gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Glossar der Telematikinfrastruktur

Version:	3.1.0
Revision:	\main\47
Stand:	18.08.2011
Status:	freigegeben
Referenz:	[gemGlossar]
Klassifizierung:	öffentlich

Dokumentinformationen

Änderungen zur Vorversion

Es erfolgte eine Anpassung der Anforderungsdefinitionen.

Die gegenüber der Vorversion vorgenommenen Änderungen wurden farblich hervorgehoben. Bei neuen Begriffen wurde der Begriff hervorgehoben, bei Änderungen in der Begriffsdefinition der erläuternde Text.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
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

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.8.0	06.06.07		Ergänzung InterKom	gematik, IQS
1.8.1	20.08.07		Ergänzungen AG4, Mandantenfähigkeit	gematik, IQS
1.9.0	20.08.07		freigegeben	gematik
1.9.2	28.09.07	3	Ergänzung AM, AG5; allg. Überarbeitung	gematik, IQS
1.9.3	02.11.07		Ergänzung Bereich Betrieb	QM
2.0.0	02.11.07		freigegeben	gematik
2.0.1	20.11.07		Ergänzung „Komponentenzertifikate“	QM
2.0.2	06.12.07	3	Ergänzungen zum Thema Gesamtarchitektur	QM
2.0.3	13.12.07	3/7	Ergänzung AFO-ID	QM
2.0.4	15.01.08	3/63	Ergänzung SM-K, SM-NK, SM-AK	QM
2.1.0	22.01.08		freigegeben	gematik
2.1.1	12.02.08	3	Ergänzungen der Abteilungen/Bereiche TST, ITS/AM und ITS/SI, SPE/FA	QM
2.2.0	15.02.08		freigegeben	gematik
2.2.1	04.04.08	3	Ergänzungen der Abteilungen ITS/AP, SPE/DK, SPE/ZD und SPE/FA	QM
2.2.2	18.04.08	3	Institution, Leistungserbringer, Mandant, Gemeinschaftspraxis, Praxisgemeinschaft	QM
2.3.0	18.04.08		freigegeben	gematik
	03.06.08	3	Umbenennung Trust Service Status List in Trustservice Status List, Abgrenzung CMS/CAMS	QM
	18.06.08	3	Begrifflichkeiten Praxis-PIN, Privat-PIN, Signatur-PIN	QM
	22.07.08	3	Begriffsdefinitionen Zertifikate, PIN Pad, Begriffe aus DaKo, SiKo ergänzen	QM
	12.08.08	3	Einarbeitung Reviewkommentare, Referenzen ergänzt	QM
	24.09.08	3	Begriffe Wirkbetrieb und Testbetrieb ergänzen	QM
2.4.0	25.09.08		freigegeben	gematik
	05.11.08	3	Einfügen der Definition für AMD und AMDD, AMDOK gestrichen	QM
	09.12.08	3	Ergänzen pt, GVD	QM
	17.12.08	3	Einarbeitung von Aktualisierungen, Ergänzung von fehlenden Begriffen	QM
	22.01.09		Einarbeitung der Reviewkommentare, Teilung der Tabelle in Glossar und Abkürzungsverzeichnis	QM
	06.03.09		Ergänzung von Begriffen aus dem Online-Rollout-Projekt (z.B. PoC)	QM
2.5.0	25.03.09		freigegeben	gematik
	02.04.09	3, 4	Anpassung „Stammdaten“, Austausch Abk CCB in	QM

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			CAB	
	08.05.09	3	Anpassung „Provider“	QM
2.6.0	08.05.09		freigegeben	QM
	18.05.09	3	Aufnahme Registrierung	QM
	07.07.09		Einarbeitung zahlreicher Anpassungswünsche	QM
	12.10.09		Anpassung Def. Gesundheitstelematik sowie weiterer Ergänzungen	QM
2.7.0	13.10.09		freigegeben	gematik
	24.11.09 24.02.10		Einarbeitung der Reviewkommentare, weiter Anpassungen QM-intern	QM
2.8.0	02.03.10		freigegeben	gematik
2.8.1	12.03.10		formelle Anpassung	gematik
	06.04.10		Ergänzung Abk.verzeichnis, Glossar	QM
	28.07.10		Übernahme Begriffe aus ehem. Projekglossar	QM
	29.11.10		„Arbeitsplatzkarte“ für SMC-A gemäß [HPC-P3]	QM
	11.01.11		Ergänzung Begriffe aus OrgGlossar	QM
	24.02.11		Übernahme der Glossarbegriffe aus der Lastenheft-phase	QM
3.0.0	01.03.11		freigegeben	gematik
	18.08.11	3	Aktualisierung Definitionen Anforderungsmanagement	QM
3.1.0	18.08.11		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Das vorliegende Glossar enthält die Definitionen und Erläuterungen der Begriffe und Abkürzungen, welche in den Ergebnisdokumenten der Projekte 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 Vorhaben zur Einführung der Gesundheitskarte verwendeten Fachbegriffe.

Ziele des Glossars sind:

- das gemeinsame Verständnis von Fachtermini zu fördern,
- die Verwendung der Fachbegriffe in der Telematikinfrastruktur von möglichen anderen Themenbereichen abzugrenzen und
- eine einheitliche Schreibweise vorzugeben.

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 Grundlagen zu diesem Dokument bilden die Lastenhefte, Fachkonzepte, Facharchitekturen und Spezifikationen der gematik.

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

Im Kapitel 3 sind die Begriffe in der linken Spalte genannt. Der englische Fachbegriff und wesentliche Synonyme sind (wenn vorhanden) in Spalte 2 angeführt. Zu den Begriffen

bestehende Abkürzungen sind in Spalte 2 in Klammern gesetzt. Die Definition eines Begriffes ist in der dritten Spalte eingetragen. Kursiv geschriebene Begriffe in der Definition sind ihrerseits im Glossar definiert.

Im vierten Kapitel, dem Abkürzungsverzeichnis, sind Abkürzungen mit dem zugehörigen Langtext (und evtl. der deutschen Übersetzung) zu finden.

3 Glossar

Begriff	Synonym, (AK)	Definition/Erläuterung
1st Level Support		Erste öffentliche Ansprechpartner im Support.
2nd / 3rd Level Support		Nachgelagerte Supportabteilungen zur Lösung tiefer gehender *Probleme*
3 Key Triple-DES	(3TDES)	Zusätzlich zu 3DES wird für jeden DES-Durchgang ein eigener Schlüssel verwendet.
A		
Ablauf, technischer		Ein technischer Ablauf beschreibt die zu einem *fachlichen Anwendungsfall* gehörenden Interaktionen mit und innerhalb der *Telematikinfrastruktur*.
Ablaufdatum	expiration date, gültig bis	Datum, ab dem eine zugesicherte *Leistung* nicht mehr verfügbar ist.
Abnahme		Mit der Abnahme erklärt der Auftraggeber gegenüber dem Auftragnehmer, dass die vereinbarte *Leistung* (z.B. das Werk zur Erstellung einer *Komponente*) auftragsgemäß erfolgt ist, somit die geschuldete *Leistung* erbracht und der Vertrag erfüllt ist. Abgrenzung zur Zulassung: Die Abnahme grenzt sich von der Zulassung insofern ab, als dass die Abnahmekriterien die vertragliche Erfüllung sicherstellen, wohingegen die Zulassungskriterien einen geeigneten Einsatz im Produktionsumfeld gewährleisten sollen. Daher kann bei einer erfolgreichen Abnahme nicht automatisch von einer erfolgreichen Zulassung ausgegangen werden und die Prüfung der Zulassungskriterien muss in der Regel gesondert erfolgen (und umgekehrt).
Abnahmeprotokoll		Ein Abnahmeprotokoll ist das Ergebnis eines juristisch definierten Vorgangs, bei dem der Auftraggeber die Annahme des Produkts erklärt. Das abgenommene Produkt geht in das Eigentum des Auftraggebers über.
Abnahmetest	acceptance test	Test eines *Produktes*, in dem geprüft wird, ob das *Produkt* die vertraglich festgelegten *Leistungen* erfüllt.
Abstract Syntax Notation One	(ASN.1)	Notation für Datenformate
Access Control Information	(ACI)	ACI bezeichnet Datensätze, in denen Informationen über Zugangsberechtigungen verschiedener *Identitäten* abgelegt sind.

Begriff	Synonym, (AK)	Definition/Erläuterung
Access Rights Instantiation Token	(ARIT)	Das Access Rights Instantiation Token (ARIT) ist ein spezielles eFA-Token (Offline-Token), das genutzt werden kann, um bei Bedarf den Kreis, der für eine spezifische eFA berechtigten Leistungserbringer zu erweitern. Das ARIT ist dabei an eine bestimmte Fachrichtung gebunden. Nur Leistungserbringer dieser Fachrichtung können die mit dem Token assoziierten Rechte instantiieren und somit (je nach Ausgestaltung des Token) temporär oder permanent für den Zugriff auf die Fallakte eines Patienten berechtigt werden. Das ARIT kann als Barcode auf Papier gedruckt (heutiges Modell) oder zukünftig auch direkt auf der eGK des Patienten gespeichert werden.
Access Rule Reference	(ARR)	Verwendung bei der Speicherung von Zugriffsregeln
Accounting		Der Begriff Accounting stammt ursprünglich aus der Betriebswirtschaftslehre und bezeichnet einen Teilbereich des Rechnungswesens. Im Kontext der *Telematikinfrastruktur* bezeichnet Accounting die verbrauchsgerechte Zuordnung der Ressourcennutzung zu einem Vertragspartner und ermöglicht so den Aufbau verschiedenster Geschäftsmodelle.
Administrative Hoheit		Verantwortlichkeit für das zweckorientiert und gesetzeskonforme Funktionieren eines *Systems*
Administrator		Fachpersonal zum Aufbau und Betrieb der *Telematikinfrastruktur* und der vorhandenen *Primär*- und *Backend*-Systeme.
Advanced Encryption Standard	(AES)	Standard für ein symmetrisches Kryptosystem
Akkreditierung	Accreditation	*Prozess* der Überprüfung bzw. Bescheinigung der efolgreichen Überprüfung bzgl. der Erfüllung einer besonderen Eigenschaft. Die Akkreditierung ist gemäß § 2 Nr. 15 des Signatugesetzes ein freiwilliges „Verfahren zur Erteilung einerr Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind.“ Die Akkreditierung von *Telematik*-Services ermöglicht die gegenseitige *Authentisierung* der *Dienste* innerhalb der *Telematikinfrastruktur*.
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	Ein Akteur ist eine gewöhnlich außerhalb des betrachteten bzw. zu realisierenden *Systems* liegende Einheit, die an der in einem *Anwendungsfall* beschriebenen Interaktion mit dem *System* beteiligt ist. Ein Akteur kann ein Mensch sein, z. B. ein *Benutzer*, ebenso aber auch ein anderes technisches *System*. [Oestereich] Akteure können fachlich oder technisch motiviert sein. Fachliche Akteure erfüllen Rollen. Technische Akteure erfüllen Funktionen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Akteur, berechtigter		Als berechtigter *Akteur* in der *Telematikinfrastruktur* werden Personen oder *Systeme* bezeichnet, für die (z.B. in *Tickets*) *Zugriffsrechte* definiert sind.
Akteur, fachlicher		Die in der gematik verwendeten fachlichen *Akteure* sind eindeutig einem Personenkreis nach § 291a SGB V (vgl. [gemSiKo#AnhD,Tab.4]) zugeordnet.
Akteur, technischer		Technische Akteure sind HW-/SW-*Komponenten* der *Telematikinfrastruktur*. Beispiele für technische Akteure sind *Konnektor*, *Broker* oder *Fachdienst VSDD*.
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 *Anwendungsfälle* werden in den *Fachkonzepten* der gematik aus fachlicher Sicht beschrieben. Dabei werden nur diejenigen Aktionen definiert, die von den *Akteuren* in Verbindung mit einem *Informationsobjekt* ausgeführt werden.
Aktualisierungspaket		Ein Aktualisierungspaket enthält Konfigurationsdaten oder Softwarepakete zur Aktualisierung von Komponenten oder Diensten. Aktualisierungspakete werden über Konfigurations- und Software-Repositories bereitgestellt.
Aktualitätsprüfung	currency check	Die von einem autorisierten und authentifizierten *Leistungserbringer* angestoßene Prüfung mit dem Ziel, den *Versicherten* betreffende Daten zu prüfen, ob diese noch aktuell sind oder ggf. zu aktualisieren sind (aktueller *Use Case*: VSD auf der eGK auf Aktualität prüfen).
Ambient Assisted Living		Unter „Ambient Assisted Living" (AAL) werden Konzepte, Produkte und Dienstleistungen verstanden, die neue Technologien und soziales Umfeld miteinander verbinden und verbessern mit dem Ziel, die Lebensqualität für Menschen in allen Lebensabschnitten zu erhöhen. Übersetzen könnte man AAL am besten mit „Altersgerechte Assistenzsysteme für ein gesundes und unabhängiges Leben". Damit wird auch schon skizziert, dass AAL in erster Linie etwas mit dem Individuum in seiner direkten Umwelt zu tun hat.
American National Standards Institute	(ANSI)	Amerikanisches Normungsinstitut, mehrere seiner Standards wurden in internationale Normen übernommen (ANSI-ASCII, DES, X.9.31 (RSA). X9.53 (3DES), X9.62 (ECDSA))
Anbieter	*Betreiber*	Anbieter sind Organisationen, welche die vollständige Verantwortung für Komponenten und Dienste der TI haben und diese bereitstellen. Anbieter können für den operativen Betrieb der verantworteten Komponenten und Dienste der TI einen oder mehrere Betreiber beauftragen. Ein Anbieter kann gleichzeitig auch Betreiber sein.
Anbieterklasse		Ist ein Ordnungsmerkmal, das Anbieter zusammenfasst, die sich in ihrem Verantwortungsumfang gleichen und für die gleiche betriebliche Rahmenbedingungen gelten.

Begriff	Synonym, (AK)	Definition/Erläuterung
Änderungs-anforderung	Change	Eine Änderungsanforderung entsteht als Resultat eines akzeptierten *Änderungsantrages* (Change Request) im Rahmen des Change-Management-Prozesses und verändert den Auftrag (Scopeänderung) oder eine verbindlich abgestimmte Lösung. Änderungsanforderungen sind Ergänzungen der Lastenheftanforderungen. Gemeinsam bilden sie die Gesamtheit aller *Auftragsanforderungen* an ein Projekt/*System*.
Änderungs-antrag	Change Request, Request for Change	Formalisierte Beschreibung eines Änderungsbedarfs zu einem abgestimmten Sachverhalt (Ergebnistypen, *Dienst* oder *Service*). Change Requests unterliegen einem geregelten Bewertungs- und Entscheidungsprozess.
Anforderung	requirement	1.) Sprachgebräuchlich: Maßstab, nach denen jemandes Leistung beurteilt wird 2.) Im IT-Bereich: Eine Anforderung ist eine Aussage über eine zu erfüllende Eigenschaft oder zu erbringende Leistung eines *Produktes*, *Systems* oder *Prozesses*.
Anforderung, funktionale	functional requirement	Eine funktionale Anforderung legt fest, was eine *Komponente* / ein *Dienst* / eine Funktion tun soll. Sie wird beschrieben durch einen Funktionsauslöser, eine erwartete Aktion und ein Ergebnis und definiert damit die Aufgabe: "WAS muss das *Produkt* erfüllen." (Beispiele: Durchführen einer Buchung, Prüfen einer Identität). In den *Spezifikationen* der gematik sollen funktionale Anforderungen durch Modelle gemäß UML-Konvention dargestellt werden.
Anforderung, informative	informative requirements	Eine informative Anforderung wird dem Umsetzenden empfehlend zur Kenntnis gegeben. Informative Anforderungen befinden sich außerhalb der Regelungskompetenz der gematik. Um die Dringlichkeit der Empfehlungen deutlich zu machen, wir trotzdem die RFC-Notation verwendet. Es besteht keine Verpflichtung der Beachtung. (siehe im Gegensatz *normative Anforderung*) Bsp. *Anforderungen* an *Primärsysteme*
Anforderung, nicht-funktionale	non-functional requirement	Eine nicht-funktionale Anforderung definiert die *Benutzerfreundlichkeit* und Leistungsfähigkeit einer *Komponente* / eines *Dienstes* / einer Funktion: "WIE muss das *Produkt* seine Aufgabe erfüllen." (Beispiele: *Benutzerfreundlichkeit*, Leistungsfähigkeit, Wartbarkeit, Effizienz und Wirtschaftlichkeit) und stellt somit eine Erwartungshaltung an die Art der Ausführung dar. Zu den nicht-funktionale Anforderungen gehören üblicherweise auch *Sicherheitsanforderungen*. Wegen der besonderen Bedeutung dieser Anforderungen für die *Anwendungen* zur *elektronischen Gesundheitskarte* werden diese in den Unterlagen der gematik gesondert ausgewiesen.
Anforderung, normative	obligatory requirement	Eine normative Anforderung muss vom Umsetzenden (z.B. Hersteller oder Betreiber) beachtet werden. Dabei ist es irrelevant, ob die *Anforderung* selbst die RFC-Notation MUSS, DARF NICHT, SOLL, SOLL NICHT oder ein KANN enthält. Die Verpflichtung besteht in der Beachtung! (siehe im Gegensatz *informative Anforderung*)

Begriff	Synonym, (AK)	Definition/Erläuterung
Anforderungs-Identifikator	(AFO-ID)	Dient zur Identifizierung von *Anforderungen* im Anforderungsmanagement und wird als Referenzierungsmerkmal verwendet.
Anforderungs-meldung	Demand note, Meldung	Schriftlich formalisierte Darstellung einer Anforderungsidee als ausschließliches Kommunikationsmittel für den Entscheidungs- und Bewertungsprozess von *Anforderungen*. Datenhaushalt: * Anforderungssteller (Name, Organisationseinheit, E-Mail, Telefon) * Erstellungsdatum * Bezug (optional) * Anforderungstext * Anforderungserläuterung (optional) * Dringlichkeit, Zusammenhänge (optional)
Annahme		Rahmenbedingungen, die noch nicht die Qualität einer *Anforderung* haben.
Anonymi-sierung		Anonymisierung gemäß § 3 Abs. 6 BDSG (Bundesdatenschutzgesetz): Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen *Person* zugeordnet werden können.
Anschlussheil-behandlung	(AHB)	AHB ist eine medizinische Rehabilitationsmaßnahme, die im Anschluss an einen Krankenhausaufenthalt durchgeführt wird.
Answer to – Reset	(ATR)	Reihe von Parametern, mit denen die *Chipkarte* dem Chipkartenleser mitteilt, wie diese miteinander kommunizieren können.
Antwortzeit, tolerable		Bezeichnet die Antwortzeit eines Systems, die unter Inkaufname aller akzeptierbaren Einschränkungen im Prozessablauf durch einen Anwender toleriert werden kann. Tolerable Antwortzeit bedeutet, dass 95% der Fälle in dieser Zeit beantwortet werden. Anforderungen zu Leistungen und speziell zu Antwortzeiten gelten für eine Anbindung eines LE mit einem ADSL 1000/128 Anschluss. Bei Bedarf können Anwendungen eigene Werte kontextbezogen festlegen.
Antwortzeit, wünschenswerte		Wünschenswerte Antwortzeit bedeutet, technisch mögliche Antwortzeit unter optimalen Bedingungen. Antwortzeiten gelten für eine Anbindung eines LE mit einem ADSL 1000/128 Anschluss. Bei Bedarf können Anwendungen eigene Werte kontextbezogen festlegen.
Anwender		Ein Anwender ist ein Akteur, der ein an die Telematikinfrastruktur angeschlossenes System nutzt und über dessen Benutzerschnittstellen Anwendungsfälle initiiert.

