt sind

Begriff	Englisch, (Abk.)	Definition (Synonym)
Ausgangs-anforderung	output requirement	Anforderungssicht Eine Anforderung aus Sicht eines Konzeptes, die dieses Konzept für Folgekonzepte als <i>Eingangsanforderung</i> ermittelt hat
AUT	authentication	<i>Authentifizierung</i>
AUT IDEM		Binäres Kennzeichen auf dem Rezeptformular oder im eRezeptdatensatz, durch welches der Arzt kenntlich macht, dass eine Ersetzung eines Arzneimittels durch ein wirkstoffgleiches zulässig oder ausgeschlossen sein soll.
Auth	authentication	<i>Authentisierung</i>
Authentifizierung	authentication (AUT)	Die Authentifizierung bezeichnet den Vorgang, die <i>Identität</i> einer Person oder eines Rechnersystems an Hand eines bestimmten Merkmals zu überprüfen. Die Authentifizierung stellt die Frage: Ist das die Person, die sie vorgibt zu sein?
Authentifizierungsdaten (-informationen)	credentials	Daten, die zur Überprüfung einer behaupteten <i>Identität</i> geeignet sind.
Authentisierung	authentication (Auth)	Dies ist ein Verfahren zum Nachweis einer <i>Identität</i> . Als Beispiel kann die Passwortabfrage beim Starten eines Rechners genannt werden. Die Authentisierung beantwortet die Frage: Bin ich die Person, die ich vorgebe?
Authentizität	authenticity	Authentizität bezeichnet den Zustand, in dem die <i>Identität</i> eines Kommunikationspartners bzw. die Urheberschaft an einem Objekt sichergestellt ist. Unter dem Nachweis der Authentizität von elektronischen Daten versteht man den Nachweis über die Echtheit der Daten (<i>Integrität</i>) und die eindeutige Zuordnung zum Verfasser, Ersteller und/oder Absender.
Autorisierung		Die Autorisierung beschreibt i. A. die Vergabe der Erlaubnis, etwas Bestimmtes zu tun (Rechteverwaltung). Im Kontext <i>Gesundheitskarte</i> wird der Begriff insbesondere im Sinne von § 291a, Abs. 5 SGB V/GMG verwendet. So wird mittels der Autorisierung durch den <i>Patienten</i> bspw. definiert, ob ein im Vorfeld authentifizierter <i>Arzt (Authentifizierung)</i> eine <i>elektronische Patientenakte</i> lesen, schreiben oder ändern kann.
Autorisierungsverfahren	authorization mechanism	Verfahren zur Vergabe und Verteilung von Zugriffsrechten an eine Person oder ein <i>System</i> (Subjekt) auf Daten oder Anwendungen (Objekt).
Availability Management	(AvM)	ITIL-basierter Prozess, der die kosteneffektive Bereitstellung von IT-Services auf dem im <i>SLA</i> vereinbarten Verfügbarkeitsniveau gewährleistet. Dazu gehört die strategische Planung der Gewährleistung der Verfügbarkeit, aber auch die Überwachung der tatsächlichen Verfügbarkeit von IT-Services.
AVS		Apothekenverwaltungssystem, <i>Primärsystem</i> der Apotheke

Begriff	Englisch, (Abk.)	Definition (Synonym)
B		
B	Byte	digitales Speicherformat für 1 Zeichen
BA		Berufsausweis für Mitarbeiter im Gesundheitswesen (siehe auch HBA)
Backbone		Als Backbone wird ein zentrales Netzwerksegment mit hoher Bandbreite bezeichnet, dessen Aufgabe es üblicherweise ist, mehrere angeschlossene Netzwerke mit einander zu verbinden
BÄK		Bundesärztekammer
BAND		Bundesvereinigung der Arbeitsgemeinschaften der Notärzte Deutschlands
Basic Input Output System	(BIOS)	Basis-Betriebssystem eines jeden x86 konformen Rechnersystems (unabhängig davon, ob es sich um einen PC oder einen Server handelt). Es ist die Software, die der Rechner direkt nach dem Einschalten lädt. Sie steuert den POST (Power On Self Test) und steht dem Steuerwerk der CPU direkt zur Verfügung. Es ist – wie eine Firmware auch – im Allgemeinen in einem nicht flüchtigen Speicher (Non volatile RAM) abgelegt.
BCD	Binary Coded Decimal	Binär kodierte Dezimalzahldarstellung, bei der jede Ziffer einzeln durch 4 oder 8 Bit dargestellt wird
BDSG		Bundesdatenschutzgesetz
Bedrohung	threat	Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die <i>Verfügbarkeit</i> , <i>Integrität</i> oder <i>Vertraulichkeit</i> von Informationen so gefährden kann, dass dem Besitzer der Informationen ein Schaden entsteht. Bedrohungen können sich aus Einwirkungen durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen ergeben.
Befruchtung, künstliche		binäres Kennzeichen zu einer Leistung, die im Zusammenhang mit einer künstlichen Befruchtung verordnet wurde (§27a SGB V).
Benutzer	user	Wird einer <i>Identität</i> das Recht für den Zugriff auf ein oder mehrere <i>Systeme</i> beispielsweise durch die Vergabe einer <i>Rolle</i> erteilt, so spricht man von einem Benutzer. Einer <i>Identität</i> können mehrere Benutzer zugeordnet werden. Ein Benutzer kann mehrere <i>Anmeldenamen</i> besitzen, mit deren Hilfe er sich gegenüber verschiedenen IT-Systemen anmelden kann.
Benutzbarkeit	chance of use	Die Benutzbarkeit eines Produktes definiert sich durch den Erfüllungsgrad aller <i>funktionalen Anforderungen</i> , angelehnt an die Qualitätsmerkmale der DIN 66272.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Benutzerfreundlichkeit	ease of use	Die Benutzerfreundlichkeit eines Produktes definiert sich durch den Erfüllungsgrad aller <i>nicht-funktionalen Anforderungen</i> .
BER	Basic Encoding Rules	
Beschaffungskosten		Kosten für die Beschaffung von Arzneimitteln, die nicht über den apothekenüblichen Bezugsweg beschafft werden können
Betäubungsmittel	(BtM)	Narkotisierende, schmerzreduzierende oder sonstige verschreibungspflichtige Arzneimittel mit Hervorrufen einer Abhängigkeit im Sinne des Betäubungsmittelgesetzes (BtMG) nach Anlage I bis III (aufgeführte Stoffe und Zubereitungen, z.B. Morphin-N-oxid).
Betriebsumgebung		Die Betriebsumgebung beschreibt eine in sich geschlossene Infrastruktur zu einem bestimmten Zweck. Beispiele für Betriebsumgebungen sind: Anwendertestumgebung, Referenzumgebung, Produktionsumgebung. Diese sind physikalisch voneinander getrennt.
Bevollmächtigter		Eine natürliche Person, die im Fall einer nicht geschäftsfähigen Person bzw. bei Verhinderung die Rechte der Person durch Vorlage oder Nachweis einer Vollmacht wahrnimmt (autorisierter Vertreter).
BfArM		Bundesinstitut für Arzneimittel und Medizinprodukte
BG-Abrechnung		Berufsgenossenschaftliche Abrechnung
Binary Large Object	(BLOB)	Binary Large Objects (BLOBs) sind große binäre und nicht weiter strukturierte Objekte beziehungsweise Felddaten. Diese werden üblicherweise dann verwendet, wenn für die speichernde oder empfangende Instanz die interne Struktur des Datenobjektes nicht relevant ist.
BinarySecurityToken		Ein BinarySecurityToken bezeichnet eine binär abgelegte Datenstruktur innerhalb des Webservice Security Standards. Diese Datenstruktur wird zum Speichern eines Security Tokens wie zum Beispiel eines <i>X.509-Zertifikates</i> verwendet und dient dazu, einen Benutzer zu authentifizieren
bindingTemplate		Element des <i>UDDI</i> Standards
Biometrisches Merkmal		Körpermerkmal, anhand dessen ein Mensch durch ein Biometrisches <i>System</i> identifiziert werden kann
BIOS	Basic Input Output System	
biT4health		Bezeichnung eines der Vorprojekte zur Vorbereitung der Einführung der Gesundheitskarte: Bessere IT für bessere Gesundheit
BLOB	Binary Large Object	
BMG		Bundesministerium für Gesundheit
BNetzA		Bundesnetzagentur, siehe RegTP

Begriff	Englisch, (Abk.)	Definition (Synonym)
Boolean		Datentyp zum Speichern der zwei Zustände: Wahr und Falsch
Broker Service	(BS)	Der Broker Service integriert einzelne Telematik-Dienste in komplexere Ablauffolgen, Telematik-Sequenzen genannt, die vom <i>Konnektor</i> aufgerufen werden können. Zur Bereitstellung dieser Telematik-Sequenzen verwendet der Broker Service die anderen Dienste des Telematik Layers (z.B. zwecks Protokollierung, Anonymisierung, usw.) sowie die Dienste des Service Provider Layers.
BS7799		Der British Standard 7799 ist eine Norm für die Auditierung und <i>Zertifizierung</i> von IT-Systemen, die in der jetzigen Form der Öffentlichkeit im 1999-04 vorgestellt wurde. Der Standard BS 7799 ist ein international anerkannter Standard für Informations-Sicherheit, der Unternehmen bei der Definition und Umsetzung einer optimalen Sicherheitsstrategie unterstützt. Er beinhaltet bestimmte Verfahren und Methoden für die Organisation und die technische Umsetzung von Informationssicherheit.
BSI		Bundesamt für Sicherheit in der Informationstechnik
BtM		Betäubungsmittel
BtM-Gebühr		Bearbeitungsgebühr für ein Betäubungsmittelrezept (BtM-Rezept) bzw. ein <i>eRezept</i> mit gekennzeichnetem BtM-Kennung, <i>BtM-Nummer</i> und verordnetem Betäubungsmittel. Die Gebühr kann in der ausgebenden Apotheke erhoben werden und beträgt zur Zeit 0,26 €.
BtM-Nummer		Eineindeutige alphanumerische 7-stellige Zahl der Erlaubnis zur Teilnahme am BtM-Verkehr, die auf Antrag vom Bundesamt für Arzneimittel und Medizinprodukte für genau einen Arzt oder Zahnarzt vergeben wird. Diese Definition wird im Projekt verwendet. Hinweis: Umgangssprachlich wird mit BtM-Nummer einerseits die fortlaufende alphanumerische 9-stellige Nummer eines BtM-Rezeptes, andererseits auch die alphanumerische 25-stellige Nummer eines <i>eRezeptes</i> bezeichnet, die sich aus Ausgabedatum, einer Prüfzahl und dem BtM-Merkmal zusammensetzt.
BtMVV		Betäubungsmittel Verschreibungsverordnung
BVG		Bundesversorgungsgesetz
C		
C	certificate	<i>Zertifikat</i>
C2C	card to card	Authentifizierungsverfahren zwischen zwei <i>Chipkarten</i>
C2S	card to server	Authentifizierungsverfahren zwischen einer <i>Chipkarte</i> und einem Server
CA	Certification Authority	Zertifizierungsinstanz

Begriff	Englisch, (Abk.)	Definition (Synonym)
Cache, cachen		Der Cache bezeichnet in der EDV einen schnellen Puffer-Speicher, der zum Beschleunigen von Zugriffen eingerichtet wird. Ein Cache enthält lokale Kopien von Inhalten eines anderen (Hintergrund-)Speichers und erlaubt somit den Zugriff ohne auf externe Datenspeicher zurückgreifen zu müssen. cachen = in den Puffer-Speicher laden.
Cache-Miss		Ein Cache Miss bezeichnet einen nicht erfolgreichen Zugriff auf einen Cache. Dies bedeutet für das den Cache verwaltende System, dass die Existenz der Daten im Hintergrundspeicher überprüft und dann dem Cache hinzugefügt werden muss
Call-Agent		<i>Akteur</i> , der in einem <i>Call-Center</i> an der Bereitstellung von Dienstleistungen mitwirkt.
Call-Center		Organisationseinheit, von der Serviceangebote telefonisch aktiv (outbound) oder passiv (inbound) bereitgestellt werden.
CAM	Card Application Management	
CAMS	Card Application Management System	<i>Kartenanwendungsmanagementsystem</i>
Capacity Management	(CpM)	ITIL-basierter Prozess, der sicherstellen soll, dass die notwendige und vereinbarte Kapazität zur Erbringung eines IT-Service zeitgerecht und kostenmäßig vertretbar bereitgestellt wird. Hierbei werden die notwendigen IT-Ressourcen aufgrund der geschäftlichen Anforderungen ermittelt, die Auslastung prognostiziert und ein Kapazitätsplan für die Planung der IT-Ressourcen erstellt. Darüber hinaus wird die Auslastung der Ressourcen überwacht und der Service gegen den SLA geprüft.
CAR	Certification Authority Reference	Referenz der <i>Zertifizierungsinstanz</i>
Card Management System	(CMS)	Das Card Management System (<i>Kartenmanagementsystem</i>) ist eine Komponente, die das gesamte Management der eGK umfasst: das Lebenszyklusmanagement, das Anwendungsmanagement und das Kartenanwendungsmanagement. Somit unterstützt das CMS alle Prozesse eines Kartenherausgebers von der Kartenproduktion über die Verwendung der eGK durch einen Karteninhaber bis zum Ende des Kartenlebenszyklus.
CBC	Cipher Block Chaining	
CC	1. Common Criteria 2. Cryptographic Checksum	1. Common Criteria for Information Technology Security Evaluation 2. kryptografische Prüfsumme
CEN	Comité Européen de Normalisation	Europäisches Komitee für Normung

Begriff	Englisch, (Abk.)	Definition (Synonym)
Certificate Policy	(CP)	Eine Certificate Policy besteht aus einer Menge von Regeln, die bei der Ausstellung des <i>Zertifikates</i> berücksichtigt wurden. Auf Basis der Certificate Policy kann entschieden werden, ob ein <i>Zertifikat</i> für einen bestimmten Einsatzzweck ausreichende Sicherheit bietet. Ein Rahmenwerk für die Entwicklung von Certificate Policies findet sich in RFC3647.
CETP	Connector Event Transport Protocol	
CG	cryptogram	Kryptogramm
CH	cardholder	<i>Karteninhaber</i>
CHA	Certificate Holder Authorization	Berechtigung des <i>Karteninhabers</i>
Change Management	(CM)	Verfahren zur Steuerung und Kontrolle verändernder Eingriffe in <i>Anwendungen</i> , Infrastruktur, Dokumentation, Prozesse und Verfahren mit dem Ziel, infolge der Änderungen erwartete Störungen zu vermeiden und die Effizienz des Änderungsverfahrens zu verbessern. Grundlage der Änderungen sind Änderungsanforderungen bzw. Request of Change. Synonym: Änderungsmanagement
Change Request		Schriftlich formalisierte Darstellung eines Änderungsbedarfs an Ergebnistypen eines abgestimmten Release und/oder einer abgestimmten veröffentlichten Version. Change Requests sind immer entscheidungs- und bewertungsrelevant. Für das Anforderungsmanagement gibt es mehrere Sichten auf Change Requests: <ol style="list-style-type: none"> 1) Eine akzeptierte Anforderung überführt ihre Inhalte in Change Requests, wenn die Anforderung auf abgestimmte veröffentlichte Versionen / Releases gilt. Erst der Change Request kann die Umsetzung auslösen. Es ist möglich, dass eine Anforderung zu 1-n Change Requests führt und umgekehrt kann ein Change Request 1-n Anforderungen enthalten. 2) Es wird ein Change Request zu einer abgestimmten Anforderung gestellt, der im ersten Schritt in AM bearbeitet wird und dann an die jeweils betroffene AG zu kommunizieren ist.
Chipkarte		Plastikkarten, die mit einem Mikrochip zu Rechen- und Speicherzwecken versehen sind. Die Informationen werden in einem Halbleiterchip abgelegt, der mit einem Chipkarten-Lesegerät ausgelesen wird. Sicherheit kann durch einen PIN und mit Kryptoverfahren erreicht werden. Anwendung als Telefonkarte, Krankenversicherungskarte, Cash-Karte
CHR	Certificate Holder Reference	Referenz des <i>Karteninhabers</i>

Begriff	Englisch, (Abk.)	Definition (Synonym)
CIA	Cryptographic Information Application	kryptografische Informationsanwendung
CIO	Cryptographic Information Objects	kryptografische <i>Informationsobjekte</i>
CLA		Class-Byte eines Befehls
ClientApplication		Synonym für <i>Primärsystem</i>
Cluster		Ein Cluster ist ein Verbund von Computern, die üblicherweise von außen als ein <i>System</i> wahrgenommen werden und somit eine höhere Ausfallsicherheit und/oder bessere Performanz ermöglichen.
CM	Change Management	
CMET	Common Message Element Type	
CMM	Cabability Maturity Model	Modell zur Bewertung des Reifegrades der Organisation eines Software-Herstellers bei der Entwicklung von <i>Anwendungen</i>
CMS	Card Management System	<i>Kartenmanagementsystem</i>
CMYK		<i>System</i> zur Definition einer Farbe; CMYK steht für Cyan (Türkis), Magenta (Fuchsinrot), Yellow (Gelb) und Key/black (schwarz)
Commit		Der Begriff aus dem Bereich Datenbanken bestätigt den erfolgreichen Abschluss einer Transaktion. Hierdurch wird das endgültige Speichern von Daten angestoßen. Das Gegenteil wäre hierbei ein <i>Roll Back</i> , wodurch die temporär gespeicherten Informationen auf den Ursprungswert zurückgesetzt würden.
Common Criteria	(CC)	Common Criteria for Information Technology Security Evaluation Internationaler gemeinsamer Standard (ISO 15408) für die Prüfung und <i>Zertifizierung</i> von Sicherheitsprodukten wie z.B. Computersystemen
Common Message Element Type	(CMET)	Wieder verwendbare HL7-Komponente, die bei der HL7-Modellierung beliebig inkludiert werden kann, ohne die gemeinsame interne Struktur zu wiederholen.
Computational View		Der Computational View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) stellt die Zerlegung einer <i>Anwendung</i> in funktionale Module und deren Interaktionsschnittstellen dar. Hier wird ein <i>System</i> in logische, funktionale Komponenten zerlegt, die für die Verteilung geeignet sind. Das Ergebnis sind Objekte, die Schnittstellen besitzen, über die diese Dienste anbieten bzw. nutzen.
Computerwurm		Schadsoftware, die sich über Netzwerke selbständig ausbreitet

Begriff	Englisch, (Abk.)	Definition (Synonym)
Configuration Item	(CI)	Formalisierte Beschreibung einer zum Betrieb erforderlichen Komponente über deren gesamten Lebenszyklus hinweg. CIs werden durch das <i>Configuration Management</i> strukturiert, dokumentiert und in einer Datenbank zusammengefasst. Dabei werden nicht nur physikalische Komponenten wie Hardware, sondern auch logische (z.B. Software) und organisatorische Mittel (z.B. Verträge) erfasst.
Configuration Management	(CfM)	Prozess, der für die Dokumentation eines logischen Abbildes der physikalischen und logischen Infrastruktur zuständig ist. Wichtige Aufgabe dabei ist die Darstellung der Relationen zwischen den Configuration Items. Zielsetzung ist die Versorgung der Betriebsprozesse mit aktuellen zuverlässigen Informationen, welche häufig in einer Datenbank verwaltet werden.
Connector Event Transport Protocol	(CETP)	Übertragungsprotokoll für die Meldung von Ereignissen im Konnektor
Coordinated Universal Time	(UTC)	Koordinierte Weltzeit. Sie stellt die aktuelle Weltzeit dar und hat in dieser Funktion die vielen geläufige Greenwich Mean Time abgelöst. Sie ist eine Kombination aus der internationalen Atomzeit TAI und der Universalzeit UT. Die Zeitzonen werden als positive oder negative Abweichung von UTC angegeben (z. B. UTC + 2 entspricht der MESZ). UTC ist unter anderem die Referenzzeit im Internet und auch vielfach in Computersystemen.
COS	Card Operating System	Kartenbetriebssystem
CoS	Class of Service	Gruppe von Verfahren zur Priorisierung in TCP/IP-basierten Netzwerken
CPI	Certificate Profile Identifier	Kennung des Zertifikatsprofils
CRL	Certificate Revocation List	Zertifikatssperrliste
Cross-Zertifikat		Ein Cross-Zertifikat ist ein <i>Public-Key-Zertifikat</i> , das eine <i>Zertifizierungsinstanz</i> für eine andere <i>Zertifizierungsinstanz</i> ausstellt.
CRT	Control Reference Template	
CS	CertSign	CertificateSigning
CT	Confidentiality Template	
CV	card verifiable	Echtheitsprüfung von <i>Chipkarten</i>
CVC	Card Verifiable Certificate	<i>Zertifikat</i> für ein asymmetrisches Verfahren zur gegenseitigen Echtheitsprüfung von systemzugehörigen <i>Chipkarten</i>
D		