Begriff	Synonym, (AK)	Definition/Erläuterung
Anwendertest		Anwendertests bilden die zweite *Teststufe* der Testmaßnahmen zur Einführung der *elektronischen Gesundheitskarte*. Begriff aus [RVO2009] Dabei führen Zugriffsberechtigte (d. h. *Leistungserbringer* und ihre Mitarbeiter) praktische Tests mit Testdaten unter Nutzung der von der gematik zur Verfügung gestellten *Musterumgebung* durch. In den Anwendertests sollen in einem ersten Schritt die Prozesse optimiert werden, so dass für die *Feldtests* von einem Mindestmaß an Praxistauglichkeit ausgegangen werden kann.
Anwendung	application, Applikation	*System* (Softwaresystem) zur Unterstützung fachlicher Prozesse. "Anwendung" ist kein Begriff, dem in der Dokumentenlandschaft der Telematik eine über den üblichen Sprachgebrauch hinausgehende Bedeutung zukommt. Durch die Einhaltung der Vorgaben der Telematikinfrastruktur und die Zulassung wird aus einer Anwendung eine Fachanwendung.
Anwendung VSDM		Beinhaltet das dezentrale Fachmodul sowie die Schnittstellen und Kommunikation zu den Fachdiensten und zu den Primärsystemen und beschreibt die Funktionalität des VSDM mit Ausnahme der Fachdienste.
Anwendung, freiwillige		Für den *Versicherten* freiwilliger Einsatzbereich in der Nutzung der eGK. Über den § 291a Abs. 3 Satz 1 SGB V festgelegte freiwillige Anwendungen sind z.B. *elektronische Patientenakte* oder *Arzneimitteldokumentation*.
Anwendungen des Versicherten	(AdV)	*Fachanwendungen* zur Wahrnehmung der Rechte des Versicherten. Die Nutzung dieser *Fachanwendung* ist nur in einer geeigneten und geschützten Umgebung möglich („Umgebung zur Wahrnehmung der Rechte des Versicherten“).
Anwendungsdaten		Anwendungsdaten beinhalten im Gegensatz zu den Nutzdaten sowohl die fachlichen Daten (Payload), als auch die zur Verarbeitung benötigten Protokolldaten (Header, XML-Strukturen, etc.).
Anwendungsfall	*Use Case*	Ein Anwendungsfall (engl. *Use Case*) spezifiziert eine abgeschlossene Menge von Aktionen eines oder mehrerer *Akteure*, die von einem *System* bereitgestellt werden und einen erkennbaren fachlichen Nutzen für einen oder mehrere *Akteure* erbringen. Ein Anwendungsfall beschreibt immer nur genau einen Ablauf oder einen *Prozess*. Dabei sind neben dem Regelprozess (bestehendes oder gewünschtes Verhalten) auch die alternativen Pfade (Fehlerverhalten, Sonderfälle) zu beschreiben. Die beschriebenen Abläufe dürfen jedoch nicht zu komplex werden. In den *Fachkonzepten* der gematik werden rein *fachliche Anwendungsfälle* beschrieben. Zur besseren Abgrenzung von den *fachlichen Anwendungsfällen* wird in den technisch ausgerichteten Dokumenten (*Facharchitekturen*, *Spezifikationen*) der Begriff „*Use Case*“ für die technischen Anwendungsfälle (*Technischer Use Case* = TUC) verwendet.

Begriff	Synonym, (AK)	Definition/Erläuterung
Anwendungs-fall, fachlicher		Ein fachlicher *Anwendungsfall* beschreibt genau einen *Anwendungsfall* mit seinen elementaren Operationen (Interaktion mit *Akteuren*, Entscheidungen etc.) Ein fachlicher *Anwendungsfall* wird durch einen fachlichen *Akteur* initiiert. Fachliche *Anwendungsfälle* beschränken sich auf die Interaktion der fachlichen *Akteure* mit der *Telematikinfrastruktur*.
Anwendungs-gateway		Anwendungsgateways sind Infrastrukturbestandteile, die spezifische Protokollanfragen 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
Anwendungs-klasse		Eine Anwendungsklasse bezeichnet eine Gruppe von Fachanwendungen, die gleiche Eigenschaften besitzen (z.B. schreibt nur Daten auf die Karte, speichert Daten auf anwendungsspezifischen Servern und schreibt auf Karte, speichert Daten ausschließlich auf anwendungsspezifischen Servern) und somit einheitlich geplant und beurteilt werden können.
Anwendungs-konnektor	(AK)	Der Anwendungskonnektor ist derjenige Funktionsblock des *Konnektors*, der die *fachlichen Anwendungsfälle* steuert und die Kommunikation mit den anderen *dezentralen Komponenten*, dem *Primärsystem* des *Leistungserbringers* und den *Diensten* der *zentralen Infrastruktur* auf Anwendungsebene durchführt.
Anwendungs-management-system	application management system, (AMS), Applikation Management System	Ein Anwendungsmanagementsystem betreut *Systeme* und *Anwendungen*, 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 *Kartenmanagements* im Gegensatz zum Begriff *Kartenanwendungsmanagement*.
Anwendungs-prozesse		Darstellung fachlicher Abläufe einer Fachanwendung. Es werden die fachlichen Aktionen der Akteure Ende-zu-Ende dargestellt.
Apothekenverwaltungs-system	(AVS)	*Primärsystem* der Apotheker
Application Identifier	(AID)	Kennung zur Identifikation einer Software
Application Management System	*Anwendungsmanagementsystem,* (AMS)	
Application Programming Interface	(API)	Ein Application Programming Interface ist eine dokmentierte Software-Schnittstelle, mit deren Hilfe ein Software-System bestimmte Funktionen eines anderen Software-Systems nutzen kann.

Begriff	Synonym, (AK)	Definition/Erläuterung
Application Protocol Data Unit	(APDU)	Kommunikationseinheit zwischen *Chipkarte* und *Anwendung* der *Chipkarte*.
Applikation, personenbezogene		Die auf eine Person bezogene Ausprägung einer *Anwendung* nach § 291a SGB V/GMG (z. B. die Arzneimitteldokumentation von Frau Klara Mustermann)
Applikationsform		Darreichungsform eines Fertigarzneimittels oder einer Rezeptur. Eine normative Liste der Benennungen und Abkürzungen ist im [gemFK_VODM] (Beispiel: Tablette, Tab.) enthalten.
Arbeitsgemeinschaften der Testregionen	ARGE	Die Projektbüros der Arbeitsgemeinschaften in den Testregionen haben im Wesentlichen folgende Aufgaben: Abstimmung der Projektarbeiten mit der gematik, technische Betreuung der Musterumgebung, Koordination der laufenden Testarbeiten in der jeweiligen Testregion, die Auszahlung der Pauschalen und Zuschläge an die Leistungserbringer sowie Reporting der Testergebnisse an die gematik. Zudem obliegt es dem Projektbüro, mit kommunikativen und Akzeptanz fördernden Maßnahmen das Gelingen der Testmaßnahmen zu unterstützen.
Architektur	architecture	Eine Architektur beschreibt den prinzipiellen Aufbau eines *Systems*, 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: Enterprise View, Computational View, Information View, Engineering View und Technology View
Arzneimitteldaten	(AMD)	Daten zur Prüfung der *Arzneimitteltherapiesicherheit*
Arzneimitteldatendienst	(AMDD)	Alle Einträge in die Daten zur Prüfung der *Arzneimitteltherapiesicherheit* (AMD) werden auf einem *Fachdienst* (AMDD) gespeichert.
Arzneimitteldokumentation		In die Arzneimitteldokumentation, die im Rahmen der *Fachanwendung* AMTS erhoben, verarbeitet und genutzt wird, werden Medikationsdaten, *Arzneimittelverordnungsdaten* und Therapievorschlagsdaten eingetragen. Diese Einträge bestehen aus Informationen zu einem Arzneimittel und dem Namen, der Adressen und der Telefonnummer dessen, der den jeweiligen Eintrag erstellt hat, um Rückfragen zu ermöglichen.
Arzneimitteltherapiesicherheit	(AMTS)	*Fachanwendung* zur Erhebung, Verarbeitung, und Nutzung der Daten zur Prüfung der Arzneimittelverträglichkeit der Versicherten.
Arzneimittelverordnungsdaten		Die Arzneimittelverordnungsdaten beinhalten Informationen über die vom Arzt ausgestellten *Verordnungen*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Arzneiverordnungsblatt		Rezeptvordruck für die *Verordnung* von bis zu drei verschiedenen Arznei- und Verbandmitteln sowie Hilfsmitteln mit Ausnahme von Seh- und Hörhilfen. Einzelheiten werden von den Parteien der Bundesmantelverträge nach gesetzlichen Vorgaben vereinbart. (z. B. Muster 16)
Arzt	doctor, physician	Ein Arzt ist ein *approbierter Heilberufler*, der einer Ärztekammer angehört. Die hier zu berücksichtigenden Ärzte sind immer einer Institution zuzuordnen (z.B. eigene Praxis, *Gemeinschaftspraxis*, Krankenhaus).
Arztbrief		Signierte papiergebundene oder elektronische Dokumentation eines *Arztes* oder Zahnarztes mit partiell vertraglich vorgegebenen Bestandteilen zu einem Versicherten und dessen Krankheitsgeschehen mit dem Ziel, dass ein anderer *Leistungserbringer* darüber informiert wird. Beispiele: Krankenhausentlassbrief oder Unfallbericht
Arztbrief, elektronischer	(eArztbrief)	Signierte elektronische Dokumentation mit partiell vertraglich vorgegebenen Bestandteilen eines *Arztes* oder Zahnarztes zu einem Versicherten und dessen Krankheitsgeschehen mit dem Ziel, dass ein anderer *Leistungserbringer* darüber informiert wird. Beispiele: Krankenhausentlassbrief oder Unfallbericht. Akronym: eArztbrief.
Asset	Wertgegenstand	Alles, was für die Organisation von Wert ist (ISO:27001). Unter Assets werden *Anwendungen*, aber auch Informationen, die für die Erreichung der Ziele der Organisation von Relevanz sind, verstanden.
Asymmetric Digital Subscriber Line	(ADSL)	Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über eine normale Kupferdraht-Telefonleitung.
Attribut	attribute	Ein Attribut ist ein beschreibendes Merkmal und definiert eine Eigenschaft eines Informationsobjekts. Beispielsweise kann das *Zertifikat* einer *elektronischen Signatur* ein Attribut enthalten, aus dem hervorgeht, dass der Zertifikatsinhaber ein *Arzt* ist.
Attributbestätigungsinstanz		Eine Attributbestätigungsinstanz ist Teil einer PKI und bescheinigt, dass der Antragsteller für ein *Zertifikat* eine bestimmte Eigenschaft besitzt, so dass diese als *Attribut* in das beantragte *Zertifikat* aufgenommen werden kann.
Attributzertifikat	Attribute Certificate	Attributzertifikate stellen die von einer CA signierte Bindung zwischen einem Basiszertifikat und einer bestimmten Eigenschaft des darin bezeichneten Subjekts dar, z. B. die Zugehörigkeit zu einem bestimmten Berufsstand oder eine monetären Beschränkung der Zertifikatsnutzung. Die bestätigte Eigenschaft kann als zusätzliches Feld eines bestehenden Basiszertifikats oder als eigenständiges Attributzertifikat herausgegeben werden. Ein derartiges Attributzertifikat enthält keinen *öffentlichen Schlüssel*, sondern verweist lediglich in eindeutiger Weise auf ein *Public-Key-Zertifikat*. Es wird also verwendet, um dem referenzierten *Public-Key-Zertifikat* weitere *Attribute* zuzuweisen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Audit		Bezeichnet eine Überprüfung von Aufzeichnungen und Aktivitäten um festzustellen, ob bestehende *Richtlinien* und vorgegebene Verfahrensweisen eingehalten werden (z.B. *Sicherheitsaudit*).
Audit Service	AuditS, Auditdienst	Der Audit Service protokolliert versichertenzentriert alle Online-Zugriffe auf die Daten eines Versicherten innerhalb der *Telematikinfrastruktur*. Die Protokollierung erfolgt zu Datenschutzzwecken und zur Wahrung der Rechte des Versicherten und der *Leistungserbringer*. Der Audit Service ist ein *Produkttyp*.
Audit, anlassbezogenes		Anlassbezogene Audits sind außerordentliche Audits, die durch besondere Anforderungen, Vorkommnisse oder Änderungen durch eine dazu berechtigte Institution veranlasst werden können.
Auftragsanforderung	order requirement, initial requirement	Eine Auftragsanforderung geht im Sinne einer Weisung (verbindlich, bewertungsrelevant) oder im Sinne eines Auftrages (unverbindlich, entscheidungs- und bewertungsrelevant) an die gematik.
Ausgangsanforderung	output requirement, (AA)	Aus Sicht eines Ergebnisdokumentes stellen die Anforderungen, die im Ergebnisdokument spezifiziert werden, die Ausgangsanforderungen dar.
Aut idem		Binäres Kennzeichen auf dem Rezeptformular oder im eVerordnungsdatensatz, durch welches der *Arzt* kenntlich macht, dass eine Ersetzung eines Arzneimittels durch ein wirkstoffgleiches zulässig oder ausgeschlossen sein soll.
Authentication Header	(AH)	Bestandteil der IPsec-Protokoll-Suite. AH dient zum Schutz der *Integrität* und der *Authentizität* der IP-Pakete.
Authentication Template	(AT)	Diese dient dazu festgelegte Parameter zur *Authentifizierung* in einer Vorlage zu erfassen. Es gibt hierbei den Typ der firmenintern festgelegten Authentifizierungselemente oder der dynamisch fortschreibbaren Authentifizierungselemente.
Authentifizierung	authentication, (AUT)	Die Authentifizierung bezeichnet den Vorgang, die *Identität* 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 *Identität* geeignet sind.
Authentisierung	authentication, (Auth)	Dies ist ein Verfahren zum Nachweis einer *Identität*. Als Beispiel kann die Passwortabfrage beim Starten eines Rechners genannt werden. Die Authentisierung beantwortet die Frage: Bin ich die Person, die ich vorgebe?

Begriff	Synonym, (AK)	Definition/Erläuterung
Authentizität	authenticity	Authentizität bezeichnet den Zustand, in dem die *Identität* 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 (*Integrität*) 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 *Gesundheitskarte* wird der Begriff insbesondere im Sinne von § 291a, Abs. 5 SGB V/GMG verwendet. So wird mittels der Autorisierung durch den *Patienten* bspw. Definiert, dass ein im Vorfeld authentifizierter *Arzt* (*Authentifizierung*) auf ausgewählte *Informationsobjekte* (Zugriff auf *freiwillige Anwendungen*) ohne Anwesenheit der eGK des Versicherten zugreifen darf [gemFK_AdV#4.4].
Autorisierungsverfahren	authorization mechanism	Verfahren zur Vergabe und Verteilung von *Zugriffsrechten* an eine Person oder ein *System* (Subjekt) auf Daten oder *Anwendungen* (Objekt).
Availability Management	(AvM)	ITIL-basierter Prozess, der die kosteneffektive Bereitstellung von IT-Services auf dem im SLA vereinbarten Verfügbarkeitsniveau gewährleistet. Dazu gehört die strategische Planung der Gewährleistung der *Verfügbarkeit*, aber auch die Überwachung der tatsächlichen *Verfügbarkeit* von IT-Services. Innerhalb der Telematikinfrastruktur handelt es sich um einen Bestandteil des *Performance Managements*.
B		
Backbone		Als Backbone wird ein zentrales Netzwerksegment mit hoher Bandbreite bezeichnet, dessen Aufgabe es üblicherweise ist, mehrere angeschlossene Netzwerke mit einander zu verbinden
Backend-VPN	Backend-Netz, (BE-Netz)	Backbone-Netz der TI auf Basis eines MPLS-VPN. Das Backend-VPN verbindet den *Broker*, *Fachdienste* und die Dienste der *zentralen Infrastruktur* miteinander. Das Backend-VPN ist ein *Produkttyp*.
Basic Encoding Rules	(BER)	Basic Encoding Rules sind Grundregeln für die Kodierung von Daten, die in ASN.1 beschrieben werden.
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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Basisdienste		Querschnittliche Leistungen der TI-Plattform auf logischer Ebene zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Basisdienste werden in der anwendungsunterstützenden Schicht der TI-Plattform angeboten.
Basis-Rollout		Bezeichnet das Projekt zur Implementierung der Grundvoraussetzungen bei den *Leistungserbringern* zum Austausch der KVK gegen die eGK und den Versand der eGK durch die *Kostenträger*.
Basis-TI		Bezeichnung für das Projekt zur Lastenhefterstellung und zur Umsetzung der TI-Plattform.
Basiszertifikat	End Entity Certificate	In einer PKI-Hierarchie an unterster Stelle stehendes *Zertifikat*, welches in der Regel die von einer CA signierte Verknüpfung zwischen einer *Identität* eines Subjekts und einem *öffentlichen Schlüssel* darstellt.
Beauftragung		Sofern keine freiwilligen Hersteller für Komponenten und Dienste der Telematikinfrastruktur zur Verfügung stehen, können diese explizit beauftragt werden. Darüber hinaus sind z.B. Beauftragungen von Prototypen, Betriebs- oder Testleistungen möglich.
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 *Verfügbarkeit*, *Integrität* oder *Vertraulichkeit* 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.
Behandlungs-dokumentation		Die personenbezogenen Daten in den Behandlungsdokumentationen sind in der Verantwortung des zugriffsberechtigten Leistungserbringers und entsprechend den Datenschutz- und Sicherheitsvorgaben des Leistungserbringers für den Umgang mit der Behandlungsdokumentation zu behandeln. Für Leistungserbringer finden der § 203 StGB zur Verletzung von Privatgeheimnissen sowie berufsspezifische Regelungen (z. B. § 9 MBO BÄK) Anwendung. Jeder Patient hat ein Recht auf Einsicht in die Behandlungsdokumentation, ohne dass er ein besonderes Interesse erklären muss. Das Einsichtsrecht erstreckt sich nach der Rechtsprechung und dem ärztlichen Berufsrecht nicht auf den Teil der Dokumentation, der subjektive Eindrücke und Wahrnehmungen des Arztes enthält.
Benutzbarkeit	chance of use	Die Benutzbarkeit eines Produktes definiert sich durch den Erfüllungsgrad aller funktionalen Anforderungen, angelehnt an die Qualitätsmerkmale der DIN 66272.

Begriff	Synonym, (AK)	Definition/Erläuterung
Benutzer	user, Anwender	Wird einer *Identität* das Recht für den Zugriff auf ein oder mehrere *Systeme* beispielsweise durch die Vergabe einer *Rolle* erteilt, so spricht man von einem Benutzer. Einer *Identität* können mehrere Benutzer zugeordnet werden. Ein Benutzer kann mehrere Anmeldenamen besitzen, mit deren Hilfe er sich gegenüber verschiedenen IT-Systemen anmelden kann.
Benutzer-freundlichkeit	ease of use	Die Benutzerfreundlichkeit eines *Produktes* definiert sich durch den Erfüllungsgrad aller *nicht-funktionalen Anforderungen*.
Berechtigter		Natürliche Person, die vom Eigentümer eines Objektes (z.B. Daten, Fachanwendung) berechtigt wurde, das Objekt zu einem definierten Zweck zu nutzen.
Beschaffungs-kosten		Im Kontext der *Gesundheitskarte* können damit Kosten für die Beschaffung von *Telematikinfrastruktur*-Komponenten oder Kosten für die Beschaffung von Arzneimitteln, die nicht über den apothekenüblichen Bezugsweg beschafft werden können, gemeint sein.
Betäubungs-mittel	(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).
Betäubungs-mitteldaten-dienst	(BtMDD)	Auf dem Betäubungsmitteldatendienst werden die Betäubungsmitteldaten gespeichert.
Beteiligter der TI		Die Beteiligten der TI sind alle, die an der Bereitstellung oder dem Betrieb der Telematikinfrastruktur (TI) mitwirken.
Betreiber	Anbieter	Betreiber sind Organisationen, welche die Verantwortung für den operativen Betrieb und die Bereitstellung von Komponenten und Dienste der TI haben. Betreiber werden i.d.R. von Anbietern beauftragt bzw. sind selbst auch Anbieter.
Betreibermodell		Das Betreibermodell ist Bestandteil des übergreifenden Betriebskonzeptes der TI und regelt die Verantwortlichkeiten für den Betrieb der TI und ihrer einzelnen Bestandteile sowie die mögliche Kardinalität von Anbietern für die einzelnen Bestandteile der TI.
Betreibertest-phase		Für alle *Komponenten* und *Dienste*, die bei einem *Provider* betrieben werden, müssen im Rahmen einer Betreibertestphase seitens der *Betreiber* (oder auch *Provider*) Tests zur Betriebsfähigkeit durchgeführt werden.
Betriebsaudit		Durch Betriebsaudits wird geprüft, ob *Betreiber* oder *Provider* von *Diensten* die für den Betrieb des *Dienstes* geschlossenen Vereinbarungen nachhaltig einhalten und ob die Betriebsführung den vereinbarten Ansprüchen gerecht wird. Betriebsaudits beziehen sich meist auf technisch nicht testbare *Anforderungen* an den *Betreiber/Provider*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Betriebsführung		Alle Tätigkeiten und Maßnahmen eines Betreibers zur Aufrechterhaltung der Funktion, Leistung und Sicherheit der von ihm betriebenen Teile der TI.
Betriebskonzept		Konzept, das Festlegungen zum Betrieb der Telematikinfrastruktur trifft. Es werden ein übergreifendes Betriebskonzept der Telematikinfrastruktur sowie nachgelagerte Detailkonzepte erstellt.
Betriebskonzept, übergreifendes		Das übergreifende Betriebskonzept der Telematikinfrastruktur definiert den Betrieb der Telematikinfrastruktur. Es zeigt auf, wie sich die Verantwortlichkeiten und Aufgaben der Betriebsführung auf die verschiedenen Betreiber verteilen und regelt die Betreiber übergreifenden Steuerungsbedarfe. Das Betreibermodell ist Teil des Betriebskonzepts.
Betriebsleitzentrale	(BLZ)	Dienstleister der Industrie im Auftrag der gematik, der seinerseits ebenfalls als *Provider* auftritt.
Betriebsleitzentrale Service		Die Betriebsleitzentrale ist eine durch die gematik beauftragte und in die *Telematikinfrastruktur* integrierte Organisationseinheit. Diese zielt darauf ab, die am operativen Betrieb der TI Beteiligten hinsichtlich der Störungsbearbeitung, Umsetzung von Änderungen und weiteren Serviceleistungen im operativen Geschäft zu unterstützen und zu koordinieren. Die Betriebsleitzentrale nimmt zur Sicherstellung der Betriebsfähigkeit der TI darüber hinaus überwachende, steuernde und qualitätssichernde Aufgaben im Auftrag der gematik wahr. Der Betriebsleitzentrale Service ist ein *Produkttyp*.
Betriebsüberwachung		Alle Tätigkeiten und Maßnahmen, welche die Einhaltung der festgelegten bzw. vereinbarten Funktionen und Leistungen von Teilen oder der gesamten TI kontrollieren, dokumentieren und zusammenfassend berichten.
Betriebsumgebung		Betriebsumgebungen werden für den TI-Betrieb oder zum Entwickeln und Testen von Fachanwendungen sowie Komponenten und Diensten der TI benötigt. Sie bestehen aus Komponenten und Diensten der TI, sind für einen bestimmten Personenkreis vorgesehen und bieten bestimmte Leistungen an, deren Qualität von den fachlichen Anforderungen abhängig ist. Beispiele für Betriebsumgebungen sind die Produktionsumgebung, die Testumgebung oder die Referenzumgebung.
Betriebszeit		Die Betriebszeit definiert die Zeiten in denen die Telematikinfrastruktur durch die Anwender genutzt werden kann.
Betriebszeit, bediente		Die bediente Betriebszeit ist der Teil der Betriebszeit, in dem ein System durch Personal betreut und Support geleistet wird.
Betroffene (im Sinne des BDSG)		Betroffene (im Sinne des BDSG) sind natürliche Personen, über die Einzelangaben zu persönlichen oder sachlichen Verhältnissen (personenbezogene Daten) durch öffentliche oder nicht-öffentliche Stellen erhoben, verarbeitet oder genutzt werden.

Begriff	Synonym, (AK)	Definition/Erläuterung
Bevoll-mächtigter		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). Im Rahmen der Festlegungen zu den Anwendungen der elektronischen Gesundheitskarte wird die Rolle „Berechtigter“ verwendet.
Billing		Billing bezeichnet den Geschäftsprozess der Rechnungslegung. Das Billing umfasst dabei die Arbeitsschritte von der Entgegennahme relevanter Accountingdaten, die Zusammenführung mit den zugehörigen Verträgen des CRM-Systems bis hin zur Erstellung und dem Versand einer Rechnung. Im Sinne der gematik handelt es sich um einen nachgeordneten Prozess des Accountings. Dieser wird durch den Betreiber erbracht und durch die gematik in dieser Phase der Implementierung der TI nicht näher spezifiziert.
Binary Coded Decimal	(BCD)	Binär kodierte Dezimalzahldarstellung, bei der jede Ziffer einzeln durch 4 oder 8 Bit dargestellt wird
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.
BinarySecurity-Token		Ein BinarySecurityToken bezeichnet eine binär abgelegte Datenstruktur innerhalb des Webservice Security Standards. Diese Datenstruktur wird zum Speichern eines Security Tokens wie zum Beispiel eines *X.509*-Zertifikates verwendet und dient dazu, einen Benutzer zu authentifizieren.
Biometrisches Merkmal		Körpermerkmal, anhand dessen ein Mensch durch ein Biometrisches System identifiziert werden kann.
biT4health		Bezeichnung eines der Vorprojekte zur Vorbereitung der Einführung der *Gesundheitskarte*: Bessere IT für bessere Gesundheit
Black-Box-Test	black box test	Bezeichnet eine Methode des Software-Tests, bei der die Tests ohne Kenntnisse über die innere Funktionsweise des zu testenden *Systems* entwickelt werden. Er beschränkt sich auf funktionsorientiertes Testen, d. h. für die Ermittlung der *Testfälle* wird nur die *Spezifikation* (gewünschte Wirkung), aber nicht die *Implementierung* des Testobjekts herangezogen. Die genaue Beschaffenheit des Programms wird nicht betrachtet, sondern vielmehr als Black Box behandelt. Nur nach außen sichtbares Verhalten fließt in den Test ein.
Blattanforderung	base requirement	Eine Blattanforderung definiert vollständig und präzise eine prüfbare Eigenschaft einer *Komponente* oder eines *Dienstes*. Zu einer Blattanforderung hat die gematik konzeptionell keine präzisere oder einschränkende Aussage mehr hinzuzufügen. In der Anforderungskette stellt die Blattanforderung das letzte Glied dar. Eine Blattanforderung wird durch eine *Prüfvorschrift* testbar bzw. auditierbar.

Begriff	Synonym, (AK)	Definition/Erläuterung
Broker		Vermittelnde Infrastrukturkomponente für die Verbindung von dezentralen *Komponenten* und verschiedenen *Fachdiensten*.
Brute-Force-Angriff		Ein Brute-Force-Angriff stellt einen gewaltsamen Angriff auf einen kryptografischen Algorithmus dar. Die Methode kann verwendet werden, um alle möglichen Schlüssel „exhaustiv“, das heißt erschöpfend durchzuprobieren. Man spricht bei dieser vollständigen Schlüsselsuche von einem „Brute-Force-Angriff“ (engl. „brute force attack“) oder auch von der „Exhaustionsmethode“.
Broker Service	(BS)	Der Broker Service integriert einzelne Telematikdienste in komplexere Ablauffolgen, Telematiksequenzen genannt, die vom *Konnektor* aufgerufen werden können. Zur Bereitstellung dieser Telematiksequenzen verwendet der Broker Service die anderen *Dienste* des *Telematik Tiers* (z.B. zwecks Protokollierung, Anonymisierung, usw.) sowie die *Dienste* des *Service Provider Tiers.* Der Broker Service ist ein *Produkttyp*.
BtM-Gebühr		Bearbeitungsgebühr für ein Betäubungsmittelrezept (BtM-Rezept) bzw. eine *eVerordnung* mit gekennzeichneter BtM-Kennung, *BtM-Nummer* und verordnetem *Betäubungsmittel*. Die Gebühr kann in der ausgebenden Apotheke erhoben werden und beträgt zur Zeit 0,26 €.
BtM-Nummer		Eineindeutige numerische 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 einer *eVerordnung* bezeichnet, die sich aus Ausgabedatum, einer Prüfzahl und dem BtM-Merkmal zusammensetzt.
Bundesnetzagentur	(BnetzA)	Vollständige Bezeichnung: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen; eine obere deutsche Bundesbehörde (Regulierungsbehörde). Ihre Aufgaben bestehen aus der Aufrechterhaltung und der Förderung des Wettbewerbs in so genannten Netzmärkten. Die Bundesnetzagentur ist außerdem Wurzelbehörde nach dem Signaturgesetz.
C		
Cache, cachen		Der Cache bezeichnet in der EDV einen schnellen Pufferspeicher, 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 Pufferspeicher laden.

Begriff	Synonym, (AK)	Definition/Erläuterung
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		*Akteur*, der in einem Call-Center an der Bereitstellung von Dienstleistungen mitwirkt.
Call-Center		Organisationseinheit, von der Serviceangebote telefonisch aktiv (outbound) oder passiv (inbound) bereitgestellt werden.
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.
Card Communication Service	(CCS)	Mit den CCS-Operationen kann eine Kommunikation zwischen einem an die *Telematikinfrastruktur* angebundenen *Dienst* und einer *elektronischen Gesundheitskarte* initiiert und durchgeführt werden.
Card Management System	*Kartenmanagementsystem,* (CMS)	*siehe dort*
card to card	(C2C)	Authentifizierungsverfahren zwischen zwei *Chipkarten*
card to server	(C2S)	Authentifizierungsverfahren zwischen einer *Chipkarte* und einem Server
card verifiable	(CV)	Echtheitsprüfung von *Chipkarten*
Card Verifiable Certificate	(CVC)	*Zertifikat* für ein asymmetrisches Verfahren zur gegenseitigen Echtheitsprüfung von systemzugehörigen *Chipkarten*
CA-Zertifikat	Certification Authority Certificate	Ein *Zertifikat*, welches innerhalb einer *PKI* die Organisationsgrenze zwischen verschiedenen (technischen) Herausgabeinstanzen abbildet und aus dem ein Endnutzerzertifikat abgeleitet werden kann. Ein CA-Zertifikat kann auch selbstsigniert sein.
Certificate Policy	(CP)	Eine Certificate Policy besteht aus einer Menge von Regeln, die bei der Ausstellung des *Zertifikates* berücksichtigt wurden. Auf Basis der Certificate Policy kann entschieden werden, ob ein *Zertifikat* für einen bestimmten Einsatzzweck ausreichende Sicherheit bietet. Ein Rahmenwerk für die Entwicklung von Certificate Policies findet sich in [RFC3647].
Certificate Revocation List	(CRL) Zertifikatssperrliste	Der CRL-Provider stellt die Certificate Revocation List zur Verfügung. Die CRL enthält alle gesperrten X.509-Zertifikate. Der CRL-Service ist ein *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Certification Authority	*Zertifizierungsinstanz,* (CA)	*siehe dort*
Challenge Handshake Authentication Protocol	(CHAP)	Authentifizierungsprotokoll, das im Rahmen von PPP eingesetzt wird.
Change Advisory Board	(CAB)	Das Change Advisory Board ist ein Gremium, welches Empfehlungen für die Umsetzung von Änderungen ausspricht. Das CAB besteht aus permanenten und für die jeweilige Änderung vorgeschlagenen Mitgliedern. Es tagt regelmäßig und wird vom Change Manager einberufen.
Change Management	(CM)	Verfahren zur Planung, *Autorisierung*/Freigabe, Steuerung und Kontrolle verändernder Eingriffe in *Anwendungen*, *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 *Requests for Change*.
Change Management Datenbank	(CMDB)	Bezeichnet die in Form einer Datenbank strukturierte elektronische Sammlung von Informationen zu einem System, das kontrollierten Änderungen unterworfen ist. Verzeichnet werden dabei der Bestand und die gegenseitigen Abhängigkeiten der verwalteten Objekte.
Change Request	*Änderungsantrag,* (CR)	*siehe dort*
Change-Kalender / Release-Kalender		Planungsdokument, welches die vorgesehenen Rollouts von Releases und Changes dokumentiert.
Change-Klassifizierung		Change-Klassifizierung bedeutet eine inhaltliche Kategorisierung und eine Priorisierung, d.h. eine Einordnung von Changes nach fachlichem Ziel bzw. dem betroffenen System sowie der Dringlichkeiten bzw. Risiken der Umsetzung (Beispiel: Change des Systems A [Kategorie] mit der Prio 1 [Priorität] zur Beseitigung einer Sicherheitslücke).
Change-Policy		Grundlegende Regeln und Festlegungen zum kontrollierten Einbringen von Änderungen ('Changes') in die Telematikinfrastruktur sowie Benennung der dafür nötigen Verfahren, Prozesse und Systeme.
Change-Typ		Ein Change-Typ gliedert Changes nach ihrem Impact/Umfang, (Beispiele: Security Changes, Notfall-Changes, Minor Changes, Major Changes).
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

Begriff	Synonym, (AK)	Definition/Erläuterung
Chipkarte, multiapplikative		Der Begriff „Multiapplikative Chipkarte“ sagt aus, dass sich auf einer Prozessorchipkarte mehrere *Anwendungen* befinden, zum Beispiel eine Bankkarte mit Telefonfunktion. Diese Anwendungen können vollständig voneinander getrennt verwaltet werden, so dass z.B. ein erlaubter Zugriff auf eine Applikation nicht impliziert, dass auch auf andere Applikationen zugegriffen werden darf.
Cipher Block Chaining	(CBC)	Eine Betriebsart, in der Blockchiffre betrieben werden kann, also ein Algorithmus, der einen Datenblock von gewöhnlich 64 oder 128 Bit mittels eines Schlüsselwerts verschlüsselt (z.B. DES, AES).
Circle of Trust		Der eFA Circle-of-Trust ist ein föderierter Vertrauensraum, in welchem die durch Krankenhäuser oder Dritte betriebenen eFA-Peers unter Einhaltung einheitlicher Standards nachvollziehbar und sicher miteinander kommunizieren können. Das notwendige gegenseitige Vertrauen wird dabei über (vertraglich) bindende Zusicherungen über die Einhaltung festgelegter informationstheoretischen Sicherheitsmaßnahmen hergestellt.
Class of Service	(CoS)	Gruppe von Verfahren zur Priorisierung in TCP/IP-basierten Netzwerken
Client-Application	*Primärsystem*	*siehe dort*
Client-System		Logischer Bezeichner für dezentrale Systeme, die als Clients mit der TI interagieren, aber selbst nicht als Bestandteil der TI betrachtet werden (z. B. PVS-, AVS-, KIS-Systeme, E-Mail-Clients). Mit diesem Bezeichner werden Hard- und Software-Bestandteile zusammengefasst.
Cluster		Ein Cluster ist ein Verbund von Computern, die üblicherweise von außen als ein *System* wahrgenommen werden und somit eine höhere Ausfallsicherheit und/oder bessere *Performanz* ermöglichen.
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 Roll Back, 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 *Zertifizierung* 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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Computational View		Der Computational View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) stellt die Zerlegung einer *Anwendung* in funktionale Module und deren Interaktionsschnittstellen dar. Hier wird ein *System* 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.
Configuration Item	(CI)	Formalisierte Beschreibung einer zum Betrieb erforderlichen *Komponente* über deren gesamten Lebenszyklus hinweg. Cis werden durch das *Configuration Management* 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 Qualität der 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)	Kommunikationsprotokoll für die Zustellung von Ereignissen des *Konnektors* an das *Primärsystem*.
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.
Cross-Zertifikat		Ein Cross-Zertifikat ist ein *Public-Key-Zertifikat*, das eine *Zertifizierungsinstanz* für eine andere *Zertifizierungsinstanz* ausstellt.
Cryptographic Checksum	(CC)	kryptographische Prüfsumme
Customer Relationship Management	(CRM)	Customer Relationship Management, kurz CRM bezeichnet die Dokumentation und Verwaltung von Kundenbeziehungen inklusive der zugehörigen Verträge.
D		
Data Element	Datenelement, (DE)	Ein Datenelement ist im Kontext der Metadaten als eine atomare Dateneinheit definiert.