Begriff	Englisch, (Abk.)	Definition (Synonym)
DALE-UV		Datenaustausch mit <i>Leistungserbringern</i> in der gesetzlichen Unfallversicherung
DAS	Digital Signature Algorithm	
Datenautorität		Begriff aus der <i>Telematik-Infrastruktur</i> . Die Datenautorität bezeichnet den Akteur innerhalb einer Telematik-Nachricht, über dessen kryptographische Identität der Zugriff auf ein Objekt autorisiert wird.
Datenbearbeiter		Begriff aus der <i>Telematik-Infrastruktur</i> . Der Datenbearbeiter ist der Akteur innerhalb einer Telematik-Nachricht, durch dessen kryptographische Identität die Berechtigung auf eine Funktion eines Fachdienstes nachgewiesen wird
Datenschutz	privacy	Bezeichnet den Schutz vor Missbrauch bei der Verarbeitung und Speicherung personenbezogener oder personenbeziehbarer Daten. Das eigentliche Schutzobjekt sind hierbei nicht nur persönliche Daten, sondern vielmehr unmittelbar die Persönlichkeitsrechte jeder natürlichen Person als Individuum.
Datensicherheit	1. safety 2. security	Unter Datensicherheit im Sinne von "safety" wird der Schutz von Daten vor dem Versagen technischer Systeme verstanden. Dabei zielt die Datensicherung besonders auf die Sicherstellung der Verfügbarkeit, der <i>Integrität</i> und der <i>Verbindlichkeit</i> der Daten ab. Unter Datensicherheit im Sinne von "security" wird der Schutz von Daten gegen intelligente Angreifer verstanden. Dabei zielt die Datensicherung besonders auf die Sicherstellung der <i>Verfügbarkeit</i> , der <i>Integrität</i> und der <i>Verbindlichkeit</i> der Daten ab.
DatenZugriffsAuditService		Service der <i>Telematik-Infrastruktur</i>
DCF77		DCF77 ist das von der Physikalisch-Technischen Bundesanstalt (http://ptb.de) in Mainflingen – südöstlich von Frankfurt – ausgestrahlte Funksignal, das die gesetzlich festgelegte Zeit gemäß Zeitgesetz trägt. Dieses Signal wird insbesondere von <i>Zertifizierungsdiensteanbietern</i> genutzt, um die Aktualität der Systemzeit der von Ihnen betriebenen OCSP- und TSP-Responder zu gewährleisten.
DDoS	Distributed Denial of Service	Prinzipiell gleiches Verfahren wie bei <i>DoS</i> , jedoch erfolgen die Anfragen gleichzeitig von einer Vielzahl Clients aus (daher auch Distributed). Daraus resultierend ergibt sich eine mit der Anzahl der anfragenden Clients linear ansteigende Last. Um über eine ausreichende Anzahl von Clients zu verfügen, verteilt der Angreifer im Allgemeinen so genannte Backdoor Programme (mit eigenen Verteilungsroutinen, die Schwachstellen in Betriebssystemen ausnutzen). Über diese Routinen kann der Angreifer dann koordiniert die DDoS Angriffe starten.
DDV		Daten Direkt Verbindung

Begriff	Englisch, (Abk.)	Definition (Synonym)
DE	Data Element	Datenelement
Denial of Service	(DoS)	<p>Der Begriff „<i>Denial of Service</i> (DoS)“ bezeichnet einen Angriff auf einen Host oder Service mit dem Ziel, einen oder mehrere Dienste durch Überlastung arbeitsunfähig zu machen.</p> <p>Dazu belasten die Angriffe die Dienste eines Servers mit einer derart hohen Anzahl von Anfragen, dass der Server diese nicht mehr oder nur noch mit einer unzureichend langen Antwortzeit (Timeout) verarbeiten kann.</p>
DER	Distinguished Encoding Rules	
DES	Data Encryption Standard	Veralteter und unsicherer Amerikanischer Standard zur Datenverschlüsselung im Gegensatz zu 3DES: Betriebsmodus des <i>DES</i> , der gegenwärtig noch sicher ist. Dabei wird der <i>DES</i> dreimal hintereinander angewendet.
DF	Dedicated File	
DFA	Differential Fault Analysis	
DHCP	Dynamic Host Configuration Protocol	
DI	Baud rate adjustment factor	
Dienst	Services	Der Begriff wird in der IT verwendet zur Bezeichnung von technischen, in sich geschlossenen Funktionskomponenten, die einen Prozess unterstützen. Der Dienst wird dabei über eines oder mehrere Netzwerkprotokolle der <i>Anwendungsschicht</i> realisiert.
Differential Fault Analysis	(DFA)	Differential Fault Analysis ist ein Angriff auf <i>Chipkarten</i> oder Sicherheitsmodule durch Erzeugung von Fehlern bei der <i>Verschlüsselung</i>
Differential Power Analysis	(DPA)	Differential Power Analysis ist ein Angriff auf <i>Chipkarten</i> und Sicherheitsmodule durch die Analyse der Leistungs- bzw. Stromaufnahme während einer <i>Verschlüsselung</i> .
Digest		<p>Ein Message Digest ist eine kryptographische Einweg-<i>Hash-Funktion</i>. Bei einer <i>Hash-Funktion</i> geht es allgemein darum, eine lange Eingabe (zum Beispiel einen Text) in eine kurze Ausgabe (den <i>Hash-Wert</i> des Textes) zu verwandeln.</p> <p>Diese Funktionen treten mit dem Anspruch auf, dass sie nicht umkehrbar seien und auch keine Kollision berechenbar sei. Das bedeutet, dass es nicht möglich sein soll, zu einem Chiffre den Originaltext wieder herzustellen (unumkehrbar). Es soll auch nicht möglich sein, einen Text zu berechnen, der das gleiche Chiffre wie der Originaltext erzeugt (kollisionsfrei).</p>
Digital Signature Algorithm	(DSA)	Der Digital Signature Algorithm [FIPS186-2] ist ein <i>Signaturalgorithmus</i> auf Basis des Diskreten Logarithmus in der multiplikativen Gruppe eines endlichen Körpers.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Digitale Signatur	digital signature	Mit dem Begriff Digitale Signatur werden Daten in elektronischer Form bezeichnet, die anderen zu schützenden elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind (z.B. durch kryptografische Umformung der zu schützenden Daten). Sie belegen die Herkunft und <i>Integrität</i> der zu schützenden Daten und schützen damit gegen Fälschungen.
DIMDI		Deutsches Institut für medizinische Dokumentation und Information
DIN		Deutsches Institut für Normung
DIR	Directory	Verzeichnis
Disease-Management-Programm	(DMP)	Disease-Management-Programme (DMP) werden auch strukturierte Behandlungsprogramme oder einfach Chronikerprogramme genannt. Im Rahmen eines DMP-Programms soll eine Krankheit (englisch: Disease) optimal behandelt (gemanaged) werden.
Dispensierdaten		Apothekenteil als Teil des elektronischen <i>eRezept</i> -Datensatzes, der das dispensierte Arzneimittel oder die Rezeptur eindeutig beschreibt und den der Apotheker nach Belieferung hinzufügt.
DIVI		Deutsche interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin
DKG		Deutsche Krankenhausgesellschaft
DKR		Deutsche Kodierrichtlinien
DM	Display Message	
DMP	Disease Management Program	
DMZ	De-Militarized Zone	
DNS	Domain Name System	Syn. Auch: Domain Name Service
DO		Datenobjekt
Domain Name		Name (Label) eines Teilbaumes innerhalb des Domain Namespace; identisch mit dem Namen des Node-Eintrags an der Spitze des besagten Teilbaumes.
Domain Name System	(DNS)	(Bereichsnamensystem). Bezeichnung für das im Internet verwendete System von hierarchisch gegliederten Bereichsnamen. Über die Domain-Datenbanken wird eine Zuordnung von sprechenden Server-Namen in IP-Adressen vorgenommen. So wird z.B. aus einem logischen DNS-Namen wie www.vianetworks.de eine numerische Adresse wie 194.77.111.24.
Domain Name-space		Spezifikation einer hierarchischen DNS Baumstruktur, in der jeder Node- und Leaf- Eintrag unterschiedlichen Typen von Informationssätzen (siehe Resource Records) beinhaltet.
DoS	Denial of Service	

Begriff	Englisch, (Abk.)	Definition (Synonym)
DPA	Differential Power Analysis	
dpi	Dots per Inch	Punkte pro Zoll
DRG	Diagnosis Related Groups	
DSI	Digital Signature Input	
DSL	Digital Subscriber Line	
DST	Digital Signature Template	
DTA-Abrechnung		Abrechnung per Datenträgeraustausch zwischen <i>Arzt</i> und <i>KV</i>
DTD	Document Type Definition	
Durchsetzungseinheit	Access Control Enforcement Unit Policy Enforcement Point	Die Durchsetzungseinheit stellt sicher, dass nur berechnigte Zugriffe auf die Zugriffsziele (Ressourcen) erlaubt werden. Die Entscheidung darüber, welche Zugriffe erlaubt sind, trifft die <i>Entscheidungseinheit</i> .
Dynamic Host Configuration Protocol	(DHCP)	Ermöglicht mit Hilfe eines entsprechenden Servers die automatische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter am Computer in einem Netzwerk
E		
eArztbrief		<i>elektronischer Arztbrief</i>
ebXML	Electronic Business XML	
ECB	Electronic Code Book	
ECDSA	Elliptic Curve Digital Signature Algorithm	
EDI	Electronic Data Interchange	
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport	
EDV		elektronische Datenverarbeitung
eEHIC		elektronische Europäische <i>Krankenversicherungskarte</i>
EEPROM	Electrical Erasable Programmable Read Only Memory	
EF	Elementary File	

Begriff	Englisch, (Abk.)	Definition (Synonym)
EFID	Short EF Identifier	
eGK		<i>elektronische Gesundheitskarte</i>
eHC	electronic Health Card	<i>elektronischer Heilberufsausweis</i>
EHIC		<i>Europäische Krankenversicherungskarte</i>
Eigenanteil		Zuzahlungsteil des <i>Versicherten</i> an den Kosten ärztlicher, zahnärztlicher oder Krankenhausleistung oder eingelöster Arznei- oder Hilfsmitteln.
einfache elektronische Signatur		Unter einer „einfachen elektronischen Signatur“ versteht man eine <i>elektronische Signatur</i> , die nicht alle Anforderungen an eine <i>fortgeschrittene elektronische Signatur</i> erfüllt.
Eingangsanforderung	input requirement	Anforderungssicht Eine Anforderung aus Sicht eines Konzeptes, die dieses Konzept zu berücksichtigen hat.
Einlösung		Vorgang der Inanspruchnahme einer verordneten Leistung durch einen <i>Patienten</i> .
Einwilligung	agreement	Zustimmungs-, Einverständniserklärung bzw. Erlaubnis eines <i>Patienten</i> für einen oder eine Gruppe von <i>Leistungserbringern</i> zu einer Handlung. Beispiel: Einwilligung zur Nutzung der <i>freiwilligen Anwendungen</i> der eGK.
Einzeltaxe		Preis des Fertigarzneimittels / Rezeptur
eKiosk		Der eKiosk ist ein <i>Primärsystem</i> zur Verwaltung von <i>Anwendungen</i> und Daten durch den <i>Versicherten</i> . Mit Hilfe des eKiosk kann der <i>Versicherte</i> z.B. <i>eRezepte</i> ausblenden, das Einverständnis zum Laden diverser <i>Anwendungen</i> erklären usw.
Electronic Business XML	(ebXML)	ebXML (http://www.ebxml.org) ist eine 1999 gestartete, gemeinsame Initiative von UN/CEFACT und OASIS, durch die eine Reihe von <i>Spezifikationen</i> für die Nutzung von XML für elektronische Geschäftsprozesse entwickelt wurden.
Electronic Data Interchange	(EDI)	EDI ist ein Sammelbegriff für alle elektronischen Verfahren zum vollautomatischen Versand von strukturierten Nachrichten zwischen Anwendungssystemen unterschiedlicher Institutionen. Zu den möglicherweise wichtigsten Standards für EDI zählen <i>EDIFACT</i> und <i>ebXML</i> .
Electronic Data Interchange For Administration, Commerce and Transport	(EDIFACT)	EDIFACT ist ein branchenübergreifender internationaler Standard (<i>ISO9735</i>) für den automatisierten Austausch elektronischer Daten im Geschäftsverkehr. Er ist einer von mehreren gebräuchlichen Standards für <i>EDI</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
elektronische Gesundheitskarte	(eGK)	Die elektronische Gesundheitskarte ist gemäß § 291 a SGB V eine personenbezogene Identifikationskarte, die <i>Versicherte</i> der <i>Gesetzlichen Krankenversicherung (GKV)</i> zur Inanspruchnahme ärztlicher und zahnärztlicher Behandlung gemäß § 15 SGB V berechtigt. Sie enthält gemäß § 291 a SGB V Angaben, die für die Übermittlung elektronisch veranlasster ärztlicher Verordnungen geeignet sind.
elektronische Patientenakte	(ePA)	Die elektronische Patientenakte beinhaltet „Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den <i>Patienten</i> “ (§ 291a Abs. 3, Satz 1, Nr. 4 SGB V/GMG). Hierbei handelt es sich um eine <i>freiwillige Anwendung</i> der <i>eGK</i> .
elektronische Signatur	(eSign)	Gemäß § 2 Nr.1 SigG sind elektronische Signaturen Daten in elektronischer Form, die der <i>Authentifizierung</i> dienen. Die Bandbreite möglicher Ausprägungen reicht von einer sehr leicht fälschbaren digitalen Abbildung einer handschriftlichen Unterschrift bis hin zur <i>qualifizierten elektronischen Signatur</i> als sehr sichere Form der <i>digitalen Signatur</i> .
elektronischer Arztbrief	(eArztbrief)	Signierte elektronische Dokumentation mit partiell vertraglich vorgegebenen Bestandteilen eines <i>Arztes</i> oder <i>Zahnarztes</i> zu einem <i>Versicherten</i> und dessen Krankheitsgeschehen mit dem Ziel, dass ein anderer <i>Leistungserbringer</i> darüber informiert wird. Beispiele: Krankenhausentlassbrief oder Unfallbericht. Akronym: eArztbrief.
elektronischer Heilberufsausweis	(HBA)	Der elektronische <i>Heilberufsausweis</i> ist ein personenbezogener Ausweis im Gesundheitswesen, der an <i>Heilberufler</i> ausgegeben wird. Er beinhaltet (neben einer visuellen Ausweisfunktion) die Dienste <i>Authentifizierung</i> , <i>Verschlüsselung</i> und <i>elektronische Signatur</i> und ermöglicht den Zugriff auf Daten der <i>elektronischen Gesundheitskarte</i> .
elektronisches Rezept	(eRezept)	Signierter elektronischer Datensatz des <i>Rezeptes</i> , welches vom <i>Arzt</i> oder <i>Zahnarzt</i> erstellt wird und in der Apotheke oder <i>Versandapotheke</i> eingelöst wird. Dient laut § 291a Abs. 2, Satz 1 SGB V/GMG zur „Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form“. Hierbei handelt es sich um die Pflichtanwendung der <i>eGK</i> .
Elliptic Curve Digital Signature Algorithm (ECDSA)		Der ECDSA ANSI-X9.62 ist ein <i>Signaturalgorithmus</i> auf Basis des Diskreten Logarithmus in der Gruppe der Punkte einer elliptischen Kurve über einem endlichen Körper.
EMV	Europay Mastercard Visa	
ENC	Encryption	<i>Verschlüsselung</i>

Begriff	Englisch, (Abk.)	Definition (Synonym)
ENC()	Encrypted data	verschlüsselte Daten
Engineering View		Der Engineering View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) stellt die Verteilung der einzelnen Elemente des <i>Systems</i> auf physikalische Ressourcen sowie deren Verbindung dar. Diese Sicht beschreibt die erforderliche Systemunterstützung, um eine Verteilung der Objekte aus dem <i>Computational Viewpoint</i> zu erlauben. Dazu gehören Ausführungseinheiten für die Objekte, wie zum Beispiel Rechner und Kommunikationsinfrastruktur, wie zum Beispiel Netzwerke, sowie alle Arten von Software-Plattformen für verteilte <i>Systeme</i> .
Enterprise View		Der Enterprise View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) spezifiziert Zielsetzung, Anwendungsbereich, Verfahren und Regeln einer <i>Anwendung</i> . Hier wird die Gesamtumgebung für das <i>System</i> und sein Zweck beschrieben. Außerdem werden die <i>Anforderungen</i> (Requirements) an das <i>System</i> , zu erfüllende Bedingungen (Constraints), ausführbare Aktionen (Actions) und DV-Zielvorgaben (Policies) aus Sicht der Organisation oder des Unternehmens definiert. Dabei werden die Verfahren, deren Regeln und die an den Verfahren beteiligten <i>Akteure</i> in ihren <i>Rollen</i> definiert.
Entscheidungseinheit	Access Control Decision Unit Policy Decision Point	Die Entscheidungseinheit beurteilt, ob eine Zugriffsanfrage berechtigt ist oder nicht. Die Entscheidung erfolgt auf Basis der Autorisierungspolitik und der <i>Entscheidungsinformation</i> inkl. des Zugriffskontexts.
Entscheidungsinformation	Access Control Decision Information	Die Entscheidungsinformation umfasst den Teil der Autorisierungsinformation, der zum Zugriffszeitpunkt der <i>Entscheidungseinheit</i> zur Entscheidung vorgelegt wird.
Entschlüsselung		Vorgang, bei dem unter Verwendung mathematischer Algorithmen und <i>privater</i> oder <i>geheimer Schlüssel</i> elektronische Daten wieder les- bzw. verarbeitbar gemacht werden. In verschlüsselter Form sind die Daten von unbefugten Dritten nicht einsehbar. Die Daten können nur vom Besitzer des entsprechenden <i>privaten</i> oder <i>geheimen Schlüssels</i> wieder in die Originalform überführt werden.
EOF	End-of-File	Dateiende
ePA		<i>elektronische Patientenakte</i>
eRezept		<i>elektronisches Rezept</i>
eSign		<i>elektronische Signatur</i>
Ethernet		Derzeit gebräuchlichste LAN-Technologie
ETSI	European Telecommunication Standards Institute	
EU		Europäische Union

Begriff	Englisch, (Abk.)	Definition (Synonym)
European Telecommunication Standards Institute	(ETSI)	Europäisches Telekommunikationsstandardinstitut. Koordinierungsstelle für Kompatibilitätsfragen europäischer Telekommunikationsentwicklungen.
Evaluation		Bezeichnet die Auswertung der Testergebnisse durch die gematik mit dem Ziel, den jeweiligen Testerfolg festzustellen. Die Evaluation der Testergebnisse erfolgt anhand gemeinsam abgestimmter, einheitlich definierter Kriterien.
Evaluationsgegenstand	(EVG)	Bei einer Evaluation gemäß <i>ITSEC</i> oder <i>Common Criteria</i> nennt man das zu bewertende Produkt oder System „Evaluationsgegenstand“ (EVG). Ein EVG kann aus mehreren Komponenten bestehen. Von besonderer Bedeutung für die Evaluation sind die sicherheitsspezifischen und sicherheitsrelevanten Komponenten
EVG	Evaluationsgegenstand	
EWG		Europäische Wirtschafts-Gemeinschaft
Extensible Markup Language	(XML)	universelle Datenbeschreibungssprache
F		
FA		Funktionsabschnitt Fachanwendung Facharchitektur Die Bedeutung des Kürzels wird durch den Kontext bestimmt.
Facharchitektur		Konkretisiert das <i>Fachkonzept</i> auf fachlicher Ebene und leitet daraus präzise, vollständig, nachvollziehbar, konsistent und bindend die technische Umsetzung inkl. aller Schnittstellen ab. Dabei werden technische Festlegungen für die Einsatzumgebung getroffen.
Fachdienst		Bezeichnung für die technische Umsetzung von Fachanwendungen wie z.B. zur Bereitstellung der <i>Versichertenstammdaten</i> , Verarbeitung der <i>Verordnungsdaten</i> oder der <i>freiwilligen Anwendungen des Versicherten</i> .
Fachkonzept		Beschreibt grob, vollständig, nachvollziehbar, konsistent und bindend die zu unterstützenden Anwendungsfälle. Daraus werden funktionale, nichtfunktionale und <i>Sicherheitsanforderungen</i> abgeleitet, welche durch die zukünftige IT-Unterstützung im Kontext der Einführung der eGK umzusetzen sind. Das Fachkonzept bezieht sich stets auf einen konkreten Fachausschnitt.
Fall-Back		Als Fall-Back wird eine Rückfallposition bezeichnet, die immer dann zum Tragen kommen soll, wenn ein eigentlich vorgesehenes Verfahren nicht durchgeführt werden kann.
FCP	File Control Parameter	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Feldtest		Der Feldtest beschreibt die Phase, in welcher eine größere Anzahl von Nutzern die zu testenden Produkte und Verfahren im Echtbetrieb einsetzen. Die Altverfahren werden dabei von der Testgruppe nicht mehr oder parallel eingesetzt.
FI	Clock Rate Conversion Factor	Frequenzumsetzungsfaktor
FID	File Identifier	Dateikennung
File Transfer Protocol	(FTP)	Netzwerkprotokoll zur Datenübertragung
Filialapotheke		Durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (<i>GMG</i>) ist es seit 01.01.2004 möglich, dass Apotheker neben ihrer Hauptapotheke weitere Apotheken (Filialapotheken) betreiben können.
Financial Management	(FM)	ITIL-basierter Prozess, der die Kosten im Rahmen der Erbringung von IT-Services identifiziert, analysiert und eine realistische Methode für die Verrechnung der Kosten anwendet. Hierbei umfasst das Financial Management drei Unterprozesse, IT Service Budgeting, IT-Accounting und Leistungsverrechnung.
Firewall		Ein Firewall ist ein System aus Hardware und/oder Software, das den Zugriff zwischen zwei Systemen beschränkt und somit ein Regelwerk erzwingt.
Firmware		"Fest eingebrannte" Betriebssoftware eines Gerätes
Forensische Untersuchung	forensics	Untersuchung, ob und wie ein Angriff auf ein IT-System stattgefunden hat. (Allgemein: Suche nach Spuren eines Vergehens)
Fortgeschrittene elektronische Signatur		Eine fortgeschrittene elektronische Signatur ist gemäß § 2 Nr. 2 SigG eine <i>elektronische Signatur</i> mit besonderen Eigenschaften, durch die zumindest ein grundlegendes Maß an <i>Authentizität</i> und <i>Integrität</i> sichergestellt werden kann. Anders als bei der <i>qualifizierten elektronischen Signatur</i> kann aber eine lediglich fortgeschrittene elektronische Signatur nicht die <i>Schriftform</i> gemäß § 126 BGB ersetzen und hat geringere Beweiskraft vor Gericht
FPU Erweiterung	Floating Point Unit	Eine physische Erweiterung eines Systems, die zur schnelleren Verarbeitung von Gleitkommazahlen dient.
Framework		Der Begriff Framework stammt aus dem Bereich der Software Entwicklung und bezeichnet ein Rahmenwerk. Diese Rahmenwerk schreibt vor, wie bestimmte Systeme zu implementieren sind, um Interoperabilität zu anderen Systemen zu gewährleisten
Freiwillige Anwendung		Für den <i>Patienten</i> freiwilliger Einsatzbereich in der Nutzung der eGK. Über den § 291a SGB V festgelegte <i>freiwillige Anwendungen</i> sind z.B. <i>elektronische Patientenakte</i> oder <i>Arzneimitteldokumentation</i> .
Frequently asked question	(FAQ)	Häufig gestellte Fragen

Begriff	Englisch, (Abk.)	Definition (Synonym)
FTP	File Transfer Protocol	
Fully-Qualified Domain Name	(FQDN)	Ein absoluter Domain Name innerhalb eines DNS Namensraumes, der ausgehend vom Knoten, den er kennzeichnet, die Labels aller darüber liegenden Hierarchiestufen bis zum Wurzelverzeichnis (root) enthält.
funktionale Anforderung	functional requirement	Eine funktionale <i>Anforderung</i> wird beschrieben durch einen Funktionsauslöser, eine erwartete Aktion und ein Ergebnis und definiert die Benutzbarkeit. WAS muss das Produkt erfüllen. Beispiele: Vollständigkeit, Angemessenheit, Korrektheit, Konsistenz, Robustheit, Fehlertoleranz, Betriebsprozessansprüche, Reife, Effizienz, Effektivität
G		
Gateway		Ein Gateway bezeichnet einen Architekturbaukasten, auf dem (Netzwerk)Protokolle zueinander übersetzt beziehungsweise erweitert werden.
GDO	Global Data Object	
Gebrauchstauglichkeit	usability	Gebrauchstauglichkeit eines Produktes definiert das Ausmaß, in dem es von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Kontext unter den Aspekten der Software-Ergonomie zu erreichen (IDIN EN ISO 9241). Sie unterteilt sich in die Bereiche <i>Benutzbarkeit</i> und <i>Benutzerfreundlichkeit</i> .
Geheimer Schlüssel		Geheime Schlüssel werden im Zusammenhang mit symmetrischen Kryptoalgorithmen verwendet. Im Gegensatz zu den bei asymmetrischen Kryptoalgorithmen eingesetzten <i>privaten Schlüsseln</i> ist das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt
Geschäftsprozess		Teilaufgabe in einer Organisation
Gesetzliche Krankenkasse	(KK)	Körperschaft des öffentlichen Rechts, die Leistungen der <i>gesetzlichen Krankenversicherung</i> für ihre <i>Versicherten</i> gewährt. Der Begriff „Gesetzliche Krankenkasse“ wird im Rahmen des Projekts <i>Gesundheitskarte</i> als <i>Akteur</i> verwendet.
Gesetzliche Krankenversicherung	(GKV)	Die gesetzliche Krankenversicherung ist ein Zweig der Sozialversicherung. Die wesentlichen Strukturprinzipien sind Solidarität, Sachleistung, paritätische Finanzierung, Selbstverwaltung und Pluralität. Der soziale Auftrag der GKV besteht darin, Versicherungsschutz in Krankheitsfall unabhängig von der finanziellen Leistungsfähigkeit des einzelnen <i>Versicherten</i> zu gewährleisten. Die Beitragsfinanzierung läuft in der GKV im Umlageverfahren und nicht - wie bei der <i>privaten Krankenversicherung</i> - durch Kapitaldeckung. Die Leistungen werden nach dem Sachleistungsprinzip erbracht, d.h. <i>Versicherte</i> müssen bei einem Arztbesuch etc. nicht in Vorleistung treten.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Gesundheitskarte	(eGK)	Wird im Rahmen des Projekts synonym zu „ <i>elektronische Gesundheitskarte</i> “ verwendet.
Gesundheitstele- matik		Telematik im Gesundheitswesen
GKV		Gesetzliche Krankenversicherung
GMG		Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GOÄ		Gebührenordnung für <i>Ärzte</i>
goTOP		gematik offene Testorganisations-Plattform
GP	Global Plattform	
Grundschutz		Erfüllung von Mindestsicherheitsmaßnahmen (z.B. definiert im IT-Grundschutzhandbuch des BSI)
GSHB		IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik
gSP		gematik-Standardisierungs-Prozess
H		
Hacker		Unauthorisierte Person, die sich Zugang zu oder Zugriff auf ein IT-System verschaffen will (Anm: dies trifft noch keine Aussage darüber ob diese Person auch tatsächlich böswillige Absichten hat!)
Halbleiterhersteller		Der Halbleiterhersteller hat (neben der eigentlichen Herstellung des Chips, der in die Karte implantiert wird) im Kontext der eGK zwei wesentliche Aufgaben, die für die Sicherheit des gesamten Systems von großer Bedeutung sind: <ol style="list-style-type: none"> 1. Sicherstellung der Eindeutigkeit jedes gefertigten Halbleiters über eine ICCSN (Integrated Circuit Card Serial Number, Halbleiterseriennummer). 2. Einbringen eines Personalisierungsgeheimnisses zum Schutz vor "falschen echten" Karten.
Hardware Si- cherheits Modul	Hardware Security Module (HSM)	Bauteil, welches sicherheitsrelevante Informationen, wie Daten und kryptographische Schlüssel sicher speichert und verarbeitet. Dieses kann auch ein spezieller Chipkartencontroller sein. Andere Bezeichnungen sind SAM und HSM.
HARP	Harmonization for the security of web technologies and applications	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Hash-Funktion		Eine Hash-Funktion ist ein kryptographischer Algorithmus, bei dem Nachrichten beliebiger Länge auf einen Hash-Wert fester Länge (z.B. 160 Bit) abgebildet werden. Bei kryptographisch geeigneten Hash-Funktionen ist es praktisch unmöglich, zwei Nachrichten mit dem gleichen <i>Hash-Wert</i> zu finden (Kollisionsresistenz) und bei einem gegebenen <i>Hash-Wert</i> eine Nachricht zu finden, die durch die Hash-Funktion auf den <i>Hash-Wert</i> abgebildet wird (Einwegigkeit).
Hash-Wert		Ein Hash-Wert ist eine mathematische Prüfsumme, die durch Anwendung einer <i>Hash-Funktion</i> aus einer elektronischen Nachricht erzeugt wird.
Hauptversicherter		Beitragspflichtiger Versicherungsnehmer einer <i>Gesetzlichen Krankenversicherung</i> , dem mehrere nicht beitragspflichtige Familienmitglieder zugeordnet sind.
HB	Historical Bytes	
HBA		Heilberufsausweis
HCA	Health Care Application	Gesundheitsanwendung
Health Level 7	(HL7)	Health Level 7 ist ein internationaler Standard für den Austausch von Daten zwischen Computersystemen im Gesundheitswesen. Die 7 des Namens bezieht sich auf die Schicht 7 des ISO/OSI-Referenzmodell für die Kommunikation (ISO7498-1) und drückt damit aus, dass hier die Kommunikation auf Applikationsebene beschrieben wird.
Health Professional Card	(HPC)	HPC ist der englische Begriff für <i>Heilberufsausweis (HBA)</i> und entsprechende Berufsausweise.
Heilberufler		Person, die einen Heilberuf ausübt. Der Heilberufler verfügt über einen <i>HBA</i> oder einen entsprechenden Berufsausweis, mittels dem er sich legitimieren kann. Der Heilberufler ist berechtigt, weitere Personen zu beauftragen, auf Verordnungsdaten und medizinische Daten zuzugreifen (§ 291a Abs. 5 SGB V/GMG). Die Zuordnung einer solchen Person zum beauftragenden Heilberufler muss nachprüfbar festgehalten werden. Der Begriff „Heilberufler“ wird im Rahmen des Projekts <i>Gesundheitskarte</i> als <i>Akteur</i> verwendet.
Heilberufsausweis	Health Professional Card (HBA, HPC)	Heilberufsausweis ist eine personenbezogene Mikroprozessorchipkarte mit kryptographische Funktionen, mit dem sich Angehörige der Heilberufe (<i>Ärzte</i> und <i>Apotheker</i>) gegenüber der <i>Telematikinfrastuktur</i> ausweisen und vertraulich (verschlüsselt) kommunizieren können. Außerdem enthält er eine <i>qualifizierte elektronische Signatur des Arztes</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
Heim-PC		Ähnlich wie der <i>eKiosk</i> ist grundsätzlich auch der Heim-PC des <i>Versicherten</i> ein mögliches <i>Primärsystem</i> , sofern dieser u. a. über ein Kartenlesegerät und einen Internetanschluss verfügt. Da der Heim-PC als unsicheres System anzusehen ist, müssen allerdings vor einer Nutzung für die <i>eGK</i> insbesondere Sicherheitsaspekte berücksichtigt werden.
HL7	Health Level 7	Amerikanischer Standard zur Normierung der Datenübertragung im Gesundheitswesen
HP	Health Professional	Heilberufler
HPC	Health Professional Card	Heilberufsausweis, Oberbegriff für <i>HBA</i> und <i>SMC</i>
HSM	Hardware Security Module	
http	Hypertext Transfer Protocol	
Hybridschlüssel	hybridkey	Ein symmetrischer kryptographischer Schlüssel, der durch den öffentlichen Schlüssel eines Public-Key-Schlüsselpaares verschlüsselt wurde und somit nur durch den Besitzer des privaten Schlüssels des Schlüsselpaares lesbar ist.
Hypertext Transfer Protocol	(http)	HTTP ist ein Protokoll zur Übertragung von Daten, das insbesondere im Rahmen des World Wide Web zum Einsatz kommt und sich meist auf das verbindungsorientierte TCP stützt.
I		
IANA	Internet Assigned Numbers Authority	
ICC	Integrated Circuit Card	
ICCSN	Integrated Circuit Card Serial Number	
ICM	IC Manufacturer	IC-Herstellerkennung
ID	Identifizier	eindeutiger Schlüssel zur <i>Identifizierung</i> von Objekten
ID des verordneten Mittels		Mit der Identifikationsnummer (ID) eines Arzneimittels ist derzeit die 7-stellige Pharmazentralnummer (PZN) gemeint, die zukünftig durch die Europäische Arzneimittelnummer (EAN) ersetzt wird. Arzneimittel oder sonstige Heil- und Hilfsmittel, die per se keine <i>PZN</i> haben werden gruppenweise einer <i>PZN</i> zugewiesen.
Identifizierung	Identification	Feststellung, ob die personenbezogenen Daten der <i>eGK</i> mit einer natürlichen Person übereinstimmen.
Identität	Identity	Im Kontext des Rechts bezeichnet Identität die Übereinstimmung der personenbezogenen Daten der <i>eGK</i> mit einer natürlichen Person. Diese Identität kann formal durch eine rechtsverbindliche Identitätsfeststellung, Vergleich von festgelegten Kriterien, bestimmt werden.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Identitätsüberprüfung		<p>Unter Identitätsüberprüfung wird der Prozess der Überprüfung einer behaupteten <i>Identität</i> einer natürlichen Person anhand eines oder mehrerer eindeutiger Identifizierungsmerkmale verstanden.</p> <p>Im Kontext der eGK findet diese Identitätsüberprüfung bei der Inanspruchnahme von Maßnahmen eines <i>Leistungserbringers</i> statt.</p> <p>Synonym: <i>Authentifizierung</i></p>
IEC	International Electrotechnical Commission	
IEEE	Institute of Electrical and Electronics Engineers	
IETF	Internet Engineering Task Force	
IFD	Interface Device	
IFSC	Information Field Size Card	
IFSD	Information Field Size Device	
IIN	Issuer Identification Number	Kennung des Kartenanbieters
IK		Institutionskennzeichen: Ordnungsbegriff für Teilnehmer am Telematikprozess
Implementierung		<p>Integration neuer Elemente in bestehende Strukturen.</p> <p>Im Kontext der Softwareentwicklung z.B. Modulentwurf, die Codierung, den Modultest und die Modulintegration, einschließlich Integrationstest.</p>
Incident		Ereignis, das eine Störung, Anfrage oder Aufträge qualifiziert und formalisiert beschreibt.
Incident Management	(IM)	ITIL-basierter Prozess, der alle <i>Incidents</i> registriert, kategorisiert, priorisiert und verfolgt. Die primäre Zielsetzung ist eine schnellstmögliche Bearbeitung der <i>Incidents</i> .
Information Technology Security Evaluation Criteria	(ITSEC)	<p>ITSEC ist ein europäischer Standard für die Prüfung und <i>Zertifizierung</i> von Produkten und <i>Systemen</i> im Hinblick auf ihre <i>Vertrauenswürdigkeit</i>. Hierbei betrachtet man die Wirksamkeit und Korrektheit der eingesetzten Sicherheitsmechanismen. Bei der Wirksamkeit spielt insbesondere die Mindeststärke der kritischen Sicherheitsmechanismen, die man in die Klassen „niedrig“, „mittel“ und „hoch“ einteilt, eine wichtige Rolle. Im Hinblick auf die Korrektheit unterscheidet man die Evaluationsstufen „E1“ bis „E6“ mit jeweils steigender <i>Vertrauenswürdigkeit</i>.</p>

Begriff	Englisch, (Abk.)	Definition (Synonym)
Information View		Der Information View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) beschreibt die Ausprägung und Semantik der verarbeiteten Daten, sowie die detaillierten Prozesse zur Datenverarbeitung. Diese Sicht legt die Struktur und Semantik der Informationen des Systems fest. Weitere Punkte sind die Definition von Quellen und Senken von Information sowie die Verarbeitung und Transformation von Information durch das System. Hierzu gibt es Integritätsregeln und Invarianten.
Informationsmodell		Das Informationsmodell gibt die fachliche Beschreibung (eindeutige Bezeichnung und Definition) der benötigten <i>Informationsobjekte</i> in einem definierten Kontext wieder (z.B. die der <i>Versichertenstammdaten</i> auf der Grundlage des §291 Abs. 2 SGB V).
Informationsobjekt		Logisches Element des <i>Informationsmodells</i> . Mit dem Informationsobjekt sind Anforderungen verknüpft wie z.B. Sicherheitsziele, welche wiederum nach bestimmten (Sicherheits-)Eigenschaften der die Informationsobjekte verarbeitenden Komponenten verlangen.
Informationssicherheit	IT- Security	Die Informationssicherheit schafft auf der Ebene der Informationstechnik (<i>Anwendungen</i> , Systeme und Netze sowie zugehörige Organisation) Voraussetzungen und bietet Lösungsmöglichkeiten zur Realisierung von Sicherheitsanforderungen, die aus der Nutzung von Informationen und IT-Ressourcen resultieren.
Informationssicherheitsmanagement		gezieltes Management von <i>Vertraulichkeit</i> , <i>Integrität</i> und <i>Verfügbarkeit</i> von Informationen/Daten, z. B. nach ISO/IEC 17799, IT-Grundschutzhandbuch, ISO/IEC TR 13335, CobiT, The Standard usw.
Infrastruktur		System von Einrichtungen, Ausrüstungen und Dienstleistungen, welches für den Betrieb einer Organisation erforderlich ist.
Installation		Funktionsfähige Bereitstellung von Hardware und Software in einer definierten Umgebung.
Institute of Electrical and Electronics Engineers	(IEEE)	IEEE (sprich ei trippel i) ist ein weltweiter Verband von Ingenieuren und Informatikern. Eine der Aufgaben des IEEE ist die Definition von Standards wie zum Beispiel des WLAN Standards (IEEE 802.11)
Institutionskarte		Die Institutionskarte entspricht technisch weitgehend der <i>Health Professional Card</i> , ist jedoch institutionsbezogen und wird lediglich bei Systemstart mit einer <i>PIN</i> freigeschaltet. In diesem Fall wird sie auch als <i>Security Module Card (SMC)</i> bezeichnet. Die Institutionskarte funktioniert nur in Verbindung mit einem <i>HBA</i> .
Institutionskennzeichen	(IK)	Das Institutionskennzeichen ist ein eindeutiges Merkmal für die <i>Identifizierung</i> von <i>Kostenträgern</i> und bestimmten <i>Leistungserbringern</i> (z.B. Apotheken)