Begriff	Synonym, (AK)	Definition/Erläuterung
Data Encryption Standard	(DES)	Bezeichnet ein normiertes *Private-Key*-Verfahren (ANSI-Standard X3.92-1981) zur Verschlüsselung von Daten. DES ist zwar weit verbreitet, allerdings aufgrund der geringen Schlüsselgröße von 56 Bit nicht mehr zeitgemäß. *Triple-DES* (3DES) erhöht die Sicherheit des normalen DES-Verfahrens, indem auf einen doppelten Schlüssel (112 Bit) der DES-Algorithmus dreifach durchlaufen wird.
Daten Direkt Verbindung	(DDV)	Form der Festverbindung, sie unterscheidet sich zur Standardfestverbindung (SFV) dadurch, dass sie eine höhere Zuverlässigkeit aufweist und vom Netzbetreiber überwacht wird, so dass dieser im Störungsfall die Schaltung auf eine Ersatzverbindung vornehmen kann.
Daten, medizinische		Medizinische Daten sind im Kontext der eGK ein Synonym für „Klinische Daten“.
Datenautorität	(DA)	Begriff aus der *Telematikinfrastruktur*. Die Datenautorität bezeichnet den *Akteur* innerhalb einer Telematiknachricht, über dessen kryptographische *Identität* der Zugriff auf ein Objekt autorisiert wird.
Datenbearbeiter	(DB)	Begriff aus der *Telematikinfrastruktur*. Der Datenbearbeiter ist der *Akteur* innerhalb einer Telematiknachricht, durch dessen kryptographische *Identität* die Berechtigung auf eine Funktion eines *Fachdienstes* nachgewiesen wird
Daten-eigentümer	(DE)	Der Dateneigentümer ist eine juristische oder natürliche Person. Jedes *medizinische Datenobjekt* besitzt einen Dateneigentümer. Der Dateneigentümer ist der Eigentümer eines Datenobjektes analog zu § 903 BGB. Der Daten-eigentümer ist eine spezielle Form eines Berechtigten für *medizinische Datenobjekte*. Der Zusammenhang zwischen Dateneigentümer und ähnlichen Begriffen ist in der Definition des *medizinischen Datenobjektes* enthalten.
Datenerhalt		Der Datenerhalt bezeichnet die Möglichkeit der Weiternutzung der Daten eines Kartenbesitzers bei Kartenwechsel. Für die eGK ist der Datenerhalt in § 291a SGB V für bestimmte Daten des Versicherten gefordert. Der Begriff des Datenerhalts ist jedoch auch für andere Karten (z.B. HBA) verwendbar.
Datenobjekt, medizinisches	(MDO)	Ein medizinisches Datenobjekt bezeichnet eine zusammengehörige Sammlung von Informationen (wie zum Beispiel eine *eVerordnung*). Jedes medizinische Datenobjekt kann in verschiedenen Darstellungen (z.B. als XML-Datenstruktur) existieren. Jedes medizinische Datenobjekt besitzt genau einen *Dateneigentümer*. Der *Dateneigentümer* kann natürliche oder juristische Personen für den Zugriff auf seine *Daten* berechtigen und sie somit zu *Berechtigten* ernennen.
Datensatz		Bezeichnet eine zusammengefasste Einheit von Datenfeldern. Beispielsweise können die Datenfelder ‚Name‘, ‚Adresse‘ und ‚Geburtsdatum‘ einen Datensatz zu einer Person bilden.

Begriff	Synonym, (AK)	Definition/Erläuterung
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.
Datenschutz-Managementsystem		Teil des gesamten Managementsystems, der die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von Verfahren zur Informationsverarbeitung sicherstellt. (BSI M7.1) Anmerkung: Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation.
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 *Integrität* und der *Verbindlichkeit* 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 *Verfügbarkeit*, der *Integrität* und der *Verbindlichkeit* der Daten ab.
Datenzugriffauditservice	*Audit Service*	Der Datenzugriffsauditservice, im folgenden kurz Audit Service genannt, hat die Aufgabe, Datenzugriffe auf Fachdienste, die zentral über den Broker erfolgen, versichertenzentriert zu protokollieren.
Dauertest		Der Dauertest (im Zusammenhang eines *Leistungstests*) hat zum Ziel, einen Überblick über das Systemverhalten in einem längeren Zeitraum bei steigenden Datenmengen zu gewinnen. Ist das System bis an die Grenze der Kapazitätsauslastung belastet, muss es trotzdem bei der Ausführung von Funktionssequenzen ein normales Verhalten zeigen.
DCF77		DCF77 ist das von der Physikalisch-Technischen Bundesanstalt (http://www.ptb.de) in Mainflingen – südöstlich von Frankfurt – ausgestrahlte Funksignal, das die gesetzlich festgelegte Zeit gemäß Zeitgesetz trägt. Dieses Signal wird insbesondere von *Zertifizierungsdiensteanbietern* genutzt, um die Aktualität der Systemzeit der von Ihnen betriebenen OCSP- und TSP-Respondern zu gewährleisten.
Dead Peer Detection	(DPD)	Methode zur schnellen Erkennung von Verbindungsabbrüchen und somit nicht mehr erreichbaren IPsec-Kommunikationspartnern.
Dedicated File	(DF)	Dateiverzeichnis im Dateisystem einer *Chipkarte*

Begriff	Synonym, (AK)	Definition/Erläuterung
De-Militarized Zone	(DMZ)	DMZ ist ein Netzwerksegment zum Schutz von IT-Systemen, die von öffentlichen Netzen als auch vom internen Unternehmensnetz her zugänglich sind. Die Schutzmechanismen für Angriffe oder unberechtigte Zugriffe erfolgen zur DMZ beidseitig: vom öffentlichen Netz her über die äußere Firewall, zum internen Unternehmensnetz über die innere Firewall. Eine Kommunikation aus der DMZ in das interne Netz ist nicht möglich.
Denial of Service	(DoS)	Der Begriff „Denial of Service (DoS)“ bezeichnet einen Angriff auf einen Host oder *Service* mit dem Ziel einen, oder mehrere *Dienste* durch Überlastung arbeitsunfähig zu machen. Dazu belasten die Angriffe die *Dienste* eines Servers z.B. mit einer derart hohen Anzahl von Anfragen, dass der Server weitere Anfragen nicht mehr oder nur noch mit einer unzureichend langen Antwortzeit (Timeout) verarbeiten kann.
Diagnosis Related Groups	(DRG)	Im Rahmen des ab 2003 eingeführten Fallpauschalensystems zur Vergütung der einzelnen Krankenhausfälle entstandenes ökonomisch-medizinisches Klassifikationssystem basierend auf diagnosebezogenen Fallgruppen.
Dienst		Der Begrifft Dienst ist ein generischer Oberbegriff, der kontextabhängig konkretisiert wird. Er beschreibt eine angebotene Leistung, kann aber auch physikalische und organisatorische Anteile zum Betrieb beinhalten. Aus diesem Grund wird der Begriff Dienst nicht alleinstehend, sondern immer zusammen mit einem erweiternden Begriff verwendet (z. B. Basisdienste, Komponenten und Dienste der TI, Fachdienste).
Dienste der TI-Plattform, zentrale		Ein zentraler Dienst der TI-Plattform stellt die kleinste Entität in der zentralen TI-Plattform mit einer i.d.R. physischen Ausprägung dar, die vollständig durch die TI-Plattform als Black-Box definiert wird, von Herstellern entwickelt und von Betreibern betrieben werden kann. Ein zentraler Dienst der TI-Plattform beinhaltet neben technischen auch alle nötigen organisatorischen Anteile in Kontext des Dienstes. Zentrale Dienste der TI-Plattform setzen anteilig die von der TI-Plattform definierten Schichten Netzwerkdienste, Infrastrukturdienste und Basisdienste um. Hier werden alle zentralen Anteile der TI-Plattform mit adressiert, also auch z.B. zentrale Netzte und Intermediär.
Dienste, anwenderunterstützende		Anwendungsunterstützende Dienste sind generische Plattformleistungen auf Anwendungsebene.
Dienste, fachanwendungsspezifische		Fachanwendungsspezifische Dienste unterliegen der Verantwortung der Fachanwendungen, gehören zur TI und nutzen Basis-, Infrastruktur- und Netzwerkdienste der TI-Plattform. In Stufe 1 definierte anwendungsspezifische Dienste sind Fachdienste und anwendungsspezifische Intermediäre.

Begriff	Synonym, (AK)	Definition/Erläuterung
Dienst-Funktionstest	(DFT)	Testphase im *Diensttest*. Testfokus sind die funktionalen *Anforderungen* eines einzelnen *Dienstes*.
Dienstgüte		Messbare und nachweisbare Qualität eines Dienstes, die sich in mehreren, pro Dienst einzeln festzulegenden Dienstgüteparametern wie z.B. der Verfügbarkeit, Antwortzeit etc. definiert.
Dienst-Interoperabilitätstest	(DIT)	Testphase im *Diensttest*. Testfokus ist das Zusammenspiel mehrerer *Dienste* (ggf. auch mit *Komponenten*). Dabei werden in mehreren Stufen immer größere *Systeme* von integrierten *Diensten* betrachtet.
Dienst-Leistungstest	(DLT)	Testphase im *Diensttest*. Testfokus ist dabei das Leistungsverhalten einzelner *Dienste* bzw. mehrerer *Dienste* im Zusammenspiel. Der DLT kann auch Ausfalltests einzelner *Dienste*/*Komponenten* enthalten.
Dienst-Monitoring- und Servicemanagementtest	(DMT)	Testphase im *Diensttest*. Beim Monitoring- und Servicemanagementtest werden die Schnittstellen für das Monitoring und das Systemmanagement der einzelnen *Dienste* sowie ihr Zusammenspiel mit *Betriebsleitzentrale* und *Leitstand* getestet.
Dienst-Sicherheitsrobustheitstest	(DST)	Testphase im *Diensttest*. Beim Sicherheitsrobustheitstest erfolgen Angriffsversuche, wie diese auch ein realer Angreifer durchführen würde. Dabei wird versucht, konzeptionelle Schwächen und Implementierungsfehler auszunutzen, um so vorhandene Sicherheitsfehler aufzudecken.
Diensttest	(DT)	Beim Diensttest wird das Verhalten eines *Dienstes* in einer konkreten Betriebsumgebung getestet. Er besteht aus den (zum Teil optionalen) Testphasen *Dienst-Funktionstest*, *Dienst-Interoperabilitätstest*, *Dienst-Leistungstest*, *Dienst-Sicherheitsrobustheitstest* und *Dienst-Monitoring- und Systemmanagementtest*.
Differential Fault Analysis	(DFA)	DFA ist ein Angriff auf *Chipkarten* oder Sicherheitsmodule durch Erzeugung von Fehlern bei der *Verschlüsselung*.
Differential Power Analysis	(DPA)	Differential Power Analysis ist ein Angriff auf *Chipkarten* und Sicherheitsmodule durch die Analyse der Leistungs- bzw. Stromaufnahme während einer *Verschlüsselung*.
Digest		Ein Message Digest ist eine kryptographische Einweg-*Hash-Funktion*. Bei einer *Hash-Funktion* geht es allgemein darum, eine lange Eingabe (zum Beispiel einen Text) in eine kurze Ausgabe (den *Hash-Wert* des Textes) zu verwandeln. 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 Chiffrat den Originaltext wieder herzustellen (unumkehrbar). Es soll auch nicht möglich sein, einen Text zu berechnen, der das gleiche Chiffrat wie der Originaltext erzeugt (kollisionsfrei).
Digital Signature Algorithm	(DSA)	Der Digital Signature Algorithm [FIPS186-2] ist ein *Signaturalgorithmus* auf Basis des Diskreten Logarithmus in der multiplikativen Gruppe eines endlichen Körpers.

Begriff	Synonym, (AK)	Definition/Erläuterung
Directory Service	*Verzeichnisdienst*	*siehe dort*
Disease-Management-Programm	(DMP)	Disease-Management-Programme (DMP) werden auch strukturierte Behandlungsprogramme oder einfach Chronikerprogramme genannt. Im Rahmen eines DMP soll eine Krankheit (englisch: Disease) optimal behandelt (gemanaged) werden.
Dispensierdaten		Information über die erbrachte Leistung und den *Leistungserbringer*, die der einlösende *Leistungs-erbringer* der *eVerordnung* hinzufügt.
Distinguished Encoding Rules	(DER)	Die Distinguished Encoding Rules sind eine Untermenge der BER (Basic Encoding Rules) und sind eine Codierung von ASN.1-Datenbeschreibungen, die auf Bit-Ebene völlig eindeutig ist.
Distributed Denial of Service	(DdoS)	Prinzipiell gleiches Verfahren wie bei *DoS*, 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.
Dokumentenlandkarte		In der Dokumentenlandkarte werden die Konzepte und Spezifikationen zusammengeführt, die einen definierten Leistungsumfang mit einem definierten Gültigkeitsstand beschreiben. Die Dokumentenlandkarte ist also das Inhaltsverzeichnis für ein *Release*.
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	Bereichsnamensystem, (DNS)	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 System Security Extensions	(DNSSEC)	Erweiterung von DNS, mit der *Authentizität* und Dateninte-grität von DNS-Transaktionen gewährleistet werden. (Quelle: Wikipedia)
Domain Namespace		*Spezifikation* einer hierarchischen DNS-Baumstruktur, in der jeder Node- und Leaf-Eintrag unterschiedlichen Typen von Informationssätzen beinhaltet.
DTA-Abrechnung		Abrechnung per Datenträgeraustausch zwischen *Arzt* und Kassenärztlicher Vereinigung.

Begriff	Synonym, (AK)	Definition/Erläuterung
Durchsetzungs-einheit	Access Control Enforcement Unit, Policy Enforce-ment Point	Die Durchsetzungseinheit stellt sicher, dass nur berechtigte Zugriffe auf die Zugriffsziele (Ressourcen) erlaubt werden. Die Entscheidung darüber, welche Zugriffe erlaubt sind, trifft die Entscheidungseinheit.
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		
Echtheit eGK/HBA/SMC		Zustand nachdem eine Chipkarte nachgewiesen hat, dass sie den zu ihrem geprüften Zertifikat gehörenden privaten Schlüssel enthält.
Effektivitätstest		Dauer der Ausführung einer spezifizierten Funktion oder Nutzung von Betriebsmitteln durch die spezifizierte Funktion: Verarbeitungsleistung: - Zeitaufwand einer Funktion - Durchsatz von verarbeiteten Daten - Antwortzeit bis reagiert wird - abgearbeitete Funktionsrate - Wartezeit bis Funktion zugänglich ist - Zeitverhalten - Auslastung als Anteil der Zeit Effizienz: Zugriffshäufigkeit und –dauer auf HW und zusätzlicher SW (Dienstleistungsfunktion) für den Funktionsablauf Speichervolumen: Menge, Häufigkeit und Zeitdauer des benutzten Speichers
Eigenanteil		Zuzahlungsteil des Versicherten an den Kosten ärztlicher, zahnärztlicher oder Krankenhausleistung oder eingelöster Arznei- oder Hilfsmittel.
Eignung, funktionale		Für die Prüfung der funktionalen Eignung einer *Komponente*/eines *Dienstes* ist generell der Nachweis der Konformität mit der *Spezifikation* inkl. der Integration und *Interoperabilität* erforderlich. Detaillierte *Anforderungen* an die durchzuführenden Prüfungen werden in den *Prüfvorschriften* geregelt. Die Prüfung einer *Komponente*/eines *Dienstes* gegen die *Spezifikation* zur Feststellung der funktionalen Eignung erfolgt durch das Testlabor der gematik. Geprüft werden neben der funktionalen Eignung auch „nicht-funktionale“ Eigenschaften sowie Aspekte der Sicherheit.
Eignung, materialtechnische		Zur *Zulassung* sind Prüfungen und der Nachweis der elektrischen und physikalischen Eignung erforderlich. Dies können in der Einführungsphase Herstellererklärungen sein und später die Berichte der Prüflabore. Es sind die elektrischen und physikalischen *Anforderungen* der *Spezifikation* in der jeweils zum Antragstellungsdatum gültigen Version zu erfüllen. Einzelheiten hierzu werden in den jeweiligen Prüfvorschriften zur *Komponente* eGK festgelegt.

Begriff	Synonym, (AK)	Definition/Erläuterung
Eignung, sicherheitstechnische		Die IT-sicherheitstechnische Eignung einer Komponente wird durch die BNA / das BSI bzw. durch ein von der BNA / BSI anerkanntes IT-Sicherheitszertifikat einer für das Prüfgebiet IT-Sicherheit akkreditierten Zertifizierungs- sowie ggf. einer Bestätigung einer anerkannten Bestätigungsstelle, nachgewiesen. Dies können in der Einführungsphase Antragsbestätigungen zur Sicherheitsprüfung sein und später die Berichte der Zertifizierungs-/Bestätigungsstellen. Die Anschriften der möglichen Prüfstellen und der Zertifizierungsstellen können abgerufen werden über die Website: http://www.bsi.de/zertifiz/zert/pruefst.htm.
Einboxkonnektor		Die Funktionsblöcke *Anwendungskonnektor* (KONN.AK), *Netzkonnektor* (KONN.NK) und *Signaturanwendungskomponente* (KONN.SAK) sind hier in einer physischen Einheit gebündelt. Diese Ausprägung des *Konnektors* ist für den Betrieb kleiner und mittelgroßer Leistungserbringereinrichtungen ausgelegt und wird durch den *Hersteller* des *Konnektors* als Komplettsystem ausgeliefert. Der Einboxkonnektor ist ein *Produkttyp*.
Eingangsanforderung	input requirement (EA)	Aus Sicht eines Ergebnisdokumentes stellen die Anforderungen, die die Ausarbeitungen im Ergebnisdokument motivieren, die Eingangsanforderungen dar.
Einlösedaten		Einlösedaten (der *eVerordnung*): Teilbereich des Datensatzes *eVerordnung*, der nach Einlösung einer *elektronischen Verordnung* in der Apotheke zu dem Datensatz *eVerordnung* hinzugefügt wird. Dieser Teil enthält z.B. die *Dispensierdaten* und die Signatur des Apothekers.
Einlöser		Zugelassener *Leistungserbringer*, der gemäß § 291a Abs. 4, Satz 1 a-e SGB V/GMG grundsätzlich berechtigt ist, *Verordnungsdaten* zu lesen und *Verordnungen* einzulösen. Beispiel: Physiotherapeut, Optiker oder Apotheker.
Einlösung		Vorgang der Inanspruchnahme einer verordneten Leistung durch einen Patienten.
Einsatzszenario, mobiles		Das mobile Einsatzszenario bezeichnet die Behandlung von Versicherten außerhalb der Arztpraxis. Eine Besonderheit des mobilen Einsatzes ist die räumliche Trennung von *Primärsystem*, *Telematikinfrastruktur-Komponenten* und Behandlungsort. Der Arzt kann wegen des fehlenden *Primärsystems* die Daten vom *Versicherten* nicht sofort und direkt abspeichern.
Einsatzszenario, NFDM		Situation, in der die notfallrelevanten medizinischen Informationen und die Hinweise auf die Willenserklärungen des Patienten ausgelesen werden und ggf. zur Anwendung kommen (Quelle: Arbeitskonzept_BÄK).
Einwilligung	agreement	Schriftlich qualifizierte Zustimmung eines Versicherten z.B. in einen Daten verarbeitenden *Prozess*, wie das Einrichten einer *freiwilligen Anwendung* der eGK (§ 291 a Abs. Satz 3 in Verb. Mit BDSG § 4a).
Einzeltaxe		Preis des Fertigarzneimittels / Rezeptur