Begriff	Englisch, (Abk.)	Definition (Synonym)
Integrated Services Digital Network	(ISDN)	Integrated Services Digital Network (ISDN) ist ein internationaler Standard für ein digitales Telekommunikationsnetz.
Integrität	Integrity	Integrität bezeichnet den Zustand der Korrektheit und Unverfälschtheit von Daten. Es sind nur erlaubte und beabsichtigte Veränderungen zugelassen und möglich. Datenintegrität bezeichnet die Integrität von gespeicherten und übertragenen Daten. Systemintegrität bezeichnet die Unverfälschtheit von Programmen und Programcode und damit die korrekte Funktion der <i>Anwendungen</i> , IT-Infrastruktur und Systemkomponenten.
Interaktionscheck		Paarweise Prüfung von Medikamenten oder Wirkstoffen auf bekannte und somit referenzierbare Wechselwirkung (Interaktion) zwischen den Medikamenten. Beispiel: Aspirin und Macumar, Referenz ABDamed.
Interface		Schnittstelle eines Systems, auf die durch andere Systeme zugegriffen werden kann
Intermediär		Vermittler zwischen zwei Systemen, wobei beide Systeme jeweils dem Intermediär vertrauen, nicht jedoch zwangsweise einander.
International Organization for Standardization	(ISO)	Die ISO (http://www.iso.org) ist eine internationale Vereinigung der Standardisierungsgremien von 151 Ländern. Sie verabschiedet internationale Standards in allen technischen Bereichen. Deutschland ist durch das Deutsche Institut für Normung (DIN) (http://www.din.de) und die USA durch ANSI in der ISO vertreten.
International Telecommunication Union	(ITU)	Die ITU ist eine weltweite Organisation, die sich mit technischen Aspekten der Telekommunikation beschäftigt. In ihrem Telecommunication Standardization Bureau (ITU-T) werden technische Normen erarbeitet und als Empfehlung veröffentlicht.
Internet Assigned Numbers Authority	(IANA)	Diese nicht-kommerzielle Organisation ist unter anderem für die Zuweisung von im Internet Protokoll verwendeten Portnummern zuständig.
Internet Engineering Task Force	(IETF)	Die Internet Engineering Task Force (IETF) ist eine große, offene, internationale Gemeinschaft, die sich um den reibungslosen Betrieb und die Weiterentwicklung der Internet-Architektur bemüht. Die in der IETF entwickelten Standards und Empfehlungen werden als Request for Comments (RFC) mit einer bestimmten laufenden Nummer unter http://www.ietf.org veröffentlicht.
Internet Protocol Security	(IPSec)	IPsec ist eine von der <i>IETF</i> entwickelte Sicherheitsarchitektur zur Gewährleistung von <i>Authentizität</i> , <i>Integrität</i> und <i>Vertraulichkeit</i> in IP-Netzen. Beispielsweise basiert die Sichere Inter-Netzwerk-Architektur (SINA) www.bsi.de/fachthem/sina/ auf IPSec.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Interoperabilität		Zusammenarbeit in einem offenen System (gemäß dem Client/Server-Modell). Unabhängig von der verwendeten Hardware, den eingesetzten Betriebssystemen, der verwendeten Netzwerktechnologie und der Realisierung einer <i>Anwendung</i> kann eine Zusammenarbeit zwischen diesen <i>Anwendungen</i> erfolgen.
IP	Internet Protokoll	
IPSec	Internet Protocol Security	
ISDN	Integrated Services Digital Network	
ISIS-MailTrust	(ISIS-MTT)	ISIS-MTT ist eine gemeinsame Spezifikation von TeleTrust e.V. (http://www.teletrust.de) und T7 e.V. (http://www.t7-isis.de) für <i>digitale Signaturen</i> , <i>Verschlüsselung</i> und <i>PKI</i> . Wesentliches Ziel ist es, durch ISIS-MTT die Voraussetzung für eine internationale Standardisierung und Interoperabilität für Anwendungen auf den genannten Gebieten zu schaffen.
ISIS-MTT	Intermediate System – Intermediate System MailTrust-Standard	
ISO	International Organization for Standardization	die internationale Vereinigung der Standardisierungsgremien von derzeit 148 Ländern
ISO 17799		vollständige Bezeichnung: ISO/IEC 17799:2000 (Information technology - Code of practice for information security management); entspricht inhaltlich dem British Standard Nr. 7799, Teil 1 (BS 7799-1:1999)
ISO/IEC 7816		Normenreihe für <i>Chipkarten</i>
IT		Informationstechnik
IT Service Management	(ITSM)	Gesamtheitliches prozessorientiertes Management definierter IT-Services mit dem Ziel der Qualitätssteigerung. Die IT Infrastructure Library (<i>ITIL</i>) stellt ein Best Practice Modell für das IT Service Management dar.
ITIL	IT Infrastructure Library	ITIL ist ein in Großbritannien entwickelter Leitfaden zur Unterteilung der Funktionen und Organisation der Prozesse, die im Rahmen des Betriebs einer IT-Infrastruktur eines Unternehmens entstehen (<i>IT Service Management</i>).
ITSEC	Information Technology Security Evaluation Criteria	Die Kriterien für die Bewertung der Sicherheit von <i>Systemen</i> in der Informationstechnik sind ein europäischer Sicherheitsstandard
ITU	International Telecommunication Union	
IV	Initial Value	

Begriff	Englisch, (Abk.)	Definition (Synonym)
K		
Kartenanwendung	card application	Die Kartenanwendung ist eine spezielle Form einer <i>Anwendung</i> .
Kartenanwendungsmanagement	Card Application Management (CAM)	Verwaltung der <i>Kartenanwendungen</i> einer <i>eGK</i> , welche bereits in die Karte geladen worden sind. Des Weiteren wird hier auch die Zuordnung, d.h. die Verknüpfung, einer <i>Anwendung</i> (sowohl Karten- als auch Serveranwendung) zu einer bestimmten <i>eGK</i> verwaltet.
Kartenanwendungsmanagementsystem	Card Application Management System (CAMS)	System für das <i>Kartenwendungsmanagement</i> .
Kartenherausgeber		Der Kartenherausgeber ist i.d.R. Eigentümer der Karte. Er ist verantwortlich für die Zuordnung einer Karte zu einer Person und veranlasst Ausstellung und Einzug von Karten. Der Begriff „Kartenherausgeber“ wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.
Karteninhaber		Der Karteninhaber ist die Person, welche die Entscheidungsbefugnis über den Einsatz einer <i>eGK</i> im Gesundheitswesen hat. Im Allgemeinen ist dies der <i>Versicherte</i> selbst.
Kartenlebenszyklus		Alle Stadien einer <i>Chipkarte</i> wie z.B. der <i>eGK</i> von der Beschaffung und Erzeugung der Daten, über die Personalisierung, die Ausgabe, die Nutzung, die Veränderung bis hin zur Terminierung. Der Kartenlebenszyklus wird im <i>Kartenmanagementsystem</i> verwaltet.
Kartenmanagement	Card Management (CM)	Dieser Begriff umfasst das gesamte Management einer <i>Chipkarte</i> wie z.B. der <i>eGK</i> : das Lebenszyklusmanagement, das Validitätsmanagement, das <i>Anwendungsmanagement</i> und das <i>Kartenanwendungsmanagement</i> . Der Begriff meint nicht die Verwaltung des Einsatzes der Karte z.B. in einem <i>Primärsystem</i> wie z.B. dem Praxis-Verwaltungssystem.
Kartenmanagementsystem	Card Management System (CMS)	System für das <i>Kartenmanagement</i>
Kartenpersonalisierer		Der Kartenpersonalisierer bringt optisch und elektronisch personenbezogene Daten in die Karte ein, die ihm authentisch und sicher zur Verfügung zu stellen sind. Zu beachten ist, dass der Kartenpersonalisierer im Allgemeinen selbst nicht für die Erhebung oder Aufbereitung der Daten verantwortlich ist. Im Speziellen ist es sogar möglich, dass der Personalisierer keinerlei Zugriff auf diese Daten erhält (mit Ausnahme der visuell auf der Karte lesbaren). Der Begriff „Kartenpersonalisierer“ wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Kartensystem	Card System (CS)	Gesamtsystem aller zur Verwaltung der eGK erforderlichen <i>Komponenten</i> . Dieses umfasst neben dem eigentlichen <i>Kartenmanagementsystem</i> zum Beispiel auch die <i>Komponenten</i> zur Verwaltung der zur eGK zugehörigen Schlüssel und <i>Zertifikate</i> .
Kartenterminal		Technische Einrichtung zum Kontaktieren der im System verwendeten <i>Chipkarten</i>
Kartenversender		Der Kartenversender übernimmt das Mailing der Karte. Dies umfasst im Allgemeinen das Personalisieren eines Anschreibens, das Aufbringen der personalisierten Karte auf das Anschreiben, das Kuvertieren und die Übergabe an ein Zustellunternehmen. Der Begriff „Kartenversender“ wird im Rahmen des Projekts eGK als <i>Akteur</i> verwendet.
Kartenverwalter		Der Kartenverwalter ist dafür zuständig, Karten ins Feld zu bringen, aus dem Feld zu nehmen und die auf der Karte befindlichen Applikationen während des gesamten Lebenszyklus der Karte zu koordinieren.
KB		Kilo Byte
KBSt		Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KBV		Kassenärztliche Bundesvereinigung
KD	Key derivation Data	
Kettenmodell		Das Kettenmodell ist ein so genanntes Gültigkeitsmodell für Zertifizierungspfade, bei dem alle <i>Zertifikate</i> im Pfad genau dann gültig sind, wenn der zugehörige <i>Zertifizierungsschlüssel</i> zum Zeitpunkt der Erstellung (des <i>Zertifikats</i>) auf einem gültigen <i>Zertifikat</i> beruht.
KGK	Key Generation Key	
KIS		Krankenhausinformationssystem, <i>Primärsystem</i> der Krankenhäuser
Kiss-'o-death		Mit Hilfe dieses Verfahrens kann der NTP Server die Anzahl der an ihn gerichteten Anfragen von korrekt implementierten und hierarchisch untergeordneten NTP Servern beeinflussen. Das Verfahren ist in Abschnitt 5.1.1.16 des Dokumentes „Spezifikation Infrastrukturkomponenten: Zeitdienst“ beschrieben.
KK		Krankenkasse
Klinische Basisdaten		Die Mindestdaten, die für eine Notfallversorgung vorhanden sein sollen. Gemäß § 291a Abs. 3, Satz 1 Nr. 1 SGB V/GMG können diese Daten mittels der eGK geführt werden. Hierbei handelt es sich um eine <i>freiwillige Anwendung</i> der eGK. Der Begriff wird synonym zu „ <i>Notfalldaten</i> “ verwendet.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Klinische Daten		Klinische Daten umfassen: § <i>klinische Basisdaten</i> (§ 291a Abs. 3, Satz 1, Nr. 1 SGB V/GMG) und die § erweiterten klinische Daten (§ 291a Abs. 3, Satz 1, Nr. 2-4 SGB V/GMG). Klinische Daten sind ein Synonym für „ <i>Medizinische Daten</i> “.
KM		<i>Kartenmanagement</i>
KMS		<i>Kartenmanagementsystem</i>
Known Error		Ein <i>Problem</i> , deren Ursache im <i>Problem Management</i> identifiziert wurde und durch das Problem Management als ein bereits bekannter Fehler deklariert wird. (ITIL-basierter Begriff)
Komponente	component	Physisches Element (z.B. <i>VODD, Kartenterminal</i>) mit bestimmten Eigenschaften, z. B. zur Gewährleistung der Einhaltung von Sicherheitszielen
Komponentenmodell		Abstraktion der physischen Systemarchitektur. Ein <i>System</i> wird soweit in einzelne Komponenten zerlegt, dass für die benötigte Sicht relevante Eigenschaft identifizierbar sind (z.B. Schnittstellen, <i>Sicherheitsanforderungen</i>).
Konkatenation		Die Konkatenation (auch Verkettung) ist der Vorgang und das Ergebnis der regelhaften linearen Aneinanderreihung von sprachlichen Elementen oder linguistischen Kategorien. Konkatenationen verknüpfen mindestens zwei Elemente (z.B. NP + VP), deren Reihenfolge durch die Verkettungsoperation festgelegt ist. In der generativen Transformationsgrammatik werden Konkatenationen durch Ersetzungsregeln im Basisteil erzeugt.
Konnektor		Der Konnektor koordiniert die Kommunikation zwischen <i>Primärsystem, eGK, HBA/SMC</i> und <i>Telematik-Infrastruktur</i> . Er stellt damit das Bindeglied zwischen diesen Komponenten auf Leistungserbringerseite bzw. eKiosk und Telematikinfrastruktur dar.
Kontra-Indikationscheck		Paarweise Prüfung von Medikamenten oder Wirkstoffe gegen Diagnosen oder Symptome auf bekannte und somit referenzierbare Gegenanzeigen (Kontraindikation). Beispiel: Morbus Crohn und Aspirin, Referenz ABDA-med.
Kostenerstattungsverfahren	procedure of compensation (for outlay)	Unter Kostenerstattungsverfahren ist, auch in Verbindung mit dem <i>SGB V</i> , die Wahl der Kostenerstattung für vorher verauslagte Kosten anstelle der zu gewährenden Sach- und Dienstleistungen zu verstehen.
Kostenträger	cost unit	Eine Person oder Institution, die für eine erbrachte Leistung die entstandenen Kosten ganz oder teilweise übernimmt. Im Kontext der <i>eGK</i> wird hiermit die Gruppe der (<i>privaten und gesetzlichen</i>) <i>Krankenversicherungen</i> bezeichnet. Der Begriff „Kostenträger“ wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Kostenträgerkennung		Institutionskennzeichen der <i>Krankenversicherung</i>
Krankenversichertenkarte	(KVK)	<i>Chipkarte</i> , welche seit 1995 den Krankenschein ersetzt hat. Die Karte enthält reine Verwaltungsdaten (<i>Krankenkasse</i> , Name, Geburtsdatum und Anschrift des <i>Versicherten</i> , <i>KVNR</i> und <i>Versichertenstatus</i>).
Krankenversichertennummer	(KVNR)	Eindeutige Krankenversichertennummer nach § 290 SGB V (20 bzw. 30 Stellen), zusammengesetzt aus: <ol style="list-style-type: none"> 1. Versicherten-ID (10 Stellen; unverkennbarer Teil der KVNR) 2. Krankenversicherungskennung (9 Stellen) 3. Versicherten-ID des zugeordneten Hauptversicherten (10 Stellen), sofern vorhanden 4. Prüfziffer (1 Stelle; über die vorangegangenen 19 bzw. 29 Stellen)
Krankenversicherung		Die Krankenversicherung umfasst die <i>Gesetzliche und Private Krankenversicherung</i> .
Krypto Subsystem		Funktionsfeld zur Verarbeitung von <i>PKI</i> Anwendungen (Signaturerstellung, -prüfung, Datenverschlüsselung, -entschlüsselung)
KV		Kassenärztliche Vereinigung
KVK		Krankenversichertenkarte
KVNR		Krankenversichertennummer
KZV		Kassenzahnärztliche Vereinigung
L		
L2TP	Layer 2 Tunneling Protocol	
Labortest	Testing in a specific test side	Unter Labortest wird der Qualitätssicherungsvorgang in einer isolierten Umgebung auf der Grundlage vorbereiteter Testdaten und Testfälle verstanden. Der Labortest beendet die Phase der Entwicklung
LAN	Local Area Network	Lokales Netzwerk (z. B. innerhalb einer Arztpraxis oder Apotheke)
Layer 2 Tunneling Protocol	(L2TP)	L2TP kommt als Protokoll bei Virtuellen Privaten Netzwerken zum Einsatz. Es dient zum Aufbau einer abgesicherten Verbindung zwischen zwei Netzwerken über ein ungesichertes Medium wie zum Beispiel das Internet.
LDAP	Leightweight Directory Access Protocol	
LE		<i>Leistungserbringer</i>
Lebenszyklus		Im Zusammenhang mit dem <i>Kartenmanagement</i> ist der Lebenszyklus der Karte gemeint. Siehe <i>Kartenlebenszyklus</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
Leistung		Jede in Verbindung mit der medizinischen Versorgung durch einen <i>Leistungserbringer</i> durchgeführte oder auch erbrachte Handlung. Eine Leistung kann aus mehreren Einzelleistungen bestehen. Eine Leistung ist ein Synonym für eine <i>medizinische Maßnahme</i> .
Leistungsanforderung	performance requirement capacity requirement benefit requirement	Leistungsanforderungen beziehen sich immer auf andere Anforderungen. In Bezug zu funktionalen Anforderungen werden Erfüllungsgrad (Abdeckung z.B. in %), Performance (Reaktionszeit in der Mensch-Maschine-Schnittstelle) oder Skalierungsangaben benötigt, im Bereich der nicht-funktionalen Anforderungen sind beispielhaft Durchlaufzeiten eines Standard-Workflows, aber auch Vorgaben zu Kosten-Nutzen-Verhältnissen nicht unüblich. WIE GUT muss das Produkt erfüllen. Beispiele: Schnelligkeit, Skalierbarkeit, Maßangaben zu funktionalen Anforderungen im Sinne von Messeinheit, Messwert, Messgrenzen
Leistungserbringer	(LE)	Organisation oder Person, die <i>Leistungen</i> des Gesundheitswesens für <i>Patienten</i> erbringen kann. Im Sinne von HL7 ist ein Leistungserbringer eine Teilnahme einer <i>Rolle</i> (z.B. <i>Heilberufler</i>) an einem Prozess (z.B. Verschreibung Rezept). Beispiele sind <i>Ärzte</i> , <i>Zahnärzte</i> , <i>Apotheker</i> , <i>Krankenhäuser</i> und sonstige Leistungserbringer. Der Begriff „Leistungserbringer“ wird im Rahmen des Projekts eGK als <i>Akteur</i> verwendet.
Leistungsniveau	Service Level	Im Rahmen eines <i>Leistungsvertrags</i> definierte <i>Leistung</i> .
Leistungsschein		Der Leistungsschein (LS) beschreibt genauestens den Vertragsgegenstand oder die vom Anbieter zu erbringende Leistung. Jeder zu erbringende Service und die zu erbringenden Supportfunktionen werden in einem separaten Dokument dargestellt. Der LS ist so gestaltet, dass neben den standardisierten, generell zu erbringenden Services auch optionale Services für diesen Bereich aufgeführt sind. Darüber hinaus regelt er die Liefermodalitäten unter Berücksichtigung der besonderen Gegebenheiten beim Kunden. Ferner soll der Leistungsschein die anzuwendenden standardisierten Funktionstests bezeichnen, mit deren Hilfe die Serviceleistung überprüft wird. Die zu einem LS gehörenden quantitativen Angaben werden in <i>Service Level Agreements</i> aufgeführt (siehe <i>SLA</i>).
Leistungsvertrag	Service Level Agreement	Als <i>Leistungsvertrag</i> , Dienstgütevereinbarung oder englisch <i>Service Level Agreement (SLA)</i> bezeichnet man eine Vereinbarung, die in der Regel Bestandteil eines Dienstleistungs- oder Wartungsvertrages ist. Darin werden beispielsweise Reaktionszeiten für Supportleistungen oder maximale Ausfallzeiten von IT-Services und deren quantitative Messung festgelegt (Definition gemäß ITIL)

Begriff	Englisch, (Abk.)	Definition (Synonym)
Leonardo		Symbolfigur im deutschen Gesundheitswesen ist die von Leonardo da Vinci in den Jahren um 1490 geschaffene Skizze "Proportionsschema der menschlichen Gestalt nach Vitruv". Auf der eGK ist diese Figur in einer gematik-spezifischen Fassung als verpflichtendes Erkennungsmerkmal dargestellt. Umgangssprachlich und auch in der eGK-Spezifikation Teil 3 wird sie als "Leonardo" bezeichnet
Lightweight Directory Access Protocol	(LDAP)	Mit dem Lightweight Directory Access Protocol (Spec. RFC2251) können Informationen, die in einem Verzeichnisdienst gespeichert sind, abgerufen oder modifiziert werden.
Linux		Populäres, quelloffenes UNIX Betriebssystem
Load Balancing		Lastenverteilung zwischen zwei Systemen, die den gleichen Dienst anbieten.
Logdaten, Logs		Daten über Ereignisse, z.B. Störungen
Lösungsarchitektur	solution outline	Ergebnisdokument des Vorprojektes bit4health: Darin wurde an Hand der in der <i>Rahmenarchitektur</i> vorgegebenen Regeln die <i>Telematikinfrastruktur</i> weiter detailliert.
Low-Level-Signaturformat		Bei Low-Level-Signaturformaten ist bitgenau spezifiziert, wie die zu signierenden Daten, oder ein <i>Hashwert</i> derselben, vor der eigentlichen <i>Anwendung</i> des asymmetrischen Kryptoalgorithmus, z.B. durch Füllmechanismen (<i>Padding</i>), aufzubereiten sind.
M		
MAC	Message Authentication Code	
MAC Adresse		eindeutige Hardware Adresse einer Netzwerkkarte
Masquerading		Masquerading (engl.) oder Adressmaskierung ist eine spezielle Form von <i>NAT</i> und wird zumeist verwendet, um mehreren Computern in einem <i>Local Area Network</i> Zugriff auf das Internet zu ermöglichen. Dabei werden im Gegensatz zu <i>NAT</i> nicht nur die <i>IP</i> -Adressen, sondern auch Port-Nummern umgeschrieben.
MB		Mega Byte
MDO		Medizinisches Daten Objekt
Medizinische Daten		Medizinische Daten sind im Kontext der eGK ein Synonym für „ <i>Klinische Daten</i> “.
Medizinische Maßnahme		Generisch für verschiedene Behandlungsarten (Diagnostik, operativer Eingriff, pflegerische Maßnahme, Rehabilitationsmaßnahme), unabhängig von der Art der durchführenden Einrichtung und der Dauer. Eine Maßnahme kann aus mehreren Einzelmaßnahmen bestehen. Eine medizinische Maßnahme ist ein Synonym für eine Leistung.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Message Authentication Code	(MAC)	Ein Message Authentication Code (MAC) dient zur Sicherung der <i>Integrität</i> und <i>Authentizität</i> einer Nachricht. Anders als bei einer <i>digitalen Signatur</i> werden hier aber keine asymmetrischen Kryptoalgorithmen, sondern symmetrische Algorithmen und <i>geheime Schlüssel</i> zur Erstellung und Prüfung des MACs eingesetzt.
Metadaten		Daten, die Informationen über andere Daten enthalten. Ein Beispiel wäre hier der Typ eines Dokumentes, der nicht zum Inhalt beiträgt, aber doch die Information enthält, über welche Anwendung das Dokument gelesen werden kann. Weitere Metadaten sind die Größe, der Eigentümer und das Datum des letzten Speicherns.
Metamodell		Mit einem Metamodell wird – wiederum in Form eines Modells – beschrieben, wie ein Modell formal auszusehen hat. Ein Metamodell ist somit ein Modell auf einer höheren Abstraktionsebene.
MF	Master File	
Migration		Übergang einer <i>Betriebsumgebung</i> von einem Release oder Versionsstand (bspw. Funktionsabschnitt) auf den Nächsten.
Migrationspfad		Der Migrationspfad beschreibt die Einführung der eGK in mehreren abgesicherten und beherrschbaren Stufen
MII	Major Industry Identifier	
Mikroprozessor-chipkarte	SmartCard	Ist eine <i>Chipkarte</i> mit einer kleinen CPU und arbeitet wie ein kleiner Computer ein ROM mit Betriebssystem und RAM. Zum Beispiel Kryptoverfahren können auf die Karte implantiert werden.
MKT		<i>Multifunktionales Kartenterminal</i>
Modellregion		Eine durch die Bundesländer festgelegte Region, mit der das jeweilige Bundesland die Einführung der eGK testen wird. Für Sachsen ist dies der Landkreis Löbau-Zittau.
Monitoring		Laufende Überwachung bestimmter kritischer Informationen, z.B. verfügbare Bandbreite, CPU-Auslastung, Anzahl fehlgeschlagener Verbindungsversuche aber auch nicht technischer Aspekte wie Rechtslage.
MPLS	Multi Protocol Label Switching	
MSB	Most Significant Byte	
MSE	Manage Security Environment	
Multi Protocol Label Switching	(MPLS)	Netzwerk-Transportprotokoll zur performanten Weiterleitung von (No Suggestions), besonders effizientes Verfahren zur Bildung von VPNs auf WANs