Begriff	Synonym, (AK)	Definition/Erläuterung
eKiosk		Umgebung zur Wahrnehmung der Rechte des Versicherten. Mit Hilfe des eKiosk soll der Versicherte zukünftig z.B. *eVerordnungen* verbergen können.
Electrical Erasable Programmable Read Only Memory	(EEPROM)	EEPROM (wörtlich: elektrisch löschbarer, programmierbarer Nur-Lese-Speicher) ist ein nichtflüchtiger, elektronischer Speicherbaustein, der unter anderem in der Computertechnik und dort hauptsächlich in eingebetteten *Systemen* eingesetzt wird.
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 *Spezifikationen* für die Nutzung von XML für elektronische Geschäftsprozesse entwickelt wurde.
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 EDIFACT und ebXML.
Electronic Data Interchange For Administration, Commerce and Transport	(EDIFACT)	EDIFACT ist ein branchenübergreifender internationaler Standard (ISO9735) für den automatisierten Austausch elektronischer Daten im Geschäftsverkehr. Er ist einer von mehreren gebräuchlichen Standards für EDI.
Elementary File	(EF)	Ein Elementary File ist eine Datei innerhalb eines Verzeichnisses auf einer *Chipkarte*. Efs besitzen eine definierte interne Struktur und Zugriffsrechte.
Elliptic Curve Digital Signature Algorithm	(ECDSA)	Der ECDSA ANSI-X9.62 ist ein *Signaturalgorithmus* auf Basis des Diskreten Logarithmus in der Gruppe der Punkte einer elliptischen Kurve über einem endlichen Körper.
Encapsulating Security Payload	(ESP)	Teil der IPsec-Protokoll-Suite
Engineering View		Der Engineering View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) stellt die Verteilung der einzelnen Elemente des *Systems* auf physikalische Ressourcen sowie deren Verbindung dar. Diese Sicht beschreibt die erforderliche Systemunterstützung, um eine Verteilung der Objekte aus dem Computational Viewpoint 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 Systeme.
Enterprise Architect	(EA)	UML-Modellierungstool

Begriff	Synonym, (AK)	Definition/Erläuterung
Enterprise View		Der Enterprise View nach RMODP (Reference Model for Open Distributed Processing nach SAGA [SAGA]) spezifiziert Zielsetzung, Anwendungsbereich, Verfahren und Regeln einer Anwendung. Hier wird die Gesamtumgebung für das *System* und sein Zweck beschrieben. Außerdem werden die *Anforderungen* (Requirements) an das *System*, 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 *Akteure* in ihren Rollen 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 *Entscheidungsinformation* inkl. des Zugriffskontexts.
Entscheidungsinformation	Access Control Decision Information	Die Entscheidungsinformation umfasst den Teil der Autorisierungsinformation, der zum Zugriffszeitpunkt der *Entscheidungseinheit* zur Entscheidung vorgelegt wird.
Entschlüsselung		Vorgang, bei dem unter Verwendung mathematischer Algorithmen und *privater* oder *geheimer Schlüssel* 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 *privaten* oder *geheimen Schlüssels* wieder in die Originalform überführt werden.
Ereignisdienst		Basisanwendung der *Primärsystemschnittstelle* des *Konnektors*, über die Ereignisse des *Konnektors* an das *Primärsystem* übergeben werden können.
Erprobungsphase		Die Erprobungsphase ist ein Teil der Einführungsphase der Telematikinfrastruktur und bietet eine vorgezogene Erprobung des Wirkbetriebs mit eingeschränkter Teilnehmerzahl. Ziel dieser Phase ist es die Betriebseignung unter realen Bedingungen zu prüfen, so dass gravierende Betriebsprobleme bereits vor der Aufnahme des Wirkbetriebs entdeckt und behoben werden können. Die Erprobungsphase erfolgt in der Wirkbetriebsumgebung und sieht echte Smartcards (z.B. eGK/HBA) und Versicherte vor, die nicht als Testteilnehmer zu bezeichnen sind.
Ethernet		Eine nach IEEE standardisierte Technologie, die im LAN und WAN weit verbreitet ist.
Europay Mastercard Visa	(EMV)	Der Begriff leitet sich aus den Anfangsbuchstaben von Europay, MasterCard und Visa ab und steht für einen technischen Sicherheitsstandard, der den weltweiten Zahlungsverkehr sicherer machen soll. EMV betrifft nur Kreditkartenzahlungen, andere Zahlungsarten sind davon nicht betroffen.
European Telecommunication Standards Institute	(ETSI)	Europäisches Telekommunikationsstandardinstitut. Koordinierungsstelle für Kompatibilitätsfragen europäischer Telekommunikationsentwicklungen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Evaluation		Bezeichnet u.a. 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. Die gematik verwendet den Begriff ebenso im Sinne einer *Sicherheitsevaluierung*.
Evaluations-gegenstand	(EVG)	Bei einer Evaluation gemäß ITSEC oder Common Criteria 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.*
Extended Trusted Viewer	(xTV)	Erweiterung der klassischen vertrauenswürdigen Darstellungskomponente (TV) einer SAK um Aufgaben im Rahmen der *Telematikinfrastruktur* wie z.B. Stapel- und *Komfortsignatur* und gesetzlicher *Anforderungen* (bspw. Anzeige des Beginns des Signaturvorganges)
Extensible Markup Language	(XML)	universelle Datenbeschreibungssprache
F		
Fach-anwendung		Die Fachanwendung ist eine Anwendung der TI mit allen nötigen technischen und organisatorischen Anteilen auf Anwendungsebene. Fachanwendungen nutzen die TI-Plattform unter Berücksichtigung der Schnittstellen- und Ablaufdefinitionen und richten sich nach der Nutzungspolicy.
Facharchitektur	(FA)	Konkretisiert das *Fachkonzept* 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	(FD)	Zentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit Anbindung an die zentrale TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform. Fachdienste sind Bestandteil der TI. Sie sind nicht Bestandteil der TI-Plattform.
Fachkonzept	(FK)	Beschreibt vollständig, nachvollziehbar, konsistent und bindend die zu unterstützenden *Anwendungsfälle* aus fachlicher Sicht. Daraus werden *Ausgangsanforderungen* aller Anforderungsklassen abgeleitet, welche durch die zukünftige IT-Unterstüzung im Kontext der Einführung der eGK umzusetzen sind. Das Fachkonzept bezieht sich stets auf einen konkreten Fachausschnitt.
Fachmodul		Ein dezentraler Anwendungsanteil der Fachanwendung innerhalb der TI mit sicherer Anbindung an die TI-Plattform unter Nutzung der Schnittstellen- und Ablaufdefinitionen der TI-Plattform.

Begriff	Synonym, (AK)	Definition/Erläuterung
Fachmodul-Positivliste		Eine Fachmodul-Positivliste ist eine Liste, die festlegt, welche Fachmodule mit den dezentralen Komponenten der TI in der lokalen Umgebung eines Leistungserbringers bzw. Kostenträgers interagieren dürfen.
Fallakte, elektronische	(eFA)	Die elektronische Fallakte ist sowohl eine Spezifikation für einen Dienst zur sektorübergreifenden Kommunikation, als auch eine Bezeichnung für eine Implementierung dieses Dienstes und für eine einzelne diagnosebezogene Akte für einen Patienten innerhalb dieses Dienstes. Die Bedeutungsunterscheidung ergibt sich aber immer klar aus dem Kontext. Die elektronische Fallakte hat eine klare Zweckbindung, einen eindeutig definierten Kreis von Berechtigten und eine festgelegte Laufzeit und kann so mit Einwilligung des Patienten komplett von den behandelnden Ärzten geführt werden.
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.
Fallzahlen		Beschreibt die Anzahl von fachlichen Vorgängen in einem bestimmten Zeitraum, die zur Evaluierung oder Überprüfung von Eigenschaften (z.B. Funktion, Leistung) erhoben wird.
Feldtest		Der Feldtest bildet die 3. und 4. Teststufe der Testmaßnahmen zur Einführung der *elektronischen Gesundheitskarte.* *(*Begriff aus [RVO2009]) In der dritten Teststufe, den 10.000er-Feldtests, führen Zugriffsberechtigte in den *Testregionen* Tests unter realen Einsatzbedingungen durch. Dabei werden Echtdaten der Versicherten und der *Leistungserbringer* verwendet. Bei den Tests sollen bis zu 10.000 Versicherte mitwirken. In der vierten Teststufe, den 100.000er-Feldtests, werden die Tests in ausgewählten *Testregionen* auf bis zu 100.000 Versicherte und die für deren Gesundheitsversorgung Zuständigen erweitert.
File Transfer Protocol	(FTP)	Dateiübertragungsverfahren, ist ein im [RFC 959] von 1985 spezifiziertes Netzwerkprotokoll zur Übertragung von Dateien über TCP/IP-Netzwerke
Filialapotheke		Durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GMG) ist es seit 01.01.2004 möglich, dass Apotheker neben ihrer Hauptapotheke dastere 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: Budgetierung, Kostenrechnung und Leistungsverrechnung.
Firewall		Eine Firewall ist ein *System* aus Hardware und/oder Software, welche den Zugriff zwischen zwei *Systemen* beschränkt und somit ein Regelwerk erzwingt.

Begriff	Synonym, (AK)	Definition/Erläuterung
Firmware		Firmware bezeichnet eine Software, die in einem Speicherchip ablegt für die Grundfunktionalität eines Gerätes verantwortlich ist. Im Auslieferungszustand hat ein Gerät für gewöhnlich eine aktuelle Firmware, je nach Typ werden vom Hersteller im Laufe der Zeit auch Firmware Updates angeboten, die Fehler korrigieren oder neue Funktionen hinzufügen.
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 Softwareentwicklung. Dieses Rahmenwerk schreibt vor, wie bestimmte *Systeme* zu implementieren sind, um *Interoperabilität* zu anderen *Systemen* zu gewährleisten.
Freigabe		Der Begriff Freigabe wird im Sinne einer Zustimmung verwendet. Eine Freigabe beinhaltet keine (auch teilweise) *Zulassung* und wird aus unterschiedlichen Gründen erteilt. So liegt z.B. die *Zulassung* von *Primärsystemen* nicht in der Verantwortung der gematik, deshalb erteilt sie hierfür eine Freigabe. Im Rahmen des Testvorgehens werden Freigaben am Ende einer Testphase ausgesprochen, wenn diese erfolgreich durchlaufen wurde. Diese Freigabe ist Voraussetzung zum Übergang eines Testobjekts in die nachfolgende Testphase.
Frequently Asked Question	(FAQ)	Ein FAQ behandelt eine Verständnisfrage zu einem Thema oder Dokument. Die Beantwortung erläutert die betroffene Festlegung, ohne sie inhaltlich zu verändern.
Friendly-User-Test		Friendly-User-Tests sind Testmaßnahmen mit wenigen, wohlgesonnenen, realen Anwendern, die bereit sind neue Funktionen in ihrer gewohnten Arbeitsumgebung zu verwenden, um deren Eignung im realen Umfeld prüfen zu können.
Frontend-VPN	Frontend-Netz, (FE-Netz)	Backbone-Netz der TI auf Basis eines MPLS-VPN. Das Frontend-VPN verbindet die *Zugangsnetze* mit den zentralen Infrastrukturdiensten und *Brokern*. Das Frontend-Netz ist ein *Produkttyp*.
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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Funktionstest		Beim Funktionstest wird das Testobjekt auf Erfüllung der funktionalen Prüfanforderungen der entsprechenden *Prüfvorschrift* getestet. Ziel ist festzustellen, ob das Testobjekt • über die für spezifizierte Aufgaben erforderlichen Funktionen verfügt, • die richtigen bzw. vereinbarten Ergebnisse/Wirkungen liefert, • die anwendungsspezifischen Normen, Vereinbarungen, gesetzlichen Bestimmungen und ähnliche Vorschriften erfüllt, • unberechtigten Zugriff auf Programme und Daten verhindert, • die Fähigkeit besitzt, ein spezifiziertes Leistungsniveau bei Fehlern oder Nichteinhaltung der spezifizierten Schnittstellen zu bewahren, • die Fähigkeit besitzt, bei einem Versagen das Leistungsniveau wiederherzustellen und direkt betroffene Daten wiederzugewinnen.
G		
Gateway	Protokollumsetzer	Ein Gateway erlaubt es Netzwerken, die auf völlig unterschiedlichen Protokollen basieren, miteinander zu kommunizieren.
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 *Benutzbarkeit* und *Benutzerfreundlichkeit*.
Gegensignatur, mit Inhaltsbestätigung		Gegensignaturen sind Signaturen bereits signierter Dokumente. Dabei muss beachtet werden, dass die Einbindung einer Signatur in ein Dokument eine Fortschreibung des Dokuments nach sich zieht. Jede neue elektronische Signatur bezieht sich dabei auf die vorangegangene Version des Dokuments und schließt dabei bereits erzeugte elektronische Signaturen mit ein.
Gemeinschaftspraxis		Wirtschaftlicher und organisatorischer Zusammenschluss von zwei oder mehreren Personen zur gemeinsamen Ausübung ihrer Berufstätigkeit in gemeinsamen Praxisräumen, repräsentieren also eine *Institution*. (Abgrenzung zu *Praxisgemeinschaft*.)
Gesamtarchitektur		Die Gesamtarchitektur ist ein *Ergebnistyp*. Sie beschreibt die technische Architektur der Telematikinfrastruktur. In ihr werden normative Festlegungen bezüglich der, innerhalb der technischen Architektur anzuwendenden, Standards und Normen getroffen. Siehe auch [gemGesArch].

Begriff	Synonym, (AK)	Definition/Erläuterung
Geschäfts-prozess	Business Process	Ein Geschäftsprozess beschreibt eine Folge von Einzeltätigkeiten, die schrittweise ausgeführt werden, um eine geschäftliches oder betriebliches Ziel zu erreichen. Im Gegensatz zum Projekt kann der Prozess öfter durchlaufen werden. Ein Geschäftsprozess kann Teil eines anderen Geschäftsprozesses sein oder andere Geschäftsprozesse enthalten bzw. diese anstoßen. Geschäftsprozesse gehen oft über Abteilungen und Betriebsgrenzen hinweg und gehören zur Ablauforganisation eines Betriebs.
Gesundheits-anwendung	Health Care Application (HCA)	Datencontainer auf der eGK, der Daten von Fachanwendungen der Telematikinfrastruktur enthält.
Gesundheits-karte, elektronische	(eGK)	Die elektronische Gesundheitskarte ist gemäß § 291a SGB V eine personenbezogene Identifikationskarte, die Versicherte der *Gesetzlichen* (GKV) und der Privaten (PKV) *Krankenversicherung* zur Inanspruchnahme ärztlicher und zahnärztlicher Behandlung gemäß § 15 SGB V berechtigt. Sie enthält gemäß § 291a SGB V Angaben, die für die Übermittlung elektronisch veranlasster ärztlicher *Verordnungen* geeignet sind. Die elektronische Gesundheitskarte ist ein *Produkttyp*.
Gesundheits-telematik	eHealth, Health Telematics	Nach [Haas_2006] handelt es sich bei dem Begriff Gesundheitstelematik um ein „Kunstwort, das sich aus Gesundheitswesen, Telekommunikation und Informatik zusammensetzt. Gemeint sind Aktivitäten, Projekte und Lösungen zur institutionsübergreifenden IT-gestützten Zusammenarbeit von Gesundheitsversorgungsinstitutionen, um Behandlungsprozesse bruchlos (nahtlos) durchführen zu können. Unter dem Begriff „Gesundheitstelematik“ – synonym auch „eHealth“ oder „Health Telematics“ – werden alle *Anwendungen* des integrierten Einsatzes von Informations- und Kommunikationstechnologien im Gesundheitswesen zur Überbrückung von Raum und Zeit subsumiert.“ Gesundheitstelematik beinhaltet die *Telematikinfrastruktur* sowie Infrastrukturen für eine Nachnutzung der TI in weiteren *Anwendungen* im Gesundheitswesen einschließlich der dafür benötigten Betriebsinfrastrukturen. Auch das *Typ2-Netz*, *Mehrwertnetze* und die darüber angeschlossenen *Mehrwertdienste* sind Teil der Gesundheitstelematik.
Grey-Box-Test		Hier werden die Vorteile von *Black Box* und *White Box* kombiniert, um qualitativ bessere Tests zu ermöglichen.
Grundschutz		Erfüllung von Mindestsicherheitsmaßnahmen (z.B. definiert im IT-Grundschutzhandbuch des BSI)
Gültigkeit eGK/HBA/SMC		Die Gültigkeit einer Karte ist Voraussetzung zur Inanspruchnahme von Leistungen oder zur Wahrnehmung von Berechtigungen, die mit dieser verbunden sind. Die Gültigkeit kann eingeschränkt werden durch Sperrung einer Gesundheitsanwendung oder Ablauf oder Sperrung des Authentifizierungszertifikates.
H		

Begriff	Synonym, (AK)	Definition/Erläuterung
Halbleiter-hersteller		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: 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 Sicherheits 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.
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 *Hash-Wert* zu finden (Kollisionsresistenz) und bei einem gegebenen *Hash-Wert* eine Nachricht zu finden, die durch die Hash-Funktion auf den *Hash-Wert* abgebildet wird (Einwegeigenschaft).
Hash-Wert		Ein Hash-Wert ist eine mathematische Prüfsumme, die durch *Anwendung* einer *Hash-Funktion* aus einer elektronischen Nachricht erzeugt wird.
Hauptversicherter		Beitragspflichtiger Versicherungsnehmer einer *Gesetzlichen Krankenversicherung*, dem mehrere nicht beitragspflichtige Familienmitglieder zugeordnet sind.
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 *Heilberufsausweis* (HBA) und entsprechende Berufsausweise.
Heilberufler		Person, die einen Heilberuf ausübt. Der Heilberufler verfügt über einen HBA 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 *Gesundheitskarte* als *Akteur* verwendet.
Heilberufler, approbierter		Eine natürliche Person (*Arzt*, Apotheker, Zahnarzt) mit gültiger Approbation (Zulassung der Ärzte-, Zahnärzte- oder Apothekerkammer), die diese Person berechtigt, entsprechende Heilbehandlungen durchzuführen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Heilberufs-ausweis	*Health Profes-sional Card,* (HBA), (HPC)	Heilberufsausweis ist eine personenbezogene Mikroprozes-sorchipkarte mit kryptographische Funktionen, mit dem sich Angehörige der Heilberufe (z.B. Ärzte und Apotheker) ge-genüber der *Telematikinfrastruktur* ausweisen und vertrau-lich (verschlüsselt) kommunizieren können. Außerdem enthält er eine *qualifizierte elektronische Signa-tur* des entsprechenden *Leistungserbringers*. Der Heilberufsausweis ist ein *Produkttyp*.
Heilberufs-ausweis, elekt-ronischer	(HBA)	Der elektronische Heilberufsausweis ist ein personenbezo-gener Ausweis im Gesundheitswesen, der an Heilberufler ausgegeben wird. Er beinhaltet (neben einer visuellen Ausweisfunktion) die Dienste *Authentifizierung*, *Ver-schlüsselung* sowie *elektronische Signatur* und ermöglicht den Zugriff auf Daten der *elektronischen Gesundheitskarte.*
Heim-PC		Bezeichnung für den privaten Computer eines *Versicher-ten*. Ähnlich wie der *eKiosk* ist grundsätzlich auch der Heim-PC des *Versicherten* ein mögliches *Primärsystem*, sofern dieser u. a. über ein Kartenlesegerät und einen In-ternetanschluss verfügt. Da der Heim-PC als unsicheres *System* anzusehen ist, müssen allerdings vor einer Nut-zung für die eGK insbesondere Sicherheitsaspekte be-rücksichtigt werden.
Hersteller		Hersteller sind für die Entwicklung von Komponenten und Diensten der TI zuständig.
Herstellertest-phase		Der Herstellertest ist die erste Testphase und wird während der Entwicklung einer *Komponente* bzw. eines *Dienstes* von dem Entwicklungs- bzw. Herstellerteam in einer eige-nen Umgebung durchgeführt.
Historical Bytes	(HB)	Die Historical Bytes sind eine Kette von maximal 15 Bytes, deren Inhalt nicht festgelegt ist, innerhalb einer Akti-vierungssequenz für kontaktlose oder kontaktbehaftete *Chipkarten*.
Hybridschlüssel	Hybrid Key	Ein symmetrischer kryptographischer Schlüssel, der durch den *öffentlichen Schlüssel* eines Public-Key-Schlüssel-paares verschlüsselt wurde und somit nur durch den Besit-zer des *privaten Schlüssels* des Schlüsselpaares lesbar ist.
Hypertext Transfer Proto-col	(http)	HTTP ist ein Protokoll zur Übertragung von Daten, das ins-besondere im Rahmen des World Wide Web zum Einsatz kommt und sich meist auf das verbindungsorientierte TCP stützt.
I		
IC Manufacturer	(ICM)	IC-Herstellerkennung
ID des verord-neten 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 PZN haben werden gruppen-weise einer PZN zugewiesen.
Identifier	(ID)	eindeutiger Schlüssel zur *Identifizierung* von Objekten