Begriff	Englisch, (Abk.)	Definition (Synonym)
Multiapplikative Chipkarte		Der Begriff „Multiapplikative Chipkarte“ sagt aus, dass sich auf einer Prozessorchipkarte mehrere <i>Anwendungen</i> befinden, zum Beispiel eine Bankkarte mit Telefonfunktion. Diese <i>Anwendungen</i> können vollständig voneinander getrennt verwaltet werden, so dass z. B. ein erlaubter Zugriff auf eine <i>Applikation</i> nicht impliziert, dass auch auf andere <i>Applikationen</i> zugegriffen werden darf.
Multifunktionales Kartenterminal	(MKT)	Zum Lesen und Beschreiben von Karten werden <i>Kartenterminals</i> benötigt. Für das Gesundheitswesen wurde in den vergangenen Jahren ein „Multifunktionales Kartenterminal (MKT)“ entwickelt, das auch in europäischen Projekten internationale Anerkennung gefunden hat. Das MKT ist für alle <i>Anwendungen</i> geeignet, die auf Karten, insbesondere <i>Smart Cards</i> basieren und durch einen PC gesteuert werden. Ein Modul zum Lesen der heutigen Versichertenkarte steht zur Verfügung. Höherwertige Terminals können auch mit Zahlungsfunktionen ausgestattet werden. Die <i>Spezifikation</i> ist im Internet unter der Adresse http://sit.gmd.de/SICA/mkt.html verfügbar (Quelle: [WuV])
Musterpraxis		Die Musterpraxis bildet die technische Infrastruktur einer Arztpraxis einschließlich Apotheke musterhaft nach. Sie dient der frühzeitigen Demonstration der Funktionsweise und Praktikabilität geplanter Lösungen. Im Sinne einer QS hat sie keine definierte <i>Rolle</i> . Gleichwohl wird empfohlen, Anregungen aus der Musterpraxis zu Abläufen und Verfahren bewertet in die QS und ggf. in die Entwicklung einfließen zu lassen.
Musterumgebung		Die Musterumgebung stellt ein Abbild der geplanten Gesundheitskartenanwendung bereit. Dabei wird ein Primärsystem oder Primärsystemsimulator mit Konnektor und Kartenterminal so verbunden, dass die Fachanwendungen durchgeführt werden können. Die Musterumgebung dient zum Anwendertest.
N		
Nachladeprozess	Post Issuance Process (PIP)	Nachladen von <i>Applikationen</i> auf die eGK
Name Server	(NS)	Programmsoftware, die auf einem Hostsystem gestartet wird und Informationen über eine spezifische DNS Namensraum-Struktur sowie die darin abgebildeten Ressourcendaten (siehe Resource Records) für anfragende Resolver bereitstellt.
NAT	Network Adress Translation	
National Institute for Standards and Technology (NIST)		Das NIST ist ein staatliches Standardisierungsinstitut in den USA. Zu den vom NIST publizierten Standards zählt beispielsweise <i>DSA</i> und <i>SHA-1</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
Need for Change	(NfC)	Formalisierte Anforderung an das <i>Change Management</i> einen Change durchzuführen. Auf Basis des NfC erstellt das <i>Change Management</i> einen <i>RfC</i> .
Network Adress Translation	(NAT)	Verfahren, das im Zuge der Verknappung von öffentlichen IPv4 Adressen entwickelt wurde und eine 1:n Umsetzung von einer öffentlichen IP Adresse auf n private Adressen erlaubt. Beispiele dafür finden sich am häufigsten bei geschäftlich genutzten, breitbandigen Internetanbindungen, die eine Vielzahl von im LAN vernetzten PC's (privates Netzwerk) über eine öffentliche Adresse mittels NAT mit dem Internet verbinden..
Network Time Protocol, The	(NTP)	Ein Netzwerkprotokoll, das mit dem Hintergrund entwickelt wurde, eine Vielzahl von vernetzten Systemen mit einer einheitlichen Zeitinformation zu versorgen, so dass diese Systeme auch tatsächlich über eine einheitliche Systemzeit verfügen. Die Entwicklung lässt sich zurückverfolgen bis zu einer Vorführung während der US National Computer Conference im Jahr 1979, während derer erste Gedanken zu einer weltweiten Computerzeitsynchronisation geäußert wurden (Quelle: [CNTS])
NFA		Nichtfunktionale Anforderungen
NFDD		Notfalldatendienst
Nichtabstreitbarkeit	Non-Repudiation	Unter Nichtabstreitbarkeit versteht man die Gewährleistung, dass die Urheberschaft, der Versand oder der Empfang von Daten und Informationen nicht in Abrede gestellt werden können. Die Nichtabstreitbarkeit ist eine Voraussetzung für die <i>Verbindlichkeit</i> und den Beweis einer Transaktion. Nichtabstreitbarkeit ist eine der zentralen <i>Sicherheitsanforderungen</i> neben <i>Verfügbarkeit</i> , <i>Integrität</i> , <i>Authentizität</i> und <i>Vertraulichkeit</i> .
Nichtapprobiertes Medizinpersonal		Personen, die gemäß § 291a Abs. 4 Satz 2.d. SGB V/GMG berechtigt sind, in einem Notfall klinische Basisdaten zu lesen. Der Begriff „Nichtapprobiertes Medizinpersonal“ wird im Rahmen des Projekts eGK als <i>Akteur</i> verwendet.
nicht-funktionale Anforderung	non-functional requirement	Eine nicht-funktionale Anforderung ist definiert durch Erwartungshaltungen, die keine Aktion darstellen, wie Effizienz, Effektivität und Selbstbeschreibungsfähigkeit und andere. Vorrangig handelt es sich um Anforderungen im Bereich der Benutzerfreundlichkeit. Nicht-funktionale Anforderungen können sich auf funktionale Anforderungen bzw. eine Gruppe funktionaler Anforderungen beziehen. Das kann ein System, eine Komponente, eine einzelne Aktion oder eine Prozessübersetzung in einen Workflow sein. WIE muss das Produkt erfüllen. Beispiele: Handhabung, Erwartungskonformität (aus EG-Richtlinie 90/270/EWG), Lernförderlichkeit, Anforderungsvielfalt, Redundanzfreiheit, Selbstbeschreibungsfähigkeit (ISO 9241/10), Steuerbarkeit, Individualisierbarkeit, Benutzeroberfläche (Schnittstelle) / Design

Begriff	Englisch, (Abk.)	Definition (Synonym)
NIST	National Institute for Standards and Technology	
Noctu		Binäres Kennzeichen des Papierrezeptes oder <i>eRezeptes</i> , welches vom <i>Arzt</i> oder Zahnarzt gesetzt wird, um eine notwendige Belieferung während der allgemeinen Ladenschlusszeiten von Apotheken zu kennzeichnen und somit eine Abrechnung des zugehörigen <i>Noctu-Zuschlages</i> der Apotheke gegenüber dem <i>Kostenträger</i> zu ermöglichen.
Non Volatile Random Access Memory	(NVRAM)	Nicht flüchtiger Speicher mit wahlfreiem Zugriff. In ihm wird in einem Rechnersystem das <i>BIOS</i> oder die Firmware abgelegt.
Notfalldaten		Elektronischer Datensatz auf der <i>eGK</i> mit den Daten zu notfallrelevanten Informationen wie z.B. Allergien.
NTP	Network Time Protocol, The	
NTP-DDoS		Distributed Denial of Service-Angriff (<i>DDoS</i>) auf den NTP-Dienst.
NTP-DoS		<i>Denial of Service</i> (DoS)-Angriff auf den <i>NTP-Dienst</i> ..
NTP-Server		Serversysteme, die mittels NTPd (NTP daemon) Zeitsynchronisationsdienste anbieten und sich selber mit einer Zeitquellesynchronisieren können. In Deutschland bietet die Physikalisch-technische Bundesanstalt beispielsweise öffentliche Stratum 1 Server an, die unter den Namen <code>ptbtime1.ptb.de</code> und <code>ptbtime2.ptb.de</code> erreichbar sind.
NVRAM	Non Volatile Random Access Memory	
O		
OASIS	Organization for the Advancement of Structured Information Standards	
ObjektReferenz		Eindeutiger Verweis auf ein Objekt innerhalb eines Fachdienstes, bestehend aus Diensttyp, Dienstinstanz und Objekt ID des Objektes. Durch die Objekt Referenz kann jedes Objekt innerhalb der Telematikinfrastruktur eindeutig adressiert werden.
ObjektTicket		Ein ObjektTicket bezeichnet Berechtigungsinformationen zu einem Objekt. In einem ObjektTicket sind sowohl die Informationen über die Zugriffsrechte einer Identität auf ein Objekt als auch der Hybridschlüssel für eine zugelassene Identität enthalten.
OCSP	Online Certificate Status Protocol	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Öffentlicher Schlüssel	public key (PK)	Der öffentliche Schlüssel ist ein Bestandteil des Schlüsselpaares bei <i>Public-Key-Kryptographie</i> . Im Gegensatz zu dem <i>privaten Schlüssel</i> muss dieser nicht geheim gehalten werden und wird zum Beispiel im entsprechenden <i>Zertifikat</i> des Eigentümers verbreitet.
OID	Object Identifier	Objektkennung
Online Certificate Status Protocol	(OCSP)	OCSP ist ein in RFC2560 von der <i>IETF</i> standardisiertes Client-Server-Protokoll zur Abfrage des Status von <i>Zertifikaten</i> . Mittels dieser Online Abfrage kann beispielsweise geprüft werden, ob ein <i>Zertifikat</i> durch den <i>Benutzer</i> gesperrt worden ist.
OP		Offene(r) Punkt(e)
Open Systems Interconnection	(OSI)	kurz für: Open Systems Interconnection Reference Model. Offenes Schichtenmodell für die Kommunikation informationsverarbeitender <i>Systeme</i> bestehend aus 7 Ebenen.
Operation Level Agreement		Ein Operation Level Agreement (OLA) ist eine Vereinbarung mit einem internen Dienstleister und enthält Absprachen über die Erbringung von definierten Services. Da es eine firmen- bzw. konzerninterne Vereinbarung ist, entspricht ein OLA in der Regel keinem Vertrag im juristischen Sinne, sondern nur einer Dienstleistungsvereinbarung. Dienstleistungen werden in den Leistungsscheinen definiert und die dazu gehörenden SLAs spezifizieren die Leistungsparameter.
Operational Level Agreement	(OLA)	Nach innen gerichtete Vereinbarung über die Erbringung definierter Services. Ziel ist die Gewährleistung eines mit Kunden vereinbarten <i>SLA</i> . (ITIL-basierter Begriff)
Operationale Risiken	operational risks	Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und <i>Systemen</i> oder infolge externer Ereignisse eintreten.
Organization for the Advancement of Structured Information Standards	(OASIS)	OASIS (http://www.oasis-open.org/) ist ein nicht-kommerzielles, globales Konsortium für die Entwicklung und Umsetzung von Standards für eBusiness und XML.
OSI	Open Systems Interconnection	
OTC	Over the Counter	OTC steht für „over the counter“. Mit OTC-Präparaten/-Medikamenten werden i.A. nicht verschreibungspflichtige und somit frei verkäufliche Präparate/Medikamente (wie z.B. Aspirin) bezeichnet.
P		
Packungsgröße		Menge und Einheit der Packung eines Arzneimittels, z.B. N20

Begriff	Englisch, (Abk.)	Definition (Synonym)
Padding		Unter Padding versteht man allgemein das Ergänzen einer Zeichenfolge um zusätzliche Zeichen, damit eine bestimmte Gesamtlänge erreicht wird. Beispielsweise wird der <i>Hash-Wert</i> einer Nachricht beim RSA-Verfahren aus Sicherheitsgründen um bestimmte Füllzeichen ergänzt, bevor die Signaturerzeugung durch Exponentiation mit dem <i>privaten Schlüssel</i> vorgenommen wird.
PassG		Passgesetz
PassV		Passverordnung
PassVwV		Passverwaltungsvorschrift zur Durchführung des Passgesetzes
Patches		Kleinere Korrekturen an ausgelieferter Software
Patient	patient	Natürliche Person, die medizinische Leistungen beansprucht. <i>Akteursbegriff</i>
Patientenfach		Elektronischer Datencontainer auf der eGK oder in der <i>Telematikinfrastruktur</i> für die Ablage und Übermittlung von vom <i>Versicherten</i> selbst oder für diesen zur Verfügung gestellten Daten, die sich ausschließlich in der Datenhoheit des <i>Versicherten</i> befinden. Mehrere Anwendungen können hierzu definiert werden (§ 291a Abs. 3, Satz 1, Nr. 5 SGB V/GMG).
Patienteninformation		Die Patienteninformation oder Aufklärung dient als Voraussetzung für eine wirksame Einwilligung zur Nutzung der <i>freiwilligen Anwendungen</i> der eGK. Die Patienteninformation muss objektiv und in einer für den Patienten verständlichen Form erfolgen.
Patientenquittung		Elektronischer Datensatz über in Anspruch genommene Leistungen und deren vorläufige Kosten mit dem Ziel, dass der Patient diese einsehen kann (§ 291a Abs. 3, Satz 1, Nr. 6 SGB V/GMG). Teile davon sind beispielsweise eine Kurzbeschreibung einer Leistung, der zugehörige Preis oder die Unterschrift des <i>Leistungserbringers</i> .
Payload		Nutzlast an Daten, die durch ein Protokoll oder eine Nachricht transportiert wird.
PB		Projektbüro
PC	Polycarbonat	Material für Karten. Auch genutzt für PC: Personal Computer
PC/SC	Interoperability Specification for ICCs an Personal Computer Systems (References)	
PCS	Procedure Coding System	
PDD		Patientendatendienst

Begriff	Englisch, (Abk.)	Definition (Synonym)
Personal Identification Number	(PIN)	Eine PIN ist eine in der Regel vier- bis achtstellige persönliche Geheimzahl, welche zur <i>Authentifizierung</i> ihres Inhabers bei der Nutzung elektronischer <i>Anwendungen</i> genutzt wird. So kann z.B. über eine PIN eine <i>Signaturerstellungseinheit</i> vor unberechtigtem Zugriff geschützt werden.
Personal Security Environment	(PSE)	Ein PSE ist ein Aufbewahrungsmedium für <i>private Schlüssel</i> und vertrauenswürdige <i>Zertifikate</i> . Ein PSE kann entweder als Software-Lösung, z.B. als mittels Passwort geschützte Datei im PKCS #12-Format, oder als Hardware-Lösung, beispielsweise in Form einer <i>Smart Card</i> , realisiert sein.
Personalisierung	personalization	Vorgang der Zuordnung einer Karte zu einer Person. Dabei werden die optische <i>Personalisierung</i> (zum Beispiel Hochprägung, Lasergravur) und die elektrische <i>Personalisierung</i> (Laden der personenbezogenen Daten in den Speicher der <i>Chipkarte</i>) unterschieden.
Personenbezogene Applikation		Die auf eine Person bezogene Ausprägung einer <i>Anwendung</i> nach §291a SGB V/GMG (z. B. die Arzneimittel-dokumentation von Frau Klara Mustermann)
Personl Unblocking Key	(PUK)	Die PUK ist ein persönlicher Entsperrungsschlüssel, der es erlaubt, ein durch <i>PIN</i> geschütztes Gerät nach mehrmaliger Falscheingabe zu entsperren und eine neue <i>PIN</i> zuzuordnen.
PET		Polyethylenterephthalat als Material für Karten
Pharmazentralnummer	(PZN)	Bundeseinheitliches Arzneimittelkennzeichen zur Kodierung von Fertigarzneimitteln, die eine <i>Identifizierung</i> nach Warenzeichen, Wirkstoffstärken, Darreichungsform, <i>Packungsgröße</i> und pharmazeutischem Hersteller ermöglicht.
PHB		Projekthandbuch
Physikalisch Technische Bundesanstalt	(PTB)	Die PTB mit Sitz in Braunschweig hat per Deutschem Zeitgesetz von 1978 den Auftrag, die amtliche Deutsche Zeit zur Verfügung zu stellen. Zur Ermittlung der Zeit wird auf das physikalische Verhalten von Cäsium 133 zurückgegriffen, aus dem sich eine Sekunde herleiten lässt: <i>"Die Sekunde ist das 9 192 631 770-fache der Periodendauer der dem Übergang zwischen den beiden Hyperfeinstruktur-niveaus des Grundzustandes von Atomen des Nuklids 133CS entsprechenden Strahlung."</i> Die PTB verfügt über verschiedene Cäsium- und Cäsium-Fontänen Uhren.
Physisches Kartenmanagement		Unter dem Begriff „Physisches Kartenmanagement“ wird im Kontext der eGK die Verwaltung von <i>Gesundheitskarten</i> als physikalische Datenträger verstanden. Dies beinhaltet alle zur Ausstellung und Verwaltung der eGK benötigten Prozesse.
PI	Padding Indicator	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Pilotierung		Als Pilotierung wird die QS-Phase verstanden, in der erstmalig mit Echtdateien und in der Zielumgebung operiert wird. Die Pilotierung wird häufig als Paralleltest aufgesetzt, so dass in dieser Phase die Altverfahren weiterhin den Regelbetrieb absichern.
PIN	Personal Identification Number	Persönliche Identifikationsnummer
PIP	Post Issuance Processing	Nachladeprozess
PK	Public Key	<i>Öffentlicher Schlüssel</i>
PKCS	Public Key Cryptography Standards	
PKI	Public Key Infrastructure	
PKV		Private Krankenversicherung
PL		Projektleiter / Projektleitung
PL-API		Plattform-API (interne Schnittstelle zu den Infrastrukturdiensten)
PLZ		Postleitzahl
Point-to-point Protocol	(PPP)	Das Point-to-point Protocol erlaubt es, TCP/IP-Verbindungen via Telefonleitung und Modem/ISDN herzustellen.
PP	Protection Profile	Schutzprofil
PPP	Point-to-Point Protocol	
PPS	Protocol Parameter Selection	
Primäres Vertragsverhältnis		Das Vertragsverhältnis eines <i>Versicherten</i> mit demjenigen <i>Kostenträger</i> , welcher in erster Instanz die Behandlungskosten trägt.
Primärsystem	(PS)	Ein IT-System, das bei einem <i>Leistungserbringer</i> eingesetzt wird - z.B. eine <i>Praxisverwaltungssoftware (PVS)</i> , ein <i>Krankenhausinformationssystem (KIS)</i> oder eine <i>Apothekensoftware (AVS)</i> und sich unter dessen administrativer Hoheit befindet.
Privater Schlüssel	Private Key (PrK)	Der private Schlüssel ist der Teil eines kryptographischen Schlüsselpaares, auf den nur der Inhaber des Schlüsselpaares zugreifen kann. Er wird in einem Personal Security Environment aufbewahrt und verwendet, um <i>digitale Signaturen</i> zu erstellen oder Daten zu entschlüsseln
PrK	Private Key	<i>Privater Schlüssel</i>
PRND	Padding Random Number	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Problem		Zusammenfassende Beschreibung von <i>Incidents</i> , deren Ursache unbekannt ist. (ITIL-basierter Begriff)
Problem Management		ITIL-basierter Prozess, der <i>Incidents</i> analysiert, um ihre Ursachen zu identifizieren. Aufgabe des Problem Management ist es ebenfalls, <i>Workarounds</i> zu erarbeiten und ggf. <i>NfC</i> zur Ursachenbehebung an das <i>Change Management</i> zu stellen. Zielsetzung des Prozesses ist die Vermeidung zukünftiger <i>Incidents</i> .
Projektrisiken	project risk	Risiken die den vorgesehene Ablauf oder die Ziele eines Projektes gefährden.
Protection Profiles		<i>Schutzprofile</i>
Proxy		Anwendungs-Gateway, welches Daten an einen Dienst weiterleitet. Hierbei kann je nach Ausprägung eine Pufferung der Daten erfolgen und somit die Last auf einem Backend-Dienst reduziert werden. Bei einem Proxy ist üblicherweise nicht vorher definiert, an welchen Dienst eine Anfrage weitergeleitet werden soll. Diese Information entnimmt der Proxy aus der Anfrage.
Prozess		Unter einem Prozess versteht man einen definierten Ablauf von Zuständen eines Systems. Der Begriff wird im Kontext der Telematik verwendet, um betriebliche Abläufe zu bezeichnen (Geschäftsprozess, Betriebsprozess) wie auch um technische Abläufe zu benennen (Ausführung von Programmen und Programmschritten).
PS		<i>Primärsystem</i>
PSE	Personal Security Environment	
Pseudo-PZN		Sonderkennzeichen für z. B. Rezeptur, Beschaffungskosten usw. (Technische Anlage 1 zur Vereinbarung über die Übermittlung von Daten im Rahmen der Arzneimittelabrechnung gemäß § 300 SGB V)
PSO	Perform Security Operation	
pt	point	Maß für die Größe einer Schrift
PTA		Pharmazeutisch-Technischer Assistent
PTB	Physikalisch Technische Bundesanstalt	
Public Key Cryptography Standards	(PKCS)	PKCS ist eine von den Laboratorien der US-amerikanischen Firma RSA Security Inc. entwickelte Reihe von Standards für Technologien auf Basis von asymmetrischen Kryptoalgorithmen.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Public Key Kryptographie		Bei der Public Key Kryptographie kommen für die <i>Ver-schlüsselung</i> und für die <i>Entschlüsselung</i> unterschiedliche Schlüssel zum Einsatz. Die beiden Schlüssel werden als Paar genutzt. Ein Schlüssel dieses Paares muss geheim gehalten werden und wird daher als <i>privater Schlüssel</i> bezeichnet. Der andere Schlüssel, der nicht geheim gehalten werden muss, wird auch <i>öffentlicher Schlüssel</i> genannt. Aufgrund der Ungleichheit der Schlüssel wird dieses Verfahren auch als asymmetrische Verschlüsselung bezeichnet.
Public-Key-Infrastruktur	(PKI)	Eine PKI ist eine technische und organisatorische Infrastruktur, die es ermöglicht, kryptographische Schlüssel-paare (<i>private Schlüssel</i> in Form von <i>PSEs</i> und <i>öffentliche Schlüssel</i> in Form von <i>Zertifikaten</i>) auszurollen und zu verwalten. Zu den wesentlichen Kernkomponenten einer PKI zählt die <i>Registrierungsinstanz</i> , die <i>Zertifizierungsinstanz</i> und der <i>Verzeichnisdienst</i> . Unter Umständen umfasst eine PKI auch einen <i>Zeitstempeldienst</i> und <i>Attributbestätigungsinstanzen</i> .
Public-Key-Kryptosystem		Public-Key-Kryptosysteme verwenden asymmetrische Verschlüsselungsalgorithmen.
Public-Key-Zertifikat		Ein Public-Key-Zertifikat ist ein <i>Zertifikat</i> , das insbesondere den Namen des Zertifikatsinhabers und den <i>öffentlichen Schlüssel</i> enthält.
Pufferüberlauf	Buffer-Overflow	Häufigste Sicherheitslücke in aktueller Software, die sich dazu eignet über Netzwerke unautorisiert die vollständige Kontrolle über Computersysteme zu erlangen oder deren <i>Verfügbarkeit</i> signifikant zu verringern. Im Wesentlichen werden bei einem Pufferüberlauf durch Fehler in einem Programm zu große Datenmengen in einen dafür zu kleinen Ziel-Speicherbereich geschrieben, wodurch dem Ziel-Speicherbereich nachfolgende Informationen überschrieben werden.
PUK	Personal Unblocking Key	
PuK	Public Key	<i>Öffentlicher Schlüssel</i>
PVC		Polyvinylchlorid als Kartenmaterial
PVS		Praxisverwaltungssystem, <i>Primärsystem</i> des Arztes
PZN		Pharmazentralnummer
Q		
QES	Qualified Electronic Signature	<i>qualifizierte elektronische Signatur</i>
QS	Quality Assurance	Qualitätssicherung

Begriff	Englisch, (Abk.)	Definition (Synonym)
Qualifizierte elektronische Signatur	Qualified Electronic Signature	Eine qualifizierte elektronische Signatur ist gemäß § 2 Nr. 3 SigG eine <i>fortgeschrittene elektronische Signatur</i> , die unter Verwendung einer <i>sicheren Signaturerstellungseinheit</i> erzeugt wurde und zum Zeitpunkt der Signaturerstellung auf einem gültigen <i>qualifizierten Zertifikat</i> beruht. Durch die qualifizierte elektronische Signatur kann die Schriftform ersetzt und somit auf kostenintensive Papierprozesse verzichtet werden.
Qualifizierter Zeitstempel	Qualified Time Stamp	Ein qualifizierter Zeitstempel ist gemäß § 2 Nr. 14 SigG ein <i>Zeitstempel</i> , der von einem <i>Zertifizierungsdiensteanbieter</i> gemäß Signaturgesetz ausgestellt wird. Ein solcher Zeitstempel hat eine sehr hohe Beweiskraft vor Gericht. Durch einen qualifizierten Zeitstempel werden die zeitgestempelten Daten quasi „rechtssicher eingefroren“.
Qualifiziertes Zertifikat		Ein qualifiziertes Zertifikat ist gemäß § 2 Nr. 7 SigG ein <i>Zertifikat</i> , das von einem <i>Zertifizierungsdiensteanbieter</i> gemäß Signaturgesetz für natürliche Personen ausgestellt wird. Die detaillierten Inhalte eines qualifizierten Zertifikats ergeben sich aus § 7 SigG. Bei der Ausgabe von qualifizierten Zertifikaten müssen die Anforderungen des Signaturgesetzes berücksichtigt werden. Insbesondere muss eine <i>Identifizierung</i> des Signaturschlüsselinhabers anhand eines amtlichen Ausweises erfolgen.
Quittung der Anforderungsmeldung	receipt	Schriftlich formalisierte Darstellung der Quittung des Eingangs einer Anforderungsmeldung. Sie gibt dem Anforderungssteller die Sicherheit, dass die Anforderungsmeldung in der gematik im Anforderungsmanagement eingegangen ist Text „Sie haben eine Anforderungsmeldung an die gematik gesendet, vielen Dank. Die Anforderungsmeldung hat die Nummer 99999 erhalten. Wir werden Sie in Kürze über den Bearbeitungsstand informieren.“
R		
RA	Registration Authority	
Rahmenarchitektur		Ergebnisdokument des Vorprojektes bit4health: Die Rahmenarchitektur von bit4health gibt basierend auf den gesetzlichen Vorgaben die Leitlinien für die Implementierung der Funktionen der eGK und der unterstützenden technischen Infrastruktur vor.
Rahmenvertrag		Durch den Rahmenvertrag (RV) wird eine Vereinbarung zwischen der gematik und einer juristischen oder natürlichen Personen geschlossen, die einfach oder mehrfach eine Zusammenarbeit, ein Auftraggeber/Auftragnehmer Verhältnis, ein Verkäufer/Käufer-Verhältnis oder ein Dienstleistungsverhältnis betreffen. Der RV regelt grundsätzliche Aspekte der Zusammenarbeit. Zu dem RV werden konkrete Einzelaufgaben in separaten Leistungsscheinen (LS) mit den dazu gehörenden <i>Service Level Agreements (SLA)</i> definiert.

Begriff	Englisch, (Abk.)	Definition (Synonym)
RAID	Redundant Array of Inexpensive Disks	
RC	Retry Counter	
RCA	Root CA	Wurzelinstanz
RD	Reference Data	Referenzdaten
Realisierung		Der Begriff bezeichnet den Vorgang der Verwirklichung von Konzepten, also z.B. die Erstellung eines Programms oder Einrichtung einer Organisation.
Realisierungskonzept		Zusammenfassendes Konzept, das die Planung von Änderungen von der Initialisierung bis zum Übergang in den Betrieb umfasst. Teil des Realisierungskonzeptes ist u. A. der Projektplan.
Rechteprüfung	Examination of Rights	Prüfung der Zugriffsberechtigung eines Benutzers/Subjekts auf ein Objekt zum Zeitpunkt der Zugriffsanforderung, basierend auf der Identität des Benutzers/Subjekts bzw. Rollen- oder Gruppeneigenschaften und den beim Objekt hinterlegten Rechten oder Zugriffsregeln.
Rechteverwaltung	Permission Management	Die Rechteverwaltung ist die konzeptionelle und administrative Festlegung von Zugriffsrechten von Benutzern/Subjekten, also z.B. die Zuordnung von Benutzern zu Gruppen, basierend auf der <i>Identität</i> des Benutzers/Subjekts.
Rechtssicherheit		Rechtssicherheit wird erreicht, wenn der jederzeitige Nachweis der Einhaltung der relevanten Gesetze möglich ist.
Redundant Array of Inexpensive Disks	(RAID)	Ein Raid-System erlaubt die Abstraktion von physikalischen Festplatten zu logischen Laufwerken, um so wirtschaftlich eine erhöhte Ausfallsicherheit (durch Redundanz) oder höhere Geschwindigkeit oder beides zu erreichen.
Referenzumgebung		Eine Referenzumgebung stellt ein Konfigurationsmuster dar, das als Vorlage für die Implementation weiterer Installationen für die Anwendung der Gesundheitskarte dient. Die Referenzumgebung enthält je eine der benötigten Komponenten in einer als Standard für die jeweilige Ausbaustufe gültigen Verbindung.
Regelbetrieb		Der Regelbetrieb ist die Phase, in welcher der Einführungsprozess für den definierten Produkt- und Prozessumfang abgeschlossen ist.
Registrierungsinstanz	Registration Authority (RA)	Eine Registrierungsinstanz ist der Bestandteil einer <i>PKI</i> , bei dem ein Benutzer ein <i>Zertifikat</i> beantragen und ggf. dessen Sperrung veranlassen kann. Im Zuge des erstmaligen Registrierungsprozesses werden die <i>Identität</i> des Antragstellers und möglicherweise zusätzliche <i>Attribute</i> überprüft, so dass die Korrektheit der Angaben im <i>Zertifikat</i> gewährleistet ist.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Registrierungsstelle	Registration Authority (RA)	Vertrauenswürdige Stelle, die die <i>Identität</i> eines Antragstellers für <i>Zertifikate</i> nach festgelegten Regeln prüft und die Daten an den ZDA weiterleitet
RegTP		Regulierungsbehörde für Telekommunikation und Post
Release		Ein Release fasst eine Reihe neuer oder geänderter Konfigurationselemente zusammen, die gemeinsam zum Einsatz gebracht werden müssen.
Release		Zusammenfassung von Versionen oder Varianten aller für eine Einsatzumgebung benötigten Ergebnistypen zu einem Terminstand.
Releasedefinition	release definition	Beschreibung des geplanten Inhaltes mit Motivation durch <i>Auftragsanforderungen</i> jedoch ohne konzeptionelle Lösungsansätze, der zu einem Release führen soll.
Release Management	(RM)	ITIL-basierter Prozess, der für die operativer Ausführung von <i>Changes</i> , die durch das <i>Change Management</i> beauftragt wurden, verantwortlich ist. Das Release Management hat eine ganzheitliche Sicht auf die Veränderungen an einem IT-Service.
Request for Change	(RFC)	Formalisierte vollständige Beschreibung eines Änderungsbedarfs. Wird im <i>Change Management</i> aus einem <i>NfC</i> generiert. (ITIL-basierter Begriff)
Resolver		Programmsoftware, die – getrieben von Client Anfragen – Informationen aus dem Datenbestand von Name Servern extrahiert und an das anfragende Clientsystem zurückgibt.
Restrisiko	residual risk	Nach der Festlegung von Maßnahmen zur Senkung von <i>Risiken</i> und/oder der bewussten Entscheidung für die Akzeptanz von <i>Risiken</i> verbleibendes <i>Risiko</i> .
Reverse Proxy		Ein Reverse Proxy dient wie ein <i>Proxy</i> zur Weiterleitung von Anfragen an einen Dienst. Jedoch ist beim Reverse Proxy fest definiert, an welchen Dienst oder welche Dienste die Weiterleitung erfolgt. Reverse Proxys werden üblicherweise als Load Balancer oder zum Überprüfen von Nachrichtenstrukturen sowie (No Suggestions) verwendet.
Revocation Status		Wird im Zusammenhang mit <i>Digitalen Zertifikaten</i> verwendet. Gibt an ob ein <i>Zertifikat</i> zu einem gegebenen Zeitpunkt gültig war oder ob die ausstellende Instanz dieses <i>Zertifikat</i> zurückgezogen hatte.
Rezept	prescription	Transportmittel zur Übermittlung ärztlicher <i>Verordnungen</i> über Arzneimittel, Heil- und Hilfsmittel und Therapien in der heutigen Form als Papierrezept, welches bis zu drei <i>Verordnungen</i> enthält, vom <i>Arzt</i> oder <i>Zahnarzt</i> ausgestellt wird und über den <i>Patienten</i> in der Apotheke oder Versandapotheke eingelöst wird. Unterformen: BtM-Rezept, Grünes Rezept, GKV-Rezept oder Privatrezept.
RF	Radio Frequency	
RFC	Request for Comment	