Begriff	Synonym, (AK)	Definition/Erläuterung
Identifizierung	Identification	Feststellung, ob die personenbezogenen Daten der eGK mit einer natürlichen Person übereinstimmen.
Identität	Identity	Im Kontext des Rechts bezeichnet Identität die Übereinstimmung der personenbezogenen Daten der eGK mit einer natürlichen Person. Diese Identität kann formal durch eine rechtsverbindliche Identitätsfeststellung, Vergleich von festgelegten Kriterien, bestimmt werden.
Identitätsüberprüfung	*Authentifizierung*	Unter Identitätsüberprüfung wird der *Prozess* der Überprüfung einer behaupteten *Identität* einer natürlichen Person anhand eines oder mehrerer eindeutiger Identifizierungsmerkmale verstanden. Im Kontext der eGK findet diese Identitätsüberprüfung bei der Inanspruchnahme von Maßnahmen eines *Leistungserbringers* statt.
Implementierung		Eine Implementierung ist die Umsetzung von festgelegten Strukturen und (Arbeits-)Abläufen in einem System unter Berücksichtigung von Rahmenbedingungen, Regeln und Zielvorgaben, also einer Spezifikation. Im allgemeinen Fall stellt die Konkretisierung einen Wechsel von einer abstrakten zu einer konkreteren Ebene dar – die Implementierung steht dabei für die tiefste Ebene. Im Kontext der Gesundheitskarte entspricht dies z.B. dem Prozess zur Einrichtung der dezentralen Komponenten (Primärsystem, Kartenterminal, Konnektor) und ihre Anbindung an die Telematikinfrastruktur.
Incident		Ereignis, das zu einer qualifizierten und formalisierten Meldung einer Störung, Anfrage oder eines Auftrages führt.
Incident Management	(IM)	ITIL-basierter Prozess, dessen Aktivitäten neben der Registrierung, Kategorisierung, Priorisierung und Verfolgung auch die Analyse und Diagnose und vor allem die Behebung und Wiederherstellung der *Services* sind. Die primäre Zielsetzung ist eine schnellstmögliche Wiederherstellung der *Services*.
Information Technology Security Evaluation Criteria	(ITSEC)	ITSEC ist ein europäischer Standard für die Prüfung und *Zertifizierung* von *Produkten* und *Systemen* im Hinblick auf ihre *Vertrauenswürdigkeit*. 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 *Vertrauenswürdigkeit*.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 ist ein konzeptionelles statisches Datenmodell. Es enthält alle in den fachlichen *Anwendungsfällen* benötigten *Informationsobjekte* und deren Beziehung zueinander. (z.B. die der *Versichertenstammdaten* auf der Grundlage des § 291 Abs. 2 SGB V)
Informationsobjekt		Logisches Element des *Informationsmodells*. Für das Informationsobjekt sind *Anforderungen* festgelegt wie z.B. Sicherheitsziele, welche wiederum nach bestimmten (Sicherheits-)Eigenschaften die Informationsobjekte der verarbeitenden *Komponenten* verlangen.
Informationssicherheit	IT-Security	Die Informationssicherheit schafft auf der Ebene der Informationstechnik (*Anwendungen*, *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 *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* von Informationen/Daten, z. B. nach ISO/IEC 17799, IT-Grundschutzhandbuch, ISO/IEC TR 13335, CobiT, The Standard usw.
Informationssicherheitsmanagementsystem		Der Teil des gesamten Managementsystems, der auf der Basis eines Geschäftsrisikoansatzes die Entwicklung, Implementierung, Durchführung, Überwachung, Überprüfung, Instandhaltung und Verbesserung der Informationssicherheit abdeckt. Anmerkung: Das Managementsystem enthält die Struktur, Grundsätze, Planungsaktivitäten, Verantwortung, Praktiken, Verfahren, Prozesse und Ressourcen der Organisation. (ISO/EN 27001)
Infrastruktur		*System* von Einrichtungen, Ausrüstungen und Dienstleistungen, welches für den Betrieb einer Organisation erforderlich ist.
Infrastruktur, zentrale		Die zentrale Infrastruktur beinhaltet die *Dienste* der *Telematik Tier* zentral. Diese können unterteilt werden, in die Basisservices DNS, NTP und PKI, welche über das *Frontend-* und *Backend-VPN* zur Verfügung stehen, und die Services *Broker*, *Audit* und *SDS*.
Infrastrukturdienste		Querschnittliche Leistungen der TI-Plattform auf logischer Ebene zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Infrastrukturdienste werden in der Infrastrukturschicht der TI-Plattform angeboten.

Begriff	Synonym, (AK)	Definition/Erläuterung
Installation		Funktionsfähige Bereitstellung von Hardware und Software in einer definierten Umgebung.
Instanz		Als Instanz wird jeweils eine konkrete Realisierung einer abstrakten Kategorie verstanden. In der TI verwendet man den Begriff für die Instanzen von *Komponenten* (z.B. ein konkretes *Kartenterminal* im Gegensatz zum abstrakten Begriff) oder bei der Modellierung der *Daten* (die *Notfalldaten* eines konkreten Versicherten zu einem Zeitpunkt als Instanz der Datenklasse „*Notfalldaten*“).
Instanz, betriebsführende	*Betreiber*	*siehe dort*
Instanz, testverantwortliche und -koordinierende		Die testverantwortliche Instanz erfüllt den gesetzlichen Testauftrag hinsichtlich § 291b SGB V, hat die zentrale Ergebnisverantwortung für alle Testmaßnahmen und regelt diese durch eine übergreifende Testkoordination der Testinstanzen. Zu diesem Zweck definiert die testverantwortliche Instanz die zu leistenden Testmaßnahmen und bestimmt die Rahmenbedingungen zum Ablauf und der Qualität der Testmaßnahmen. Die testverantwortliche Instanz hat als Schwerpunkt die regulären Aufgaben im Rahmen von Zulassungstests wahrzunehmen, als auch die Unterstützung zum Aufbau und der Fortführung der TI und ihrer Dienste. Weitere Details zu den Aufgaben der testverantwortlichen Instanz liefert das Test & Migrationskonzept.
Institution, medizinische		In der *Telematikinfrastruktur* handelt es sich bei der Institution des *Leistungserbringers* um eine Einrichtung in der *Gesundheitstelematik*, die an der Versorgung der *Versicherten* teilnimmt, wie zum Beispiel eine Arztpraxis, Krankenhaus oder eine Apotheke.
Institutionsidentität		Die Institutionsidentität ist eine durch eine *SMC-B* repräsentierte *Identität* der Institution des *Leistungserbringers* bzw. einer Organisationseinheit in einer solchen Institution. Beispiele für solche Organisationseinheiten sind einzelne Arztpraxen innerhalb einer *Praxisgemeinschaft*.
Institutionskarte	Security Module Card Typ B	Die Institutionskarte entspricht technisch weitgehend dem *Heilberufsausweis* (HBA), bezieht sich jedoch auf eine organisatorische Instanz des Gesundheitswesens (z.B. Praxis, Apotheke, Krankenhaus). Die Institutionskarte wird auch als *Security Module Card Typ B* (SMC-B) bezeichnet. Die *SMC-B* kann durch einen *HBA* oder aber die Eingabe ein PIN freigeschaltet und kann dann für 24 h verwendet werden bevor eine erneute Freischaltung notwendig ist.
Institutionskennzeichen	(IK)	Das Institutionskennzeichen ist ein eindeutiges Merkmal für die *Identifizierung* von *Kostenträgern* und bestimmten *Leistungserbringern* (z.B. Apotheken)
Integrated Circuit Card	(ICC)	Oft auch als *Chipkarten* oder Smartcard bezeichnet, sind spezielle Plastikkarten mit eingebautem, integriertem Schaltkreis (Chip), der eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthält.

Begriff	Synonym, (AK)	Definition/Erläuterung
Integrated Circuit Card Serial Number	(ICCSN)	Die ICCSN ist eine eindeutige Identifikationsnummer (Seriennummer) einer Smartcard.
Integrated Services Digital Network	(ISDN)	Integrated Services Digital Network (ISDN) ist ein internationaler Standard für ein digitales Telekommunikationsnetz.
Integrationstest		Nachweis der funktionalen und technischen Eigenschaften des Gesamtsystems oder von Teilsystemen. Ziel des Integrationstests ist die Identifikation von Fehlern in der Interaktion zwischen *Komponenten und Diensten*, die durch die reine Prüfung der Spezifikationskonformität nicht nachgewiesen werden können. Das Hauptaugenmerk liegt hier auf den Schnittstellenformaten und dem Datenaustausch. Folgende Fehlerzustände werden unterschieden: 1. Eine *Komponente* sendet keine oder syntaktisch falsche Daten, so dass die empfangende *Komponente* diese nicht korrekt verarbeiten kann (funktionaler Fehler, inkompatible Schnittstelle). 2. Die übertragenen Daten zwischen *Komponenten* werden unterschiedlich interpretiert (funktionaler Fehler, ungenügende *Spezifikation*). 3. Die Daten werden zum falschen Zeitpunkt übergeben (bspw. Zu spät oder in zu kurzen Intervallen). In den meisten Fällen handelt es sich um ein Problem bei der Aufrufreihenfolge (Protokoll).
Integrität	Integrity	Integrität ist auf dem Gebiet der Informationssicherheit ein Schutzziel und bezeichnet den Zustand der Korrektheit und Unverfälschtheit von Daten und Systemen und deren Vollständigkeit. Änderungen dürfen nur durch autorisierte Anwender durchgeführt werden. Datenintegrität bezeichnet die Integrität von gespeicherten und übertragenen Daten. Systemintegrität bezeichnet die Unverfälschtheit von Programmen und Programmcode und damit die korrekte Funktion der Anwendungen, 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	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.
Intermediate System – Intermediate System MailTrusT-Standard	(ISIS-MTT)	*Spezifikation* international verbreiteter und anerkannter Standards für *elektronische Signaturen*, *Verschlüsselung* und *Public-Key-Infrastrukturen*.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 Internetprotokoll verwendeten Portnummern zuständig.
Internet Control Message Protocol	(ICMP)	Das ICMP dient in Netzwerken zum Austausch von Informations- und Fehlermeldungen über das Internetprotokoll (IP).
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 Internetarchitektur 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 Key Exchange	(IKE)	Bestandteil des IPsec-Protokolls. IKE dient zur (siehe auch den Bezug IPS1) automatischen Schlüsselverwaltung innerhalb des IPsec-Protokolls.
Internet Protocol Control Protocol	(IPCP)	Protokoll zur automatischen Konfiguration von IP-Parametern beim PPP-Verbindungsaufbau.
Internet Protocol Security	(IPsec)	IPsec ist eine von der IETF entwickelte Sicherheitsarchitektur zur Gewährleistung von *Authentizität*, *Integrität* und *Vertraulichkeit* in IP-Netzen. Beispielsweise basiert die Sichere Inter-Netzwerk-Architektur (SINA) www.bsi.de/fachthem/sina/ auf IPsec. [RFC2401], [RFC4301]
Internet Security Association and Key Management Protocol	(ISAKMP)	ISAKMP definiert Formate und Prozeduren um Security Associations (SA) auszuhandeln und zu verwalten.

Begriff	Synonym, (AK)	Definition/Erläuterung
Interoperabilität		Die Interoperabilität wird dann gewährleistet, wenn Systeme beliebiger Hersteller oder Anbieter so beschaffen sind, dass sie gemeinsam Prozesse verarbeiten können, ohne dass Funktionen durch bestimmte Hersteller -oder Anbieterkombinationen beeinträchtigt oder begünstigt werden. Ziel ist die Austauschbarkeit von Komponenten und Diensten unterschiedlicher Hersteller/Betreiber. Die Interoperabilität von Systemen und Anwendungen ist unabhängig von der verwendeten Hardware, den eingesetzten Betriebssystemen, der verwendeten Netzwerktechnologie und der Realisierung zu betrachten und grenzt sich von der Integration insofern ab, dass diese ähnlich wie die Interoperabilität das Zusammenspiel von Systemen fordert, dabei aber die Austauschbarkeit vernachlässigt.
Interoperabilität, semantische		Semantische Interoperabilität beschreibt die fehlerfreie Austauschbarkeit von Fachinhalten innerhalb einer Anwendung, die von unterschiedlichen Anbietern zur Verfügung gestellt wird.
Interoperabilitätstest		Interoperabilitätstests dienen dem Nachweis der Austauschbarkeit von einzelnen *Komponenten* unterschiedlicher Hersteller/Betreiber. Im Rahmen des Interoperabilitätstests werden für ausgewählte Kombinationen von *Komponenten* der *Telematikinfrastruktur* die Fähigkeit zum verlässlichen Datenaustausch und die Zusammenarbeit der aufgebauten Teilsysteme gegen die Prüfanforderungen der entsprechenden *Prüfvorschriften* überprüft.
Intrusion Detection System	(IDS)	Software oder Systemsoftware zur Erkennung von Angriffen bzw. Angriffsversuchen auf Computersysteme.
IP-Adressen		Eine IP-Adresse ist eine Adresse in Computernetzen, die – wie z. B. das Internet – auf dem Internetprotokoll (IP) basieren. Sie wird Geräten zugewiesen, welche an das Netz angebunden sind und macht die Geräte so adressierbar und damit erreichbar.
IP-Adressen, private		Private IP-Adressen gehören zu bestimmten IP-Adressbereichen, die im Internet nicht geroutet werden. Sie können von jedem für private Netze wie etwa LANs verwendet werden.
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 *digitale Signaturen*, *Verschlüsselung* und PKI. Wesentliches Ziel ist es, durch ISIS-MTT die Voraussetzung für eine internationale Standardisierung und *Interoperabilität* für *Anwendungen* auf den genannten Gebieten zu schaffen.
Issuer Identification Number	(IIN)	Kennung des Kartenanbieters
IT Infrastructure Library	(ITIL)	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 (IT Service Management).

Begriff	Synonym, (AK)	Definition/Erläuterung
IT Service Management	(ITSM)	Gesamtheitliches prozessorientiertes Management definierter IT-Services mit dem Ziel der Qualitätssteigerung. Die IT Infrastructure Library (ITIL) stellt ein Best Practice Modell für das IT Service Management dar.
K		
Kanal, transparenter		Der Begriff Transparenter Kanal beschreibt im Bereich der *Mehrwertanwendungen* die Eigenschaft der Anbindung an das *Typ2-Netz*. Es wird ein Kanal aus dem Netz des *Leistungserbringers* durch den *Konnektor* in das *Typ2-Netz* angeboten, der keine Einschränkungen der Anwendungsprotokolle und Zieladressen vornimmt und somit den transparenten Zugriff aus den Systemen der Leistungserbringer auf die *Mehrwertdienste des Typ2* ermöglicht.
Kartenanwendung	card application	Die Kartenanwendung ist eine spezielle Form einer *Anwendung*.
Kartenanwendungsmanagementsystem	*Card Application Management System,* (CAMS)	System für das Kartenwendungsmanagement – im Rahmen der Festlegungen zur *Telematikinfrastruktur* wird dieser Funktionsbereichung unter *Kartenmanagementsystem* (CMS) subsumiert.
Kartengeneration		Eine Chipkartengeneration ist durch einen gewissen Funktionsumfang im Betriebssystem gekennzeichnet, zu dem insbesondere auch kryptographische Algorithmen und Schlüssellängen gehören. Ändert sich das Betriebssystem signifikant und/oder ändern sich zu unterstützende kryptographische Mechanismen und/oder Schlüssellängen, dann handelt es sich um eine neue Chipkartengeneration.
Kartenherausgeber		Der Kartenherausgeber ist verantwortlich für die Zuordnung von Karten der TI zu Personen, Institutionen und Geräten und verantwortet die Ausstellung, die Ausgabe und den Einzug von Karten.
Karteninhaber		Der Karteninhaber ist die Person, welche die Entscheidungsbefugnis über den Einsatz einer eGK im Gesundheitswesen hat. Im Allgemeinen ist dies der *Versicherte* selbst.
Kartenlebenszyklus		Alle Stadien einer *Chipkarte* wie z.B. der eGK von der Beschaffung und Erzeugung der Daten, über die Personalisierung, die Ausgabe, die Nutzung, die Veränderung bis hin zur Terminierung. Der Kartenlebenszyklus wird im *Kartenmanagementsystem* verwaltet.
Kartenmanagement, physisches		Unter dem Begriff „Physisches Kartenmanagement“ wird im Kontext der eGK die Verwaltung von *Gesundheitskarten* als physikalische Datenträger verstanden. Dies beinhaltet alle zur Ausstellung und Verwaltung der eGK benötigten *Prozesse*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Karten-management-system	Card Management System, (CMS)	Das Kartenmanagementsystem ist eine vom *Kartenherausgeber* zur Verwaltung der eGK (über den gesamten Lebenszyklus) benötigte *Anwendung*, die die Ausgabe und Verwaltung von Karten und kartenbezogenen Daten umfasst. Der Begriff bezeichnete auch den *Fachdienst* in der TI, der allerdings nur ein Teil der TI ist. Das Kartenmanagementsystem ist ein *Produkttyp*.
Karten-personalisierer		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 eGK als *Akteur* verwendet.
Kartenterminal	(KT)	Technische Einrichtung zum Kontaktieren der im *System* verwendeten *Chipkarten*
Kartenterminal, eHealth-	(eH-KT)	LAN-fähiges *Kartenterminal* nach SICCT-Spezifikation, das die spezifischen Anforderungen zum Lesen und Schreiben von Daten auf die *eGK* und zur sicheren Kommunikation mit der *Telematikinfrastruktur* erfüllt. Das eHealth-Kartenterminal ist ein *Produkttyp*.
Kartenterminal, eHealth-BCS-		Spezifische Ausprägung des *eHealth-Kartenterminals*. Migrationsfähige (entsprechen der aktuellen eHealth-Kartenterminal *Spezifikation* [gemSpec_KT]) Kartenlesegeräte, welche zusätzlich eine USB- bzw. V24-Schnittstelle unterstützen sowie mit einem Upgrade ohne Austausch der Geräte zu einem vollwertigen LAN-fähigen „*eHealth-KT*“ aufgerüstet werden können. Kartenlesegeräte auf dieser Basis MÜSSEN an der V.24- und/oder USB-Schnittstelle mindestens den „Basis Command Set (BCS)“ unterstützen. Das eHealth-BCS-Kartenterminal ist ein *Produkttyp*.
Kartenterminal, mobiles	(mob-KT)	Das mobile Kartenterminal kommt hauptsächlich außerhalb der Arztpraxis – z. B. bei Hausbesuchen oder Behandlungen in Heimen – zum Einsatz. Es soll dem *Leistungserbringer* ermöglichen, außerhalb seiner Praxis die *Versichertenstammdaten* seiner Patienten zu Abrechnungszecken zu erfassen, sowie *Notfalldaten* anzuzeigen. Beim mobilen Kartenterminal handelt es sich um einen *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Kartenterminal, multi-funktionales	(MKT)	Zum Lesen und Beschreiben von Karten werden *Karten-terminals* benötigt. Für das Gesundheitswesen wurde ein „Multifunktionales Kartenterminal (MKT)“ entwickelt. Das MKT ist für alle *Anwendungen* geeignet, die auf Karten, insbesondere Smart Cards basieren und durch einen PC gesteuert werden. Ein Modul zum Lesen der heutigen Versichertenkarte steht zur Verfügung. Unter der Bezeichnung MKT+ wird die Er-weiterung dergestalt verstanden, dass das KT auch die elektronische Gesundheitskarte lesen kann. Die Weiterent-wicklung wird als *eHealth- (BCS-) Kartenterminal* bezeich-net. Die *Spezifikation* ist im Internet unter der Adresse http://sit.gmd.de/SICA/mkt.html verfügbar (Quelle: [WuV])
Karten-versender		Der Kartenversender übernimmt das Mailing der Karte. Dies umfasst im Allgemeinen das Personalisieren eines An-schreibens, 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 *Akteur* 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 Lebens-zyklus der Karte zu koordinieren.
Kettenmodell		Das Kettenmodell ist ein so genanntes Gültigkeitsmodell für Zertifizierungspfade, bei dem alle *Zertifikate* im Pfad genau dann gültig sind, wenn der zugehörige Zertifizierungs-schlüssel zum Zeitpunkt der Erstellung (des *Zertifikats*) auf einem gültigen *Zertifikat* beruht.
Key Generator		Ein Key Generator ist ein Programm welches zum einen automatisch nach einem Algorithmus Seriennummern oder Freischaltungscodes erstellt und zum anderen Passwörter für Verschlüsselungsmechanismen erzeugt.
Key Performan-ce Indikator	(KPI)	Eine Messgröße, die eine Prozessoptimierung, einen IT-Service oder eine Aktivität unterstützen soll. Es können Messungen anhand von zahlreichen Messgrößen erfolgen, es werden jedoch nur die wichtigsten dieser Größen als KPI definiert und für eine aktive Verwaltung und Be-richtserstellung in Bezug auf den *Prozess*, den IT Service oder die Aktivität eingesetzt. Bei der Auswahl der KPIs sollte die Sicherstellung von Effi-zienz, Effektivität und Wirtschaftlichkeit berücksichtigt wer-den.
Kiss-’o-death		Mit Hilfe dieses Verfahrens kann der NTP-Server die An-zahl der an ihn gerichteten Anfragen von korrekt imple-mentierten und hierarchisch untergeordneten NTP-Servern beeinflussen. Das Verfahren ist im Dokument „Spezifikation Infrastrukturkomponenten: Zeitdienst“ [gemNTP] beschrie-ben.

Begriff	Synonym, (AK)	Definition/Erläuterung
Known Error		Ein *Problem*, deren Ursache im *Problem Management* identifiziert wurde und durch das *Problem Management* als ein bereits bekannter Fehler deklariert wird. (ITIL-basierter Begriff)
Komfort-signatur		Bezeichnung eines Signaturverfahrens, bei dem das wissensbasierende auslösende Merkmal (PIN) bei der Erzeugung einer Signatur durch eine Kombination aus biometrischen Merkmal (Fingerabdruck) oder besitzbasierenden Merkmal (RFID-Token) ggf. mit einem schwachen wissensbasierenden Merkmal (PIN) ergänzt wird. Der Besitz der sicheren *Signaturerstellungseinheit* (SSEE) ist neben den o.g. Merkmalen Voraussetzung für die Anwendung des Signaturschlüssels.
Kommunikation für Leistungs-erbringer	(KOM-LE)	Gesamtheit der Komponenten und Prozesse, die die sichere Kommunikation für Leistungserbringer gemäß Projektauftrag umsetzen.
Kommunikation für Leistungs-erbringer-Teilnehmer		Leistungserbringer oder medizinische Institutionen, die bei einem KOM-LE-Anbieter zur Nutzung von KOM-LE registriert sind.
Kompatibilitäts-matrix		Liste von durch die gematik freigegebenen Hard- und Softwarekomponenten, die für den *Betrieb* eines *Services* zugelassen und getestet sind.
Komponente	component	Eine Komponente der *Telematikinfrastruktur* ist ein physischer (z.B. *Konnektor*) oder logischer (z.B. *VODD*) Bestandteil eines *Systems*, der im Rahmen einer *Spezifikation* beschrieben wird. In konkreten Zusammenhängen wird der Begriff der Komponente weiter eingeschränkt. Verschiedene Komponenten und *Dienste* können *Produkttypen* bilden. Die Komponentenzulassung wird gemäß § 291b Abs. 1a SGB V erteilt.
Komponenten der TI-Plattform, dezentrale		Dezentrale Komponenten der TI-Plattform sind Anteile der TI-Plattform in den lokalen Netzen der Leistungserbringer und Kostenträger. Beispiele für dezentrale Komponenten der TI-Plattform sind: Konnektor, Kartenterminal, eGK, HBA, SMCs. Fachmodule der Fachanwendungen sind hier nicht enthalten.
Komponenten, dezentrale		Kurzform für *dezentrale Komponenten der TI-Plattform*
Komponenten und Dienste der TI		Der Begriff umfasst als Sammelbegriff die Fachmodule, dezentralen Komponenten der TI-Plattform, zentrale Dienste der TI-Plattform und Fachdienste.
Komponenten und Dienste der TI-Plattform		Der Begriff umfasst als Sammelbegriff die dezentralen Komponenten der TI-Plattform und die zentralen Dienste der TI-Plattform.
Komponenten-Funktionstest	(KFT)	Testphase im *Komponententest*. Testfokus sind die *funktionalen Anforderungen* einer einzelnen *Komponente*.
Komponenten-Interoperabilitätstest	(KIT)	Testphase im *Komponententest*. Testfokus ist das Zusammenspiel mehrerer *Komponenten* und die Austauschbarkeit einer einzelnen *Komponente*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Komponenten-Leistungstests	(KLT)	Testphase im *Komponententest*. Testfokus ist das Leistungsverhalten einer einzelnen *Komponente* (oder auch im Zusammenspiel mit anderen *Komponenten*.
Komponenten-modell		Abstraktion der physischen oder logischen Systemarchitektur. Ein *System* wird soweit in einzelne *Komponenten* zerlegt, dass für die benötigte Sicht relevante Eigenschaft identifizierbar sind (z. B. Schnittstellen, *Sicherheitsanforderungen*).
Komponententest	(KT)	Beim Komponententest werden *Komponenten* (typischerweise in einer Labortestumgebung) getestet.
Komponenten-zertifikate		Diejenigen *Zertifikate*, mit denen die *Identität* und/oder *Integrität* von Hardware- und Softwarekomponenten sichergestellt werden soll. Beispielhaft hierfür stehen die *Zertifikate* für *Fachdienste*, *Konnektoren*, *Kartenterminals* oder Softwareversionsstände. Die derartige Komponentenzertifikate herausgebenden *Trust Service Provider* (TSP) werden in der „Trusted Component List“ (TCL) zusammengefasst.
Konfigurations- und Software-Repository		Ein Konfigurations- und Software-Repository ist ein Dienst, der Konfigurationsdaten und oder Softwarepakete (allgemein Aktualisierungspakete) verwaltet und zum Download bereitstellt.
Konfigurations-daten		Unter dem Begriff Konfigurationsdaten sind sowohl die Informationen über ein Konfigurationsobjekt selber als auch alle Beziehungen zu anderen Konfigurationsobjekten zu verstehen.
Konnektor	(Konn)	Der Konnektor koordiniert und verschlüsselt die Kommunikation zwischen *Primärsystem*, eGK, HBA/SMC und *Telematikinfrastruktur*. Er stellt damit das Bindeglied zwischen diesen *Komponenten* auf Leistungserbringerseite bzw. *eKiosk* und *Telematikinfrastruktur* dar.
Konnektor-identität		Die Geräteidentität des *Konnektors* teilt sich in drei *Identitäten* auf, eine für den *Netzkonnektor* (ID.NK.VPN), eine für den *Anwendungskonnektor* (ID.AK.AUT) und eine für die *Signaturanwendungskomponente* (ID.SAK.AUT). Die Geräteidentität des *Konnektors* ist also die Summe dieser drei *Identitäten*.
Kontra-Indikations-check		Paarweise Prüfung von Medikamenten oder Wirkstoffe gegen Diagnosen oder Symptome auf bekannte und somit referenzierbare Gegenanzeigen (Kontraindikation). Beispiel: Morbus Crohn und Aspirin, Referenz ABDamed.
Kosten-erstattungs-verfahren	procedure of compensation (for outlay)	Unter Kostenerstattungsverfahren ist, auch in Verbindung mit dem SGB V, die Wahl der Kostenerstattung für vorher verauslagte Kosten anstelle der zu gewährenden Sach- und Dienstleistungen zu verstehen.
Kostenträger	cost unit, (KTR)	Kostenträger sind im Kontext der TI die privaten und gesetzlichen Krankenversicherungen.
Kosten-trägerkennung		*Institutionskennzeichen* der *Krankenversicherung*

Begriff	Synonym, (AK)	Definition/Erläuterung
Krankenkasse, gesetzliche		Körperschaft des öffentlichen Rechts, die Leistungen der *gesetzlichen Krankenversicherung* für ihre Versicherten gewährt.
Kranken-versicherten-karte	(KVK)	Chipkarte gemäß §291 SGB V, welche seit 1995 den Krankenschein ersetzt hat. Die Karte enthält reine Verwaltungsdaten (Krankenkasse, Name, Geburtsdatum und Anschrift des Versicherten, KVNR und Versichertenstatus).
Krankenversicherten-nummer	(KVNR)	Eindeutige Krankenversichertennummer nach § 290 SGB V (20 bzw. 30 Stellen), zusammengesetzt aus: 1. *Versicherten-ID* (10 Stellen; unveränderbarer 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)
Kranken-versicherung		Die Krankenversicherung umfasst die *gesetzliche* und private *Krankenversicherung*.
Kranken-versicherung, gesetzliche	(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 *Versicherten* zu gewährleisten. Die Beitragsfinanzierung läuft in der GKV im Umlageverfahren und nicht – wie bei der privaten Krankenversicherung – durch Kapitaldeckung. Die Leistungen werden nach dem Sachleistungsprinzip erbracht, d.h. Versicherte müssen bei einem Arztbesuch etc. nicht in Vorleistung treten.
Krypto Subsystem		Funktionsfeld zur Verarbeitung von PKI-Anwendungen (Signaturerstellung, -prüfung, Datenverschlüsselung, -entschlüsselung)
L		
Labortest	Testing in a specific test side	Der Labortest ist die erste Teststufe der Testmaßnahmen zur Einführung der *elektronischen Gesundheitskarte*. Die gematik führt im Labortest zentral Tests einzelner *Komponenten*, integrierter *Systeme* und grundsätzlicher Verfahren unter Laborbedingungen mit Testdaten durch. (Begriff aus [RVO2009]) Die Ziele der Labortests sind: - *Komponententests* - *Integrationstests* - *Interoperabilitätstests* - *Sicherheitstests*

Begriff	Synonym, (AK)	Definition/Erläuterung
Lastenheft		Das Lastenheft enthält die aus Auftraggebersicht zu erfüllenden Anforderungen an ein System und dokumentiert diese. Kern sind die funktionalen und nicht-funktionalen Anforderungen. Das Lastenheft ist Grundlage für die Pflichtenheftphase.
Lasttest	load test	Im Lasttest wird das spezifizierte Antwortzeit- und Durchsatzverhalten für definierte Anwendungsfälle auf Übereinstimmung (Zeitrestriktionen) mit den Spezifikationen bzw. Service Level Agreements (SLAs) überprüft.
Layer 2 Tunneling Protocol	(L2TP)	L2TP ist ein reines Tunneling-Protokoll, welches auf der PPP-Ebene angesiedelt ist. L2TP stellt dabei eine Mischform von PPTP und L2F dar und hat eine Benutzerauthentifikation mittels PAP und CHAP implementiert.
Lebenszyklus		Im Zusammenhang mit dem *Kartenmanagement* ist der Lebenszyklus der Karte gemeint. Siehe *Kartenlebenszyklus*.
Leer-PIN		Eine spezielle Ausführung der *Transport-PIN*, bei der vom Benutzer zur Zuordnung einer Echt-PIN keine vorgegebene PIN eingegeben werden muss.
Leistung		Eine Leistung wird bei der gematik im technischen Sinne innerhalb der Telematikinfrastruktur (durch z.B. Dienste) erbracht und ist abzugrenzen von Leistungen im medizinischen Sinne, die durch Leistungserbringer angeboten werden.
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 nichtfunktionalen 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
Leistungsanpruch, nachgehender		Leistungsanspruch für längstens einen Monat nach Ende der Mitgliedschaft, solange keine Erwerbstätigkeit ausgeführt wird. Bei Ende der Mitgliedschaft durch Tod des Versicherten erhalten die nach § 10 SGB V versicherten Angehörigen Leistungen längstens für einen Monat nach dem Tode des Mitglieds (§ 19 SGB V).
Leistungsanspruch		Anspruch des Versicherten auf Leistungen gemäß Drittem Kapitel SGB V aus der gesetzlichen Krankenversicherung.
Leistungsanspruch, ruhender		Leistungsansprüche können gemäß § 16 SGB V für einen bestimmten Zeitraum ruhen. Dabei ist zwischen Fällen des eingeschränkten Ruhens (§ 16 Absatz 3a SGB V) und Fällen des vollständigen Ruhens (§ 16 Absätze 1 bis 3 SGB V) zu unterscheiden.
Leistungserbringer	(LE)	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach § 291a Abs. 4 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte.