Begriff	Englisch, (Abk.)	Definition (Synonym)
RID	Registered Application Provider Identifier	
Risiko	risk	Ein Risiko ist die Kombination der Wahrscheinlichkeit, dass ein Schadensfall eintritt, und die hieraus resultierende Schadenshöhe
RM		Risikomanagement
RND	Random Number	Zufallszahl
Rolle	role	Eine Rolle beschreibt die Verhaltensweise eines <i>Akteurs</i> in einer definierten Aufgabenstellung.
Rollenbasierte Zugriffskontrolle	role based access control	Die <i>Zugriffskontrolle</i> eines IT-Systems ist nicht unmittelbar auf ein Objekt (Person, Anwendung) bezogen, sondern wird je <i>Rolle</i> festgelegt.
Rollout		Markteinführung. Als Rollout wird der Vorgang bezeichnet, über den neue Produkte und Verfahren in die Fläche gebracht werden, hier also insbesondere der Vorgang der Auslieferung, Verteilung und Installation von Software und Hardware.
Root		Wurzel: Oberste CA in einer Hierarchie einer <i>PKI</i>
Root-CA		Wurzel-Zertifizierungsinstanz.
Router		Aktive Netzwerkkomponente, die zwischen zwei Netzen gleichen Typs mit unterschiedlichen Adressräumen vermittelt.
RSA		Risiko-Struktur-Ausgleich
RSA-Algorithmus		Der nach seinen Erfindern (Rivest, Shamir und Adleman) benannte RSA-Algorithmus ist ein asymmetrischer Kryptalgorithmus, der zur <i>Verschlüsselung</i> und zur Realisierung <i>digitaler Signaturen</i> verwendet werden kann. Die Sicherheit dieses Verfahrens basiert auf der kryptographischen Annahme, dass das Faktorisierungsproblem für große Zahlen nicht effizient gelöst werden kann.
S		
SAGA		Standards und Architekturen für eGovernment-Anwendungen des Bundesministerium des Inneren
SAVeD		Sicherer Anbindungs- und Vermittlungsdienst
SC	1. Security Condition 2. Smart Card	1. Sicherheitsbedingung 2. anderer Begriff für Prozessorkarte
Schalenmodell		Das Schalenmodell ist ein so genanntes Gültigkeitsmodell für <i>Zertifizierungspfade</i> , bei dem alle <i>Zertifikate</i> im Pfad zu einem einheitlichen Prüfzeitpunkt gültig sind. Für <i>Authentisierungen</i> wird dabei der aktuelle Zeitpunkt betrachtet und für <i>elektronische Signaturen</i> der Erstellungszeitpunkt. Siehe auch <i>Kettenmodell</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
Schlüsselmanagement	Key Management (KM)	Verwaltung von Schlüsseln. Bezüglich des <i>Kartensystems</i> ist hier das Schlüsselmanagement für die <i>eGK</i> gemeint.
Schlüsselmanagementsystem	Key Management System (KMS)	System (bzw. eine Komponente im gesamten Kartensystem) für das <i>Schlüsselmanagement</i> .
Schutzprofile	protection profile	Schutzprofile ermöglichen es, eine Sicherheitslage anhand von Gefährdungen, Annahmen über die Betriebsumgebung der IT, Sicherheitszielen usw. zu beschreiben. Schutzprofile bilden somit die Grundlage für die Standardisierung der Sicherheitsanforderungen an bestimmte Produkte und deren Prüfung.
Schwachstellenanalyse	vulnerability assessment	Gezielte Untersuchung (Auditierung) von Prozessen und Verfahrensabläufen zur Ermittlung von Prozess- und / oder Verfahrensfehlern (Inplausibilitäten, Nonkonformitäten) mit dem Ziel, Prozess- und Verfahrenssicherheit herzustellen.
SE	Security Environment	Sicherheitsumgebung
Secure Hash Algorithm	(SHA-1)	Der Secure Hash Algorithm (SHA-1) [FIPS180-2] ist ein von der US-amerikanischen Sicherheitsbehörde NSA entwickelter <i>Hashalgorithmus</i> , der 160 Bit <i>Hashwerte</i> produziert.
Secure Signature creation Device	(SSCD)	Ein Secure Signature Creation Device ist ein Hardware-Module zum vertrauenswürdigen Erstellen von <i>digitalen Signaturen</i> . Der <i>private Schlüssel</i> für die Erstellung der Signatur befindet sich hierbei innerhalb der Karte. Sämtliche kryptographischen Funktionen werden auf dem SSCD durchgeführt, um so die Integrität des Schlüssels garantieren zu können. Eine <i>SmartCard</i> mit Krypto-Funktionalität ist ein Beispiel für ein SSCD.
Secure Socket Layer	(SSL)	SSL ist ein ursprünglich von Netscape entwickeltes Protokoll zur sicheren Übertragung von Daten, das vor allem für die sichere Übertragung von Webseiten zwischen Web-Server und Browser eingesetzt wird.
Security Management	(SeM)	ITIL-basierter Prozess, der gewährleistet, dass ein angemessener, definierter Grad an Sicherheit für die Informationen und IT-Services erreicht wird. Dazu gehört die Planung, Implementierung und Bewertung von Sicherheitsmaßnahmen zur Erhaltung des Niveaus der IT-Sicherheit, aber auch die angemessene Reaktion auf Sicherheitsverletzungen.
Serveranwendung		Die Serveranwendung ist eine spezielle Form einer <i>Anwendung</i> .
Service Consumer Layer		Schicht der <i>Telematik-Infrastruktur</i> , welche die Primärsysteme der Leistungserbringer umfasst.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Service Continuity Management	(CtM)	ITIL-basierter Prozess, der gewährleistet, das im Anschluss an eine schwerwiegende Unterbrechung der Geschäftsprozesse das vereinbarte Niveau von Mindestanforderungen der IT-Services erbracht wird. Neben der Erstellung und dem Tests von Plänen zur kontrollierten Wiederherstellung der IT-Services nach einer Katastrophe, wird eine Analyse der Bedrohungen und Schwachstellen durchgeführt, um die Auswirkungen einer Katastrophe auf das Gesamtsystem zu begrenzen.
Service Directory Service	(SDS)	Der Service DirectoryService (SDS) registriert alle Dienste und Dienstinstanzen der Telematik- und der Serviceproder-Schicht und ordnet den Instanzen Adressen (URLs) zu, unter denen die Dienste angesprochen werden können. Technische Grundlage für die Implementierung des SDS ist UDDI v3 [UDDI]: der SDS wird als private UDDI Registry mit einem Knoten (Node) implementiert
Service Katalog		Im Service Katalog werden die verfügbaren IT-Services inklusive der möglichen <i>Service Level</i> beschrieben, aus denen ein Nutzer wählen kann.
Service Level Agreement	(SLA)	Vereinbarung über die Qualität von IT-Dienstleistungen, siehe auch SLR
Service Level Management		ITIL-basierter Prozess, der die Qualität der IT-Services fokussiert. Aufgabe ist die Vereinbarung von <i>SLA</i> mit den Nutzern von IT-Services und deren Sicherstellung durch interne Vereinbarungen (<i>OLA</i>) und externe Verträge (<i>UC</i>).
Service Level Requirement	(SLR)	Formalisierte umfassende Beschreibung der Service Anforderungen des Kunden für einen oder mehrere IT-Services. Auf Basis des SLR werden durch das Service Level Management Servicespezifikationen und SLA erstellt. (ITIL-basierter Begriff)
Service Provider Layer		Schicht der <i>Telematik-Infrastruktur</i> , welche die Fachdienste umfasst, in denen Versicherten- und Patientendaten persistent gespeichert werden.
Servicespezifikation	Service Specification Sheet	Detaillierte technische Beschreibung einer Kundenanforderung (<i>SLR</i>), die als Informationsquelle für die Realisierung des IT-Services dient. (ITIL-basierter Begriff)
ServiceTicket		Ein ServiceTicket bezeichnet Berechtigungsinformationen zu einem Service. In einem ServiceTicket sind sowohl die Informationen über die Zugriffsrechte einer Identität auf einen Service als auch mögliche Hybrid-schlüssel für eine zugelassene Identität enthalten.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Servicevereinbarung		Eine Servicevereinbarung (SVB) ist eine Vereinbarung mit einem internen Kunden und enthält Absprachen über die Erbringung von definierten Services. Da es eine firmen- bzw. konzerninterne Vereinbarung ist, entspricht ein SVB in der Regel keinem Vertrag im juristischen Sinne, sondern Dienstleistungsvereinbarungen. Dienstleistungen werden in den Leistungsscheinen definiert und die dazu gehörenden SLAs spezifizieren die Leistungsparameter.
Servicevertrag		Ein Servicevertrag (SVT) ist eine Vereinbarung mit einem externen Kunden und enthält Absprachen über die Erbringung von definierten Services. Da er eine externe Vereinbarung ist, entspricht ein Servicevertrag einem Vertrag im juristischen Sinne sowie Dienstleistungsvereinbarung. Die juristischen Regelungen sind im Rahmenvertrag enthalten. Dienstleistungen werden in den zum Rahmenvertrag gehörenden Leistungsscheinen definiert und die dazu gehörenden SLAs spezifizieren die Leistungsparameter.
SFID	Short EF Identifier	
SGB		Sozialgesetzbuch
SGB V		Sozialgesetzbuch Fünftes Buch
SHA-1	Secure Hash Algorithm	
SICCT	Secure Interoperable ChipCard Terminal	
Sichere Signaturerstellungseinheit	(SSEE)	Eine sichere <i>Signaturerstellungseinheit</i> ist gemäß § 2 Nr. 10 SigG eine <i>Signaturerstellungseinheit</i> , die den anspruchsvollen Anforderungen des Signaturgesetzes, insbesondere § 17 Abs. 1 SigG und § 15 Abs. 1 SigV, genügt.
Sicherheit	Safety Security	Objektiv ist Sicherheit eine Sachlage, bei der das <i>Risiko</i> nicht größer als ein identifiziertes Grenzkrisiko ist. Subjektiv ist Sicherheit das sich immer wieder bestätigende Gefühl von bestimmten negativen Ereignissen nicht getroffen zu werden. Im Deutschen werden darunter die beiden Teilbereiche "Safety" und "Security" gemeinsam beschrieben: Safety ist dem Schutz von Menschen und Sachwerten vor dem Versagen technischer Systeme gewidmet und Security als Schutz von Informationen und Informationsverarbeitung gegen intelligente Angreifer gedacht. Eine Vielzahl sicherheitskritischer Anwendungen zeigt das starke Zusammenwachsen dieser Themenbereiche, die aber trotz allgemeinen Bemühens immer noch weitgehend nebeneinander her bearbeitet werden.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Sicherheits-(grund)funktion	Security Function	Funktion zur Erfüllung der <i>Sicherheitsanforderungen</i> eines IT-Systems, die übergreifende Bedeutung haben. Sie besteht i.d.R. aus mehreren Sicherheitsmechanismen. Eine Sicherheitsgrundfunktion ist z.B. die <i>Vertraulichkeit</i> der Datenübertragung.
Sicherheitsanalyse		Analyse der IT-Sicherheit durch festgeschriebene Methoden
Sicherheitsanforderung	Security/Safety Requirement	Sicherheitsanforderungen legen fest, gegen welche kritischen Bedrohungen eines IT-Systems bzgl. <i>Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität</i> Maßnahmen ergriffen werden müssen. Sicherheitsanforderungen bauen entweder auf funktionalen oder nicht-funktionalen Anforderungen auf und detaillieren ausschließlich deren Sicherheitsrelevanz oder sie beschreiben eigenständige Anforderungen, die nur Sicherheitsaspekte erfüllen. Sie klassifizieren sich in Sicherheitsanforderungen mit und ohne Geheimhaltung.
Sicherheitsaudit	security audit	Befragung der Mitarbeiter eines Unternehmens bzgl. der IT-Sicherheit
Sicherheitsdienst		Sicherheits(grund)funktion
Sicherheitskomponente	Security Component	Eine Sicherheitskomponente dient unmittelbar zur Abdeckung einer oder mehrerer <i>Sicherheits(grund)funktionen</i> . Sie spezifiziert die bereitgestellte Dienstleistung, ohne aber zu beschreiben, wie die Dienstleistung realisiert ist. Die Komponenten werden durch Sicherheitsmechanismen und Sicherheitsobjekte aufgebaut und durch Produkte realisiert.
Sicherheitskonzept		Konzept, das die Sicherheit der Systemkomponenten sowie deren sicheren Betrieb festlegt
Sicherheitsmodell	security modell	Formulierung bestimmter Regeln für die <i>Zugriffskontrolle</i> oder allgemein einer umfassenden <i>Sicherheitspolitik</i> .
Sicherheitspolitik		Grundlegende Aussagen bzgl. der Sicherheit für ein Unternehmen/System
SIG	Signature	Signatur
SigG		Signaturgesetz
Signaturalgorithmus		Ein Signaturalgorithmus ist ein asymmetrischer Kryptoalgorithmus, der zur Erzeugung <i>digitaler Signaturen</i> verwendet wird. Zu den populärsten Signaturalgorithmen zählen <i>RSA, DSA</i> und <i>ECDSA</i> .
Signaturanwendungskomponente		Signaturanwendungskomponenten sind gemäß § 2 Nr. 11 [SigG] Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem Prozess der Erzeugung oder Prüfung <i>qualifizierter elektronischer Signaturen</i> zuzuführen oder <i>qualifizierte elektronische Signaturen</i> zu prüfen oder <i>qualifizierte Zertifikate</i> nachzuprüfen und die Ergebnisse anzuzeigen.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Signaturerstellungseinheit		Eine Signaturerstellungseinheit ist eine Hardware oder Software, in der <i>private Schlüssel</i> , die zur Erstellung von Signaturen erforderlich sind, wie in einem PSE, aufbewahrt und darüber hinaus auch angewandt werden können. Als Signaturerstellungseinheit kommen <i>Smart Cards</i> , <i>HSMs</i> oder Standard-Rechner-Systeme in Frage, wobei der <i>private Schlüssel</i> beispielsweise in einer mittels Passwort verschlüsselter Datei im <i>PKCS #12</i> -Format gespeichert wird. Zur Erstellung von <i>qualifizierten elektronischen Signaturen</i> sind <i>sichere</i> Signaturerstellungseinheiten nötig.
SigV		Signaturverordnung
Simple Network Management Protocol	(SNMP)	Leichtgewichtiges Protokoll für die Steuerung und Status-Abfrage von Netzwerkkomponenten und Servern
Simple Mail Transfer Protocol	(SMTP)	Übertragungsprotokoll für E-Mails
Single Point Of Failure (SPOF)		Nicht redundant ausgelegte technische Komponente bei deren Ausfall ein Dienst nicht mehr verfügbar ist.
SK	Secret Key	<i>geheimer Schlüssel</i>
SL		Stationäre Leistungen
SLA	Service Level Agreement	
SM	Secure Messaging	
SMC	Security Module Card	Sicherheitsmodulkarte
SMK	SM key	SM-Schlüssel
SMTP	Simple Mail Transfer Protocol	
SN	Serial Number	Serien-Nummer
SNMP	Simple Network Management Protocol	
SNMP-Traps		Dezentral initiierte Statusmeldungen, Teil des SNMP
SOAP		Standard für die Kommunikation innerhalb der WEB-Services
SP	Service Provider	
Spec.	specification	<i>Spezifikation</i>
Sperrliste		Eine Sperrliste wird durch eine <i>Zertifizierungsinstanz</i> erstellt und in einem <i>Verzeichnisdienst</i> veröffentlicht. Sie beinhaltet Informationen darüber, welche <i>Zertifikate</i> durch den Zertifikatsinhaber oder andere berechnigte Stellen gesperrt (revoziert) worden sind. Ein weithin akzeptiertes Format für Sperrlisten wurde in <i>X.509</i> spezifiziert und in RFC3280 näher profiliert.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Spezifikation		Eine Spezifikation ist ein technisches Dokument. Sie beschreibt detailliert und formal prüfbar den funktionalen Umfang und die technische Umsetzung eines Gegenstands im Kontext der Einführung der eGK. Sie bildet den Bezugspunkt für Zulassung und <i>Zertifizierung</i> durch die gematik.
SPOF	Single Point Of Failure	
Spoofing		Vortäuschen falscher Identitäten
SSC	Send Sequence Counter	
SSCD	Secure Signature Creation Device	
SSEE		Sichere Signaturerstellungseinheit
SSL	Secure Socket Layer	
Stammdaten	master data	Daten einer Person oder eines Gegenstandes, welche über längere Zeit unverändert bleiben. Bezogen z.B. auf die <i>Versicherten</i> handelt es sich um die Personenstammdaten wie Name, Geburtsdatum und Wohnort. Die Stammdaten sind Teil der <i>Vertragsdaten (VSD)</i> nach §291 a.
Status im Anforderungsmanagement		<p>Ein Prozessschritt im Anforderungsmanagement erhält einen Ergebnistypen in definiertem Status und gibt ihn in einem anderen definierten Status wieder aus.</p> <p>Die Ergebnistypen Anforderung und Anforderung-Dokument-Beziehung werden durch den Prozess anhand der Statusvergabe geführt. Die Anforderung unterliegt den Status „quittiert“, „ZurVorentscheidungVorgelegt“, „offen“, „redundant“, „ZurBewertungAbgegeben“, „Zur EntscheidungVorgelegt“, „akzeptiert/Umsetzung offen“, „komplett umgesetzt“, „abgelehnt“, „zurückgestellt“ und „storniert“.</p> <p>An der Beziehung zwischen Anforderung und Dokument sind folgende Status möglich: „zugeordnet“, „umzusetzen“ und „umgesetzt“. Zwischen den Status der Anforderung und der Anforderung-Dokument-Beziehung bestehen Regelwerke, die die Abhängigkeiten festlegen.</p>
Strategische Risiken	strategic risk	Strategische Risiken sind Gefährdungen der Zielerreichung, die aus den Veränderungen des Umfeldes eines Systems resultieren.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Stratum		Die Nähe einer Server-Zeit zu einer geeichten Normal-Zeit (z.B. Atomuhr o.ä.) wird durch das sog. Stratum ausgedrückt. Der Wert des Stratums ist Null für einen NTP-Server, der seine Zeit direkt mit einer geeichten Quelle synchronisiert. Server, die ihre Zeitinformation direkt von einer Cäsium Atomuhr beziehen, können selbst als Stratum-0-Server fungieren. Der hierarchisch eine Stufe tiefer angeordnete Server, der seine Zeitinformationen vom Stratum 0 Server bezieht bzw. etwa per DCF-77 Funksignal erhält, bezeichnet sich als Stratum 1 Server.
Subscriptio		Herstellungsanweisung für Rezepturen, Beispiel: Salbebeschreibung, die sich aus mehreren Bestandteilen zusammensetzt.
SVA		Sozialversicherungsabkommen (der EU)
SVR		Server
SW		1. Software 2. Status Word
Switch		Verbindet mehrere Geräte in einem LAN
Symmetrischer Schlüssel		Zeichen- oder bit-Folge, die zum Entschlüsseln und Verschlüsseln von Daten verwendet wird. Bei einem symmetrischen (No Suggestions) Schlüssel dient der gleiche Schlüssel sowohl zum Ver- als auch zum Entschlüsseln
System		Die Gesamtheit miteinander verknüpfter und sich gegenseitig beeinflussender Elemente, die entsprechend einem bestimmten Zweck organisiert ist. Das System hat eine gänzlich andere Qualität als die Summe seiner Elemente.
System Management		Zusammenfassung aller Aufgaben, die den operativen Betrieb der IT-Infrastruktur technisch und organisatorisch unterstützen.
T		
Target of Evaluation	(TOE)	<i>Evaluationsgegenstand (EVG)</i>
TBD	To be determined	
TC	1. Trusted Channel 2. Trust Center	1. sicherer Kanal 2. Trust Center
TCP/IP	Transmission Control Protocol/Internet Protocol	herstellerunabhängiges Protokoll zur Übertragung von Daten im Internet oder Intranet.
TCS	Test Case Specification	
TDS	Time Distribution System	

Begriff	Englisch, (Abk.)	Definition (Synonym)
Technology View		Der Technology View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) beschreibt die zur Realisierung des Systems verwendeten Technologien. Dieser Punkt beschreibt die Wahl konkreter Technologien zur Implementierung und Realisierung des Systems.
Teileinlösung		Immer dann, wenn eine <i>Verordnung</i> (Beispiel: Massageverordnung oder Papierrezept) mehrere Einheiten beinhaltet, aber nicht alle Einheiten gleichzeitig eingelöst werden könnten, also nur Teile eingelöst werden, so spricht man von einer Teileinlösung.
Telematik		Telematik ist zusammengesetzt aus den Begriffen Telekommunikation und Informatik. Er beschreibt die Zusammenführung, Verarbeitung und Weitergabe verteilter, u.U. heterogener Datenbestände.
Telematik Layer		Der Telematik Layer ist die verbindet den <i>Service Consumer Layer</i> mit dem <i>Service Provider Layer</i> . Er stellt dazu vermittelnde Netzwerk- und Transportdienste sowie Sicherheitsdienste bereit und steuert die Fachdienste an.
Telematikinfrastruktur	(TI)	Gesamtmenge der technischen Komponenten die zur Realisierung einer integrierten Versorgung der Gesellschaft mit medizinischen Dienstleistungen benötigt werden.
Telematikzulasungsinfrastruktur	(TZI)	dient der Zuteilung von Zertifikaten für von der Gematik freigegebene Komponenten
Terminal API		Schnittstelle für <i>Primärsysteme</i> zum <i>Kartenterminal</i>
Testregion		Eine durch Region, in der Teile der <i>Telematikinfrastruktur</i> vor dem <i>Roll-out</i> in einem kontrollierten Testverfahren getestet werden.
Testumgebung		Infrastruktur, die zum Testen der Komponenten zur Einführung der Gesundheitskarte bereitgestellt wird. Die Testumgebung stellt dafür definierte Werkzeuge und Verfahren sowie die für die Testung erforderliche Plattform bereit (<i>TOP</i>).
TI		<i>Telematikinfrastruktur</i>
Ticket		Bezeichnet ein Objekt mit Berechtigungsinformationen, in welchem sowohl Informationen über die Zugriffsrechte einer Identität als auch mögliche Hybridschlüssel für eine zugelassene Identität enthalten sind. Oberbegriff für Objekt- und Service-Ticket
Tiefenverteidigung	defense in depth	Grundprinzip der IT-Sicherheit, im Speziellen aus der Netzwerksicherheit, bei dem man sich nicht nur auf eine einzige Maßnahme zum Erreichen eines Sicherheitszieles verlässt.
Time Distribution System	(TDS)	Verfahren zur Distribution der amtlichen Deutschen Zeit. Dabei besteht die Möglichkeit, per Modem das TDS der PTB anzuwählen und so ein Zeitsignal zur Uhrsynchronisation zu erhalten. Es ist – wie auch per DCF77 und GPS – geeignet, <i>Stratum 1</i> Server aufzubauen.

Begriff	Englisch, (Abk.)	Definition (Synonym)
TLS	Transport Layer Security	
TLV	Tag Length Value	
TMS	Token Management Service	
To be determined	(TBD)	Noch zu entscheiden
TOE	Target of Evaluation	
TOP		Testorganisations-Plattform
TPM	Trusted Platform Module	
Transmission Control Protocol	(TCP)	Das in RFC793 spezifizierte TCP ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Rechnernetzen, das auch im Internet zum Einsatz kommt.
Transport Layer Security	(TLS)	Nachfolger von SSL
Treuhänder		Natürliche oder auch juristische Person, die im Sinne einer Treuhand tätig wird, also ein Recht für den Treugeber verwaltet und in bestimmten Fällen als Mittelsmann zwischen zwei Vertragsparteien geschaltet wird. In der <i>Telematikinfrastruktur</i> wird ein Treuhänder als vertrauenswürdige Instanz gesehen, welche treuhänderisch die Möglichkeit bietet, den Zugriff zu Daten eines <i>Versicherten</i> zu gewähren, um diesem im Falle eines Zugangs(Schlüssel)Verlusts durch den <i>Versicherten</i> wieder Zugang zu den eigenen Daten zu ermöglichen
Trojaner, Trojansches Pferd		Scheinbar nützliche Software, die durch Anwender installiert wird, aber geheimen Schadcode enthält
Trustcenter		Institution, die <i>Zertifikate</i> im Zusammenhang mit der <i>Digitalen Signatur</i> ausgibt, welche die <i>Identität</i> einer Person oder eines Systems bestätigen (<i>Zertifizierungsstelle</i>).
Trust-Center		Im Umfeld der <i>elektronischen Signatur</i> wird der Begriff „Trust-Center“ häufig als Synonym für die von einem <i>Zertifizierungsdiensteanbieter</i> betriebenen Infrastrukturen verwendet.
Trusted Channel		Siehe virtueller Kanal
Trusted Platform Module	(TPM)	Ein Trusted Platform Module ist ein Chip zur Ausführung von kryptographischen Funktionen sowie zur Speicherung von Schlüsseln. Ein TPM kann mit einer fest eingebauten Smartcard verglichen werden, wobei ein TPM im Gegensatz zur Smartcard fest an ein Gerät gebunden ist.
TrustedService	(TS)	Service der <i>Telematik-Infrastruktur</i> , der für die Umsetzung eines Teils der Sicherheitspolicy zuständig ist
Trusted Viewer		Vertrauenswürdige Anzeige dessen, was signiert werden soll
Trust-service Provider	(TSP)	Organisation, welche einen oder mehrere (elektronische) Trust-services anbietet

Begriff	Englisch, (Abk.)	Definition (Synonym)
Trust-service Status List	(TSL)	Eine Trust-service Status List bietet alle relevanten Informationen zur vertrauenswürdigen Verteilung und Prüfung der Wurzelzertifikate verschiedener "Certifikation Authorities" in Form einer signierten XML-Datei (ETSI-Standard). Hierdurch können auch bereits existierende heterogene PKI's nach einem einheitlichen Schema eingebunden werden.
TS	TrustedService	
TSL	Trust-service Status List	
TSP	Trust-service Provider	
TVS	Ticket Validation Service	
TZI		Telematikzulassungsinfrastruktur
TZP		Telematik-Zugangsprovider
U		
Übergabedokument		Dokumente, die von einem <i>Leistungserbringer</i> zwecks Fortführung der Behandlung einem anderen <i>Leistungserbringer</i> übergeben werden.
UC	Use Case	Anwendungsfall
UDDI	Universal Description, Discovery and Integration	
UDDI Registry		Implementierung des UDDI Standards, siehe auch (<i>UDDI, Universal Description, Discovery and Integration</i>)
UDP	User Datagram Protocol	
UML	Unified Modelling Language	
Umsetzungsanforderung	implementation requirement	Klassifizierung von Anforderung Anforderungen aus dem Umsetzungsprozess in der gematik (nicht entscheidungsrelevant).
Underpinning Contract	(UC)	Ein Underpinning Contract (UC) ist eine Vereinbarung mit einem externen Dienstleister und enthält Absprachen über die Erbringung von definierten Services. Da es eine externe Vereinbarung ist, entspricht ein UC einem Vertrag im juristischen Sinne sowie einer Dienstleistungsvereinbarung. Die juristischen Regelungen sind im Rahmenvertrag enthalten. Dienstleistungen werden in den zum Rahmenvertrag gehörenden Leistungsscheinen definiert und die dazu gehörenden SLAs spezifizieren die Leistungsparameter.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Unified Modelling Language	(UML)	Die Unified Modelling Language (UML) ist eine Sprache zur <i>Spezifikation</i> , Visualisierung, Konstruktion und Dokumentation von Modellen für Softwaresysteme, Geschäftsmodelle und andere Nicht-Softwaresysteme. Sie bietet den Entwicklern die Möglichkeit, den Entwurf und die Entwicklung von Softwaremodellen auf einheitlicher Basis zu diskutieren. Die UML wird seit 1998 als Standard angesehen.
Uniform Resource Identifier	(URI)	Zeichenfolge, die zur Identifizierung einer abstrakten oder physikalischen Ressource dient. Die Struktur der URI ist hierbei im Standard festgelegt
Unit-of-Work		Arbeitseinheit bzw. geschlossenes Arbeitspaket, welches stets vollständig ausgeführt werden muss.
Universal Description, Discovery and Integration	(UDDI)	Standard für einen Verzeichnisdienst, der basierend auf dem SOAP-Protokoll die dynamische Verwaltung von Webservices ermöglicht.
Updates		Umfassendere Aktualisierung von Software
Update Flag Service	(UFS)	Der Update Flag Service (UFS) zeigt an, welche Fachdienste auf die eGK zugreifen möchten. Durch den UFS entfällt der Aufwand, bei jedem Kontakt der eGK mit der Telematikinfrastruktur jeden Fachdienst, der potentiell auf die eGK zugreifen möchte, explizit nach einem Update zu fragen. Der UFS optimiert diesen Ablauf.
UQ	Usage Qualifier	
URI	Uniform Resource Identifier	
URL	Uniform Resource Locator	
Usability		Die Usability eines Produktes ist das Ausmaß, in dem es von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Kontext effektiv, effizient und zufrieden stellend zu erreichen (ISO-Norm 9241). Ins Deutsche ließe sich das Ganze am ehesten mit "Benutzbarkeit", "Bedienungsfreundlichkeit" oder "Ergonomie" übersetzen.
USB	Universal Serial Bus	Standardschnittstellenformat am PC
Use Case		<i>Anwendungsfall</i>
User Datagram Protocol	(UDP)	Auf Transportebene (Schicht 4) neben TCP als zweites Protokoll implementiert. Es garantiert gegenüber TCP keine Ende-zu-Ende Kontrolle. Es setzt auf dem Internet Protocol (IP) auf Schicht 3 auf.
User Help Desk	(UHD)	Annahmestelle für <i>Incidents</i> , die ein Diensteanbieter den Anwendern als zentrale Kontaktstelle bereitstellt.
UTC	Coordinated Universal Time	Koordinierte Weltzeit
UTF8	8-bit Unicode Transformation Format	

Begriff	Englisch, (Abk.)	Definition (Synonym)
UUID		Universal Unique ID
V		
VdAK/AEV		Verband der Angestellten-Krankenkassen e.V./Arbeiter-Ersatzkassen-Verband e.V.
VDAP		Verband deutscher Arztpraxis-Softwarehersteller eV
VDDS		Verband Deutscher Dental-Software Unternehmen
Verbindlichkeit	Liability	Verbindlichkeit bezeichnet den Zustand, in dem die Eigenschaften der <i>Integrität</i> , <i>Authentizität</i> , <i>Nichtabstreitbarkeit (Non-Repudiation)</i> und <i>Zurechenbarkeit</i> gemeinsam erfüllt sind.
Verfügbarkeit	Availability	Verfügbarkeit ist die Fähigkeit, bestimmte Informationen/Dienste in zugesicherter Form und Qualität innerhalb eines definierten Zeitraums am benötigten Ort zu liefern.
Verordner-ID		Eindeutige Identifikationskennnummer eines verordnenden <i>Arztes</i> oder <i>Zahnarztes</i> .
Verordnung	prescription	Leistungsbeschreibung, die von einem approbierten <i>Heilberufler</i> auf ein (elektronisches) Anforderungsformular aufgebracht den Empfänger zur Durchführung der Leistung legitimiert. Beispiel: Papierrezept mit mehreren Verordnungen (z.B. Arzneimitteln) oder elektronische Verordnung.
Verordnungseinlöser		Zugelassener <i>Leistungserbringer</i> , die gemäß § 291a Abs. 4, Satz 1 a-e SGB V/GMG grundsätzlich berechtigt sind, <i>Verordnungsdaten</i> zu lesen und <i>Verordnungen</i> einzulösen. Beispiel: Physiotherapeut, Optiker oder Apotheker. Der Begriff wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.
Verordnungsgeber	(VG)	Zugelassener <i>Leistungserbringer</i> , der berechtigt ist, <i>Verordnungen</i> (und <i>Überweisungen</i>) auszustellen (z.B. <i>Arzt</i> oder <i>Zahnarzt</i>). Der Begriff wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.
Versand-Apotheke		Zugelassene Apotheke, die in der Regel die <i>Papierrezepte</i> oder <i>eRezepte</i> zugesendet bekommt und nach erfolgreicher Prüfung die verordneten Arzneimittel an vom Patienten benannte Lieferadresse versendet.
Verschlüsselung	encoding, encryption	Bei der Verschlüsselung werden Informationen unter Verwendung eines symmetrischen oder <i>asymmetrischen Kryptoalgorithmus</i> mit <i>geheimen bzw. öffentlichen Schlüsseln</i> so codiert, dass die ursprüngliche Nachricht vor unbefugter Einsicht geschützt ist. Der Empfänger der Nachricht kann diese entschlüsseln, um sie wieder lesbar zu machen.
Versicherten-ID		Unveränderbarer und eindeutiger Teil der <i>Krankenversicherungsnummer</i> zur <i>Identifikation</i> des <i>Versicherten</i> .

Begriff	Englisch, (Abk.)	Definition (Synonym)
Versichertenstammdaten (VSD)		Über die Versichertenstammdaten definieren sich Art und Umfang des Versicherungsverhältnisses zwischen <i>Kostenträger</i> und <i>Versichertem</i> . Die VSD sind inhaltlich normiert und von ihrer Struktur für alle <i>Kostenträger</i> einheitlich vorgegeben. Grundlage für den Dateninhalt der VSD sind die bei den <i>Kostenträgern</i> gespeicherten Sozialdaten des <i>Versicherten</i> (§§ 284, 288 SGB V). Die VSD liegen im Verantwortungsbereich des zuständigen <i>Kostenträgers</i> . Dieser ist verantwortlich für die Bereitstellung, kontinuierliche Pflege, bedarfsgerechte Aktualisierung und schließlich Löschung der Daten.
Versicherter		Person, die in einer Vertragsbeziehung zum Krankenversicherer steht. Im Fall einer nicht geschäftsfähigen Person bzw. bei Verhinderung können die Rechte des Versicherten durch einen <i>Bevollmächtigten</i> wahrgenommen werden. Der Begriff wird im Rahmen des Projekts <i>eGK</i> als <i>Akteur</i> verwendet.
Vertragsarztnummer		Eindeutige alphanummerische Nummer für einen <i>Arzt</i> , der an der <i>GKV</i> -Versorgung teilnimmt. Die Nummer wird auf Antrag durch den Zulassungsausschuß der Kassenärztlichen Vereinigung zugeteilt.
Vertragsdaten		Die Daten, die in § 291 SGB V aufgeführt sind. Sie setzen sich zusammen aus Stammdaten und Daten bezogen auf den Krankenversicherer.
Vertrauenswürdig	trust worthy	In der IT-Sicherheit gilt ein System als vertrauenswürdig, wenn es die gesetzten Sicherheitsziele nach dem aktuellen Stand der Technik derart erfüllt, dass ein nicht Erreichen der Schutzziele unmöglich erscheint. Die Vertrauenswürdigkeit repräsentiert das subjektive Empfinden einer Person über den Zustand eines Systems. Die Vertrauenswürdigkeit kann durch Maßnahme wie z.B. einer <i>Zertifizierung</i> von Produkten erhöht werden.
Vertraulichkeit	Confidentiality	Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
Verzeichnisdienst	Directory Service	Ein Verzeichnisdienst ist Bestandteil einer <i>PKI</i> und wird zur Veröffentlichung von <i>Zertifikaten</i> und Zertifikatsstatusinformationen in Form von Sperrlisten oder <i>OCSP</i> -Antworten verwendet. In einem Verzeichnisdienst werden die <i>öffentlichen Schlüssel</i> aller zertifizierten Teilnehmer online zur Verfügung gestellt um die <i>Authentizität</i> des Absenders einer verschlüsselten Nachricht feststellen zu können. <i>OCSP</i> , <i>LDAP</i> und <i>X.500</i> sind die bekanntesten Protokolle für Verzeichnisdienste.
VG		Verordnungsgeber
VhitG		Verband der Hersteller von IT-Lösungen für das Gesundheitswesen
VHK		Verein patientenorientierter Informations- und Kommunikationssysteme

Begriff	Englisch, (Abk.)	Definition (Synonym)
Virtuelles Privates Netz	(VPN)	Bei einem VPN wird unter Verwendung kryptographischer Mechanismen und öffentlicher Transportnetze (z.B. Internet) ein virtuelles privates Netz geschaffen, in dem die Teilnehmer so sicher wie in einem lokalen Netz kommunizieren können.
Virus		Virus eine sich selbst verteilende Software mit meist schädlichen Eigenschaften
VODD		Verordnungsdatendienst
VODM		Verordnungsdatenmanagement
VPN	Virtual Private Network	Virtuelles Privates Netz
VPN-Gateway		siehe VPN Konzentrator
VPN-K		VPN-Konzentrator
VPN-Konzentrator		Sammelpunkt für mehrere VPN-Verbindungen. (Siehe auch VPN)
VS_		Bezeichnung der Use Case Gruppe VS = Versichertenstammdaten
VSD		Versichertenstammdaten
VSDD		Versichertenstammdatendienst
VSDM		Versichertenstammdatenmanagement
W		
WAN	Wide Area Network	
Wert	asset	Allgemein eine Sache mit einem wirtschaftlichen Wert welche von einer Privatperson oder Organisation im Besitz in Cash umgetauscht werden kann. Im Rahmen der IT-Sicherheit sind auch nicht in Geld wandelbare Werte (z.B. Reputation, Persönlichkeitsrechte) davon umfasst.
Wide Area Network	(WAN)	Globales Netzwerk, bei dem der private Entscheidungsbereich des Anwenders verlassen wird, d.h. zur Datenübertragung müssen in der Regel öffentliche Leitungen (bspw. das Kabelnetz der Deutschen Telekom) eingesetzt werden.
Willenserklärung	declaration of intention	Eine Willenserklärung ist eine Äußerung eines auf die Herbeiführung einer Rechtswirkung gerichteten Willens. Sie kann als ausdrückliche Erklärung, durch schlüssiges Handeln oder sogar durch Schweigen kundgetan werden.
Wohnortprinzip	(WOP)	Das in 2002 eingeführte Wohnortprinzip sieht vor, dass Vertrags- und Abrechnungsbeziehungen unmittelbar zwischen einer Krankenkasse und allen KVen bestehen, in deren Bezirk Mitglieder der Krankenkasse wohnen.
WOP		<i>Wohnortprinzip</i>
Workaround		Übergangslösung eines <i>Known Error</i> mit dem Ziel der schnellen Wiederherstellung eines Services. (ITL basierter Begriff)

Begriff	Englisch, (Abk.)	Definition (Synonym)
Wurm		siehe Computerwurm
Wurzel-Zertifizierungsinstanz	Root-CA	Eine Wurzel-Zertifizierungsinstanz (engl. <i>Root-CA</i>) ist eine <i>Zertifizierungsinstanz</i> , deren <i>Zertifikat</i> als vertrauenswürdig gilt.
X		
X.500		X.500 ist eine von der <i>ITU</i> entwickelte Empfehlung für einen (globalen) <i>Verzeichnisdienst</i> , bei dem die Einträge in einem hierarchischen Verzeichnisbaum, dem so genannten „Directory Information Tree (DIT)“, angeordnet sind und durch ihren Distinguished Name adressiert werden. Für den Zugriff auf die Einträge in diesem Verzeichnis ist das in X.519 spezifizierte „Directory Access Protocol (DAP)“ vorgesehen
X.509		Rahmenwerk der ITU-T für standardisierte Zertifikatsformate und die Zertifikatsprüfung in Authentisierungsdiensten
X.509 Directory Service		Ein X.509 Directory Service (Verzeichnisdienst) ist Bestandteil der X.509-PKI und wird zur Veröffentlichung der Zertifikate und Zertifikatsinformationen der X.509-Zertifikate (x.509-ENC und X.509-AUT) verwendet, welche auf der eGK abgelegt sind.
XML	Extensible Markup Language	universelle Datenbeschreibungssprache
XML Digital Signature	(XML-DSig)	Für die <i>digitale Signatur</i> von Daten im <i>XML</i> -Format wurde von einer Arbeitsgruppe des <i>W3C</i> ein spezifisches Signaturformat entwickelt. Im Vergleich zum generischen Signaturformat <i>PKCS #7</i> , mit dem Daten beliebigen Formats signiert werden können.
XML Encryption		Standard des <i>W3C</i> zur Verschlüsselung digitaler Inhalte einschließlich Teilen von <i>XML</i> -Dokumenten und Protokoll-Nachrichten
XML Signature		Standards des <i>W3C</i> zur Verarbeitungsregeln und Syntax von <i>digitalen Signaturen</i> im Kontext von <i>XML</i>
XML-Appliance		Hardware-Modul für die performante Verarbeitung von <i>XML</i> -Daten.
XSD	Extensible Schema Definition	
Z		
Zahlungsbeteiligung		Eine Kostenbeteiligung des Patienten. Sie kann u.a. in einer vollen Kostenübernahme des <i>Patienten</i> unabhängig von einer Kostenerstattung bzw. einer Zuzahlungsverpflichtung gem. § 61 <i>SGB V</i> bestehen.
ZDA		<i>Zertifizierungsdiensteanbieter</i>

Begriff	Englisch, (Abk.)	Definition (Synonym)
Zeitdienst		Er beschreibt ein Verfahren, das basierend auf existenten und weltweit jahrelang erprobten Technologien (<i>NTP</i>) für alle zentralen und dezentralen Komponenten und Systeme der <i>Telematikinfrastruktur</i> im Deutschen Gesundheitswesen, bis hinunter zu den <i>Primärsystemen</i> der <i>Leistungserbringer</i> eine bundesweit einheitliche Systemzeit gewährleistet.
Zeitstempel	time stamp	Digitale Daten, mit denen die Existenz bestimmter Daten vor einem bestimmten Zeitpunkt bewiesen werden kann. Häufig, wie z.B. beim Time Stamp Protocol, werden Zeitstempel unter Einsatz <i>digitaler Signaturen</i> erstellt. Somit sind Zeitstempel elektronische Bescheinigung darüber, dass die mit dem Zeitstempel signierten Daten zum Zeitpunkt der <i>Signatur</i> in der signierten Form vorgelegen haben.
Zeitstempeldienst		Ein Zeitstempeldienst stellt <i>Zeitstempel</i> aus. Oft wird hierbei das in der <i>IETF</i> spezifizierte <i>Time Stamp Protocol</i> verwendet.
Zeitsynchronisation	time synchronization	Verfahren zum Sicherstellen einer einheitlichen Zeitbasis in verteilten <i>Systemen</i> , dass eine maximale Abweichung der verteilten Uhren voneinander sicherstellen soll.
Zertifikat	certificate	Zertifikate sind elektronische Bescheinigungen, die von einer <i>Zertifizierungsinstanz</i> ausgestellt (signiert) werden, mit denen dem Zertifikatsinhaber bestimmte Informationen zugeordnet werden. Hierbei unterscheidet man zwischen <i>Public-Key-Zertifikaten</i> , bei denen dem Zertifikatsinhaber insbesondere ein <i>öffentlicher Schlüssel</i> zugeordnet wird und <i>Attributzertifikaten</i> . Das gebräuchlichste Format für Zertifikate ist X.509v3.
Zertifizierer		Der Zertifizierer bestätigt die Zugehörigkeit eines bestimmten öffentlichen Schlüssels zu einem Nutzer (public key certificate) oder bestimmter Attribute zu einer Identität (attribute certificate)
Zertifizierung	certification process	Die Zertifizierung ist das Ergebnis einer standardisierten Überprüfung von Produkten oder Verfahren auf Übereinstimmung mit einer vorgegebenen <i>Spezifikation</i> . Die Zertifizierung wird durch ein dazu legitimes Institut vorgenommen.
Zertifizierungsdiensteanbieter (ZDA)	Certification Authority (CA)	Ein Zertifizierungsdiensteanbieter ist gemäß § 2 Nr. 8 SigG eine natürliche oder juristische Person, die <i>qualifizierte Zertifikate</i> oder <i>qualifizierte Zeitstempel</i> ausstellt. Ein ZDA muss die Aufnahme des Betriebes bei der <i>BNetzA</i> anzeigen oder sich <i>akkreditieren</i> lassen. Synonym: Trust Center
Zertifizierungsinstanz	Certification Authority (CA)	Eine Zertifizierungsinstanz stellt <i>Zertifikate</i> aus, indem sie die Zertifikatsinhalte mit einer <i>digitalen Signatur</i> versieht. Meist stellt eine Zertifizierungsinstanz auch <i>Sperrlisten</i> aus, die in ähnlicher Art und Weise signiert werden.

Begriff	Englisch, (Abk.)	Definition (Synonym)
Zertifizierungsstelle	Certification Authority (CA)	Der Begriff der Zertifizierungsstelle war in § 2 Abs. 2 SigG97 definiert als eine „natürliche oder juristische Person, die die Zuordnung von <i>öffentlichen Signaturschlüsseln</i> zu natürlichen Personen bescheinigt und dafür eine Genehmigung gemäß § 4 SigG97 besitzt.“ Im Zuge der Überarbeitung des Signaturgesetzes wurde dieser Begriff durch den Begriff des <i>Zertifizierungsdiensteanbieters</i> ersetzt.
ZI		Zentralinstitut für die Kassenärztliche Versorgung
ZIS		Zugangs- und Integrationsschicht
ZPVS		Zahnarztpraxisverwaltungssystem
ZS		Zuzahlungsstatus
Zugangskontrolle	Admission Control	Die Zugangskontrolle soll den unbefugten Zugang zu einem IT-System verhindern und führt hierzu eine <i>Identifikation</i> und eine Überprüfung der angegebenen <i>Identität (Authentifizierung)</i> des <i>Benutzers</i> (Subjekt) durch, bevor der Zugang gewährt wird. Sie umfasst die Verwaltung der Benutzerkennungen (Benutzerverwaltung) und die Rechteprüfung beim Zugangsversuch, einschließlich der Beweissicherung.
Zugriffskontrolle	Access Control	Die Zugriffskontrolle eines IT-Systems soll den unbefugten Zugriff auf Objekte (z.B. Daten, <i>Anwendungen</i>) verhindern. Sie umfasst die Rechteverwaltung, die Rechtezuweisung und die Rechteprüfung beim Zugriffsversuch, einschließlich der Beweissicherung.
Zugriffskontrollverfahren	Access Control Mechanism	Access Control Mechanism sind Verfahren, die Verknüpfung von Zugriffkontrollinformationen effizient abzulegen und zu verwenden, z.B. Access Control Lists, Security Labels, Gruppen, Rollen.
Zurechenbarkeit	Accountability	Accountability bezeichnet den Zustand, in dem alle Handlungen einer Entität eindeutig auf diese Entität zurückzuführen sind.
Zuzahlung		Die gesetzlich vorgeschriebene Kostenbeteiligung eines Versicherten gem. § 61 SGB V.
Zuzahlungsstand		Die Information, in welcher Höhe der <i>Patient</i> bereits <i>Zuzahlungen</i> geleistet hat.
Zuzahlungsstatus		Die Information innerhalb der Vertragsdaten, ob der <i>Patient</i> prinzipiell eine <i>Zuzahlung</i> leisten muss. Der prinzipielle Status kann unterjährig durch einen tatsächlichen Status überlagert werden, bspw. wenn ein <i>Patient</i> aufgrund des Erreichens der Belastungsgrenze für den Rest des Jahres von weiteren <i>Zuzahlungen</i> befreit wird.

Anhang

A1 – Abkürzungen

Technische Abkürzungen sind – soweit verwendet – in der jeweiligen Tabellenzeile erklärt.

Generell werden Abkürzungen in den jeweiligen Ergebnisdokumenten des Projektes erläutert.

A2 - Glossar

Das vorliegende Dokument ist das zentrale Projektglossar.

A3 - Abbildungsverzeichnis

entfällt

A4 - Tabellenverzeichnis

entfällt

A5 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Oestereich]	B. Oestereich (2001): Objektorientierte SW-Entwicklung, Analyse und Design mit der UML, 5. Auflage