Begriff	Synonym, (AK)	Definition/Erläuterung
Leistungs-erbringer-organisation	(LEO)	Standesorganisation von *Leistungserbringern* (KBV, BÄK, DAV, DKG etc.)
Leistungs-niveau	Service Level	Im Rahmen eines Leistungsvertrags definierte *Leistung*.
Leistungspflicht		Umfasst alle gesetzlich vorgeschriebenen Leistungen, die von der Gesetzlichen Krankenkasse gegenüber ihren Versicherten zu erbringen sind.
Leistungs-schein		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 *Service Level Agreements* aufgeführt (siehe SLA).
Leistungstest		Leistungstest ist ein Oberbegriff verschiedener Tests zum Leistungsverhalten: • Lastverhalten (Lasttest) • Antwortzeit- und Durchsatzverhalten (Performanztest) • Verhalten bei Überlast (Stresstest)
Leistungs-vertrag	*Service Level Agreement*	Als Leistungsvertrag, Dienstgütevereinbarung oder englisch *Service Level Agreement* (SLA) 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)
Leitstand		Bereich innerhalb der gematik, der für die Koordination des Betriebes der *Telematikinfrastruktur* zuständig ist.
Leitstand Service	(LS)	Für die *Telematikinfrastruktur* konkret realisierbarer *Dienst* um die Erfüllung des Sicherstellungsauftrags an die gematik während des operativen Betriebs zu unterstützen. Der *Dienst* Leitstand Service kommuniziert hierzu mit dem *Dienst Betriebsleitzentrale Service* um die hierzu nötigen Steuerungs- und Aufsichtsfunktionen durchzuführen. Weitere Anteile der Steuerungs- und Aufsichtsfunktion finden rein organisatorisch zwischen dem *Leitstand* und der *Betriebsleitzentrale* statt. Der Leitstand Service ist ein *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 Erkennungs-merkmal dargestellt. Umgangssprachlich und auch in der eGK-Spezifikation Teil 3 wird sie als „Leonardo“ bezeich-net.
Lightweight Directory Ac-cess Protocol	(LDAP)	Mit dem Lightweight Directory Access Protocol (Spec. [RFC2251]) können Informationen, die in einem *Verzeich-nisdienst* gespeichert sind, abgerufen oder modifiziert wer-den.
Load Balancing		Automatisierte Lastenverteilung zwischen mehreren IT-*Systemen*, die den gleichen *Dienst* anbieten.
Logdaten, Logs		Daten über Ereignisse, z.B. Störungen
Logging		Protokollierung von technischen Ereignissen, z. B. zur Er-leichterung einer Fehlerdiagnose oder zur Überwachung der Systemauslastung.
Long Term Ar-chive Notary Services		Standard für das Format der Integritätsnachweise in digita-len Langzeitarchiven.
Lösungsanaly-se		Als Lösungsanalyse wird die vorbereitende Phase für die Erstellung des Pflichtenheftes bezeichnet („Big picture“).
Lösungsanbie-ter		Lösungsanbieter ist der Oberbegriff für alle Anbieter und Hersteller von Anwendungen, Komponenten, Diensten und Fachdiensten der TI.
Lösungs-architektur	solution outline	Ergebnisdokument des Vorprojektes *biT4health*: Darin wur-de an Hand der in der *Rahmenarchitektur* vorgegebenen Regeln die *Telematikinfrastruktur* weiter detailliert.
Low-Level-Signaturformat		Bei Low-Level-Signaturformaten ist bitgenau spezifiziert, wie die zu signierenden Daten, oder ein *Hash-Wert* derse-ben, vor der eigentlichen *Anwendung* des asymmetrischen Kryptoalgorithmus, z.B. durch Füllmechanismen (*Padding*), aufzubereiten sind.
M		
MAC Adresse		eindeutige Hardware-Adresse einer Netzwerkkarte
Major Release		Ein Major Release enthält wesentliche – ggf. auch nicht kompatible – neue Funktionen und Leistungen und löst Vor-gängerrelease(s) nach einer Übergangszeit vollständig ab. Es wird gekennzeichnet durch die Änderung der 1. Stelle der Releaseversion.
Management-Netz	(Mgmt-Netz)	Das Management-Netz auf Basis von MPLS verbindet die BLZ mit allen Dienste-Betreibern der TI zur Kommunikation über die Systemmanagementschnittstelle. Das Managementnetz ist ein *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Mandant		Ein Mandant ist eine rechtlich selbstständige Organisationseinheit innerhalb einer *Institution* (z.B. innerhalb eines Krankenhauses oder innerhalb einer *Praxisgemeinschaft*). In den meisten Fällen wird eine *Institution* eines *Leistungserbringers* gegenüber der *Telematikinfrastruktur* nicht in mehrere Organisationseinheiten gegliedert sein. Sie stellt sich somit als ein Mandant dar.
Mandantenfähig		Als mandantenfähig werden IT-*Anwendungen* und IT-*Komponenten* bezeichnet, wenn sie von mehreren *Mandanten* (Kunden, Auftraggeber, juristische Firmen) genutzt werden können, ohne dass diese Zugriff auf oder Einblick in die Daten der jeweils anderen *Mandanten* haben.
Masquerading		Masquerading (engl.) oder Adressmaskierung ist eine spezielle Form von *Network Adress Translation* (NAT) und wird zumeist verwendet, um mehreren Computern in einem Local Area Network Zugriff auf das Internet zu ermöglichen. Dabei werden im Gegensatz zu NAT nicht nur die IP-Adressen, sondern auch Port-Nummern umgeschrieben.
Maßnahme, medizinische		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.
Mechanismenstärke		Bewertung der Wirksamkeit von Sicherheitsmechanismen, Widerstand gegen einen direkten Angriff zu leisten. Für die Stärke der Mechanismen sind mehrere Stufen definiert, die ein Maß für das Vertrauen sind, inwieweit die beschriebenen Sicherheitsmechanismen in der Lage sind, direkten Angriffen zu widerstehen.
Mechanismenstärke von kryptographischen Algorithmen		Definiert die Stärke eines kryptographischen Algorithmus, d. h. wie viel Aufwand es bedarf, einen kryptographischen Algorithmus zu brechen. Dieser Aufwand wird in verschiedenen Klassen angegeben.
Medikationsdaten		Die Medikationsdaten beinhalten Informationen über abgegebene oder applizierte Arzneimittel.
Mehrfachsignatur		Erstellung einer begrenzten Anzahl Signaturen nach der einmaligen Authentisierung des Signaturschlüssel-Inhabers (Quelle: Technische Richtlinie [BSI-TR-03114])
Mehrkomponentenkonnektor	(Mkonn)	Bei der Mehrkomponentenlösung ist die Funktionalität des *Konnektors* auf getrennte *Anwendungs-* und *Netzkonnektoren* verteilt. Diese Ausprägung des *Konnektors* ist für den *Betrieb* in großen Leistungserbringereinrichtungen ausgelegt. Der Mehrkomponentenkonnektor ist ein *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Mehrwertan-wendung	(MWA)	Nicht in §291a SGB V genannte Anwendungen in der Telematikinfrastruktur, die die dezentralen und zentralen Komponenten bzw. Dienste der TI nutzen und selbst Funktionalitäten für Anwender innerhalb der Telematikinfrastruktur bereitstellen. Diese Anwendungen müssen eine Zulassung durch die gematik besitzen.
Mehrwert-anwendung des Typs 1	(MWA TYP1)	Eine *Mehrwertanwendung* Typ1 ist eine konkrete Ausprägung einer *Mehrwertanwendung*. In diese Kategorie fallen *Mehrwertanwendungen*, die die durch die *dezentralen Komponenten* der *Telematikinfrastruktur* beim *Leistungserbringer* lokal angebotenen Funktionen nachnutzen. Diese Funktionen werden über ein Typ1-API angeboten. Die Nutzung von *Diensten* der zentralen TI (z.B. OCSP o.ä.) ist für diesen Typ von *Mehrwertanwendungen* nicht möglich.
Mehrwertan-wendung des Typs 2	(MWA TYP2)	Eine *Mehrwertanwendung* Typ2 ist eine konkrete Ausprägung einer *Mehrwertanwendung*. In diese Kategorie fallen *Mehrwertanwendungen*, die *Dienste* außerhalb der *Telematikinfrastruktur* im *Typ2-Netz* nutzen, wobei die dezentralen *Komponenten* der *Telematikinfrastruktur* einen transparenten Zugang zu diesen Netzen schaffen. Im Gegensatz zu den Typen 1,3 und 4 besteht für Typ2 kein eigenes API sondern es wird ein *transparenter Kanal* in ein Netz angeboten.
Mehrwertan-wendung des Typs 3	(MWA TYP3)	Eine *Mehrwertanwendung* Typ3 ist eine konkrete Ausprägung einer *Mehrwertanwendung*. Bestimmte Infrastrukturdienste sind auch für die Nutzung durch *Anwendungen* außerhalb der *Telematikinfrastruktur* interessant, beispielsweise der Zugriff auf die Verzeichnisse von *Leistungserbringern* oder die Nutzung der HBA-OCSP-Responder für Zertifikatsprüfungen. Die *Mehrwertanwendungen*, die ausgewählte Funktionalität der *zentrale Infrastruktur* nachnutzen, selbst aber keine zentralen Bestandteile haben, werden als Typ 3 – Mehrwertanwendungen bezeichnet. Die Nutzung der zentralen Infrastrukturdienste erfolgt über die Nutzung der durch das *Typ3-API* bereitgestellten Funktionen.
Mehrwertan-wendung des Typs 4	(MWA TYP4)	Eine *Mehrwertanwendung* Typ4 ist eine konkrete Ausprägung einer *Mehrwertanwendung*. Analog zu den gesetzlich geregelten *Anwendungen* können diese *Mehrwert-anwendungen* zentrale *Dienste* (Mehrwertfachdienste) umfassen und die technischen Mechanismen der gesetzlichen *Anwendungen* in vollem Umfang nachnutzen. Die Kommunikation mit den *Mehrwertfachdiensten* erfolgt über das, durch den *Konnektor* bereitgestellte, *Typ4-API*.
Mehrwertclient	(MWC)	Ein Mehrwertclient ist eine Client-*Komponente* einer *Mehrwertanwendung* außerhalb der *Telematikinfrastruktur*, die über die *Primärsystemschnittstelle* des *Konnektors* Funktionen der Mehrwert-APIs nutzt, oder auf Funktionen von Mehrwertmodulen zurückgreift.

Begriff	Synonym, (AK)	Definition/Erläuterung
Mehrwertdienst	(MWD)	Als Mehrwertdienst wird eine zentrale Komponente einer *Mehrwertanwendung* bezeichnet. Dies kann sich sowohl auf einen Server im *Typ2-Netz* beziehen, als auch auf einen *Mehrwertfachdienst* einer *Mehrwertanwendung* des Typ4. Der Begriff umfasst neben der reinen *Anwendung* auch die für den Betrieb nötige Infrastruktur des *Betreibers*. Ein Mehrwertdienst liegt immer in der Verantwortung genau eines *Betreibers*.
Mehrwertdienst Typ2	(MWD2)	Ein Mehrwertdienst Typ2 ist ein *Dienst* zur Bereitstellung einer *Mehrwertanwendung*, also die serverseitige technische Bereitstellung einer *Mehrwertanwendung*. Der Mehrwertdienst Typ2 ist ein *Produkttyp*.
Mehrwertdienst Typ4	(MWD4)	Ein Mehrwertdienst Typ4 ist ein *Dienst* zur Bereitstellung einer *Mehrwertanwendung*, also die serverseitige technische Bereitstellung einer *Mehrwertanwendung*. Der Mehrwertdienst Typ4 ist ein *Produkttyp*.
Mehrwertfachdienst	(MWFD)	Ein Mehrwertfachdienst ist ein *Mehrwertdienst* innerhalb der *Telematikinfrastruktur*, d.h. Server einer *Mehrwertanwendung des Typs 4.*
Mehrwertmodul	(MWM)	Ein Mehrwertmodul ist eine, in eine der *dezentralen Komponenten* der *Telematikinfrastruktur* integrierte, *Komponente*. Das Mehrwertmodul ist entweder vollkommen isoliert von der *Telematikinfrastruktur* und nutzt weder Funktionen noch Identitäten der TI (einschließlich der *dezentralen Komponenten*, in die es integriert ist) oder agiert als *Mehrwertclient* einer *Mehrwertanwendung* und nutzt dann von der TI ausschließlich die, über Mehrwert-APIs des *Konnektors* angebotenen Funktionen. Der Begriff Mehrwertmodul unterscheidet nicht zwischen implementierter Client- und Server-Funktionalität.
Message Authentication Code	(MAC)	Ein Message Authentication Code (MAC) dient zur Sicherung der *Integrität* und *Authentizität* einer Nachricht. Anders als bei einer *digitalen Signatur* werden hier aber keine asymmetrischen Kryptoalgorithmen, sondern symmetrische Algorithmen und *geheime Schlüssel* 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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Migration		Eine Migration ist ein geordneter Prozess, der ein System von einem Status in einen anderen überführt. Bezogen auf die *Telematikinfrastruktur* wird durch eine Migration der *Wirkbetrieb* von einem *Releasestand* A eines *Releases* R1 auf einen *Releasestand* B eines neuen *Releases* R2 überführt. Bedingt durch die verteilte Infrastruktur ist für Migrationen der TI ein längerer Zeitraum einzuplanen, was dazu führt, dass sich mehrere *Releases* über einen längeren Zeitraum parallel im *Wirkbetrieb* befinden können.
Migrationspfad		Der Migrationspfad beschreibt die Schritte, die für die Durchführung einer *Migration* erfolgen. Zum Beispiel ist die Einführung der eGK in mehreren abgesicherten und beherrschbaren Stufen ein Migrationspfad.
Minor Release		Ein Minor Release umfasst Ergänzungen und Erweiterungen, die weitgehend kompatibel und in der Regel langfristig koexistent zum Vorgängerrelease sind. Ein Minor Release stellt eine Ausbaustufe eines Major Release dar. Es wird gekennzeichnet durch die Änderung der 2. Stelle der Releaseversion.
Mitarbeiter medizinische Institution		Ein „Mitarbeiter medizinische Institution“ arbeitet in einer *Institution* zur medizinischen Versorgung (z.B. Arztpraxis, Krankenhaus) auf Weisung des verantwortlichen Vorgesetzten als berufsmäßiger Gehilfe des *Arztes*/ Zahnarztes oder zur Vorbereitung auf den Beruf. Er kann auf die Daten der *freiwilligen Anwendungen* und der *eVerordnungen* zugreifen, soweit dies im Rahmen der von ihm zulässigerweise zu erledigenden Tätigkeiten erforderlich ist (§ 291a Abs. 4 Satz 1). Dazu muss er von einer Person autorisiert sein, die über einen HBA oder entsprechenden BA verfügt. Die *Autorisierung* und der Zugriff müssen nachprüfbar elektronisch protokolliert werden (§ 291a Abs. 5 Satz 4). Der „Mitarbeiter medizinische Institution“ verkörpert gegenüber der *Telematikinfrastruktur* die *Institution* des *Arztes*/Zahnarztes/Krankenhauses.
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.
Modultest	unit test	Der Modultest ist Teil eines Softwareprozesses. Er dient zur Verifikation der Korrektheit von Modulen einer Software, z.B. von einzelnen Klassen, Librarymodulen oder Funktionen.
Monitoring		Mit dem Monitoring können *Dienste*, *Services* und *Prozesse* einer *Infrastruktur* überwacht und gegen Schwellwerte verglichen werden. Dies geschieht in „Echtzeit“.
Multi Protocol Label Switching	(MPLS)	Netzwerktransportprotokoll zur performanten Weiterleitung von Datenpaketen über eine verbindungsorientierte Verbindung mit integrierten Möglichkeiten zum Aufbau von VPNs (Virtual private Network), und Unterstützung von Quality of Services (QoS) in verbindungslosen Netzen.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 Rolle. 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 *Telematikinfrastruktur* 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 Applikationen 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 (Ressource Records) für anfragende *Resolver* bereitstellt.
Namensdienst	(DNS)	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. Der Namensdienst ist ein *Produkttyp*.
National Institute for Standards and Technology	(NIST)	Das NIST ist ein staatliches Standardisierungsinstitut in den USA. Zu den vom NIST publizierten Standards zählt beispielsweise DAS und SHA-1.
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. (Quelle: [CNTS])
Netz, virtuelles privates	(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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Netzkonnektor	(NK)	Der Netzkonnektor als dezentrale Komponente der TI-Plattform stellt die sichere Verbindung auf Netzwerkebene zwischen den dezentralen Systemen auf der einen Seite und den zentralen Diensten der TI-Plattform sowie den fachanwendungsspezifischen Diensten auf der anderen Seite her.
Netzwerk-dienste		Querschnittliche Leistungen der TI-Plattform auf logischer Ebene zur Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Netzwerkdienste werden in der Netzwerkschicht der TI-Plattform angeboten.
Nichtabstreit-barkeit	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 Verbindlichkeit und den Beweis einer Transaktion. Nichtabstreitbarkeit ist eine der zentralen *Sicherheitsanforderungen* neben *Verfügbarkeit*, *Integrität*, *Authentizität* und *Vertraulichkeit*.
Noctu		Kennzeichen des Papierrezeptes oder der *eVerordnung*, welches vom *Arzt* gesetzt wird, um eine notwendige Belieferung während der allgemeinen Ladenschlusszeiten von Apotheken zu kennzeichnen und somit eine Abrechnung des zugehörigen Noctu-Zuschlages der Apotheke gegenüber dem *Kostenträger* zu ermöglichen.
Non Volatile Random Access Memory	(NVRAM)	Nicht flüchtiger Speicher mit wahlfreiem Zugriff. Darin werden vorrangig Konfigurationsdaten abgelegt.
Notfalldatensatz		Die Gesamtheit der notfallrelevanten medizinischen Informationen eines Patienten bildt den Notfalldatensatz.
Notfallrelevante medizinische Daten		Notfallrelevante medizinische Daten sind diejenigen Informationen aus der medizinischen Vorgeschichte des Patienten, die dem behandelnden Arzt zur Abwendung eines ungünstigen Krankheitsverlaufs sofort zugänglich sein müssen.
NTP-Server		Serversysteme, die mittels NTPd (NTP daemon) Zeitsynchronisationsdienste anbieten und sich selber mit einer Zeitquelle synchronisieren können. In Deutschland bietet die Physikalisch-technische Bundesanstalt beispielsweise öffentliche Stratum-1-Server an, die unter den Namen `ptbtime1.ptb.de` und `ptbtime2.ptb.de` erreichbar sind.
Nutzdaten		Als Nutzdaten (Englisch: payload) bezeichnet man in der Kommunikationstechnik diejenigen während einer Kommunikation zwischen zwei Partnern transportierten Daten eines Datenpakets, die keine Steuer- oder Protokollinformationen enthalten. Nutzdaten sind unter anderem Sprache, Text, Zeichen, Bilder und Töne.
Nutzer	*Anwender*	*siehe dort*

Begriff	Synonym, (AK)	Definition/Erläuterung
Nutzungspolicy		Die Nutzungspolicy legt fest, welche TI-Anwendungen aus Sicht der Gesellschafter in der Telematikinfrastruktur erwünscht sind und welche nicht. Sie definiert Kriterien, auf deren Basis eine Entscheidung zur Aufnahme von Anwendungen in die TI erfolgen kann. Bei Nichterfüllung der Kriterien ist von einer ungeeigneten Anwendung auszugehen, so dass die Anwendung nicht in die TI aufgenommen werden darf.
O		
Objektreferenz		Eindeutiger Verweis auf ein Objekt innerhalb eines *Fachdienstes*, bestehend aus Diensttyp, Dienstinstanz und Objekt-ID des Objektes. Durch die Objektreferenz kann jedes Objekt innerhalb der *Telematikinfrastruktur* eindeutig adressiert werden.
ObjektTicket	(OT)	Beim ObjektTicket handelt es sich um einen Begriff aus dem Bereich der Datenelemente. ObjektTickets werden durch das Berechtigungskonzept der gematik definiert. Jedem *medizinischen Datenobjekt* ist in der TI genau ein ObjektTicket zugeordnet, das die *Hybridschlüssel* und optional Berechtigungsinformationen aller Zugriffsberechtigten sowie Informationen zur Sichtbarkeit des Objektes enthält. Jedes ObjektTicket enthält eine Referenz auf das ihm zugeordnete Objekt.
OCSP-Responder	*Validierungsdienst*	Der OCSP-Responder ist eine spezifische, für die *Telematikinfrastruktur* vorgegebene Ausprägung eines *Validierungsdienstes* für Zertifikate und Signaturen, wobei die Prüfung Online, also zeitnah und aktuell, durchgeführt wird (siehe auch *Online Certificate Status Protocol*).
OCSP-Responder eGK	(OCSP-eGK)	Der *Validierungsdienst* stellt Statusinformationen für eine automatische Gültigkeitsüberprüfung von elektronischen Zertifikaten unter Verwendung von OCSP (*Online Certificate Status Protokoll*) zur Verfügung. Dabei stellt der OCSP-Responder eGK Zertifikatsstatusinformationen für die eGK bereit und bestätigt oder widerlegt die Gültigkeit der darauf aufgebrachten Personenzertifikate. Es handelt sich um einen *Produkttyp*.
OCSP-Responder HBA/SMC-B	(OCSP-HBA-SMCB)	Der *Validierungsdienst* stellt Statusinformationen für eine automatische Gültigkeitsüberprüfung von elektronischen Zertifikaten unter Verwendung von OCSP (*Online Certificate Status Protokoll*) zur Verfügung. Dabei stellt der OCSP-Responder HBA/SMC-B Zertifikatsstatusinformationen für den HBA sowie die SMC-B bereit und bestätigt oder widerlegt die Gültigkeit der darauf aufgebrachten Personenzertifikate. Es handelt sich um einen *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
OCSP-Responder Komponenten PKI	(OCSP-Komp)	Der *Validierungsdienst* stellt Statusinformationen für eine automatische Gültigkeitsüberprüfung von elektronischen Zertifikaten unter Verwendung von OCSP (*Online Certificate Status Protokoll*) zur Verfügung. Dabei stellt der OCSP-Responder Komponenten PKI Zertifikatsinformationen für die Komponenten der TI bereit und bestätigt oder widerlegt die Gültigkeit der Komponentenzertifikate, insbesondere für Konnektoren sowie Server- und (Fach-)Dienste. Es handelt sich um einen *Produkttyp*.
Offline Szenario	*Standalone-Szenario*	*siehe dort*
Offline-Modus Konnektor		Im Offline-Modus des *Konnektors* kann keine Verbindung zum *VPN-Konzentrator* aufgebaut werden (z. B. weil die WAN-Schnittstelle nicht angeschlossen oder die Verbindung gestört ist).
Online Certificate Status Protocol	(OCSP)	Ein Internet-Protokoll, das es Clients ermöglicht, den Status von X.509-Zertifikaten bei einem Validierungsdienst abzufragen. Benötigt wird dies bei der Prüfung *digitaler Signaturen*, bei der *Authentisierung* in Kommunikationsprotokollen (z. B. bei SSL) oder für die Versendung verschlüsselter E-Mails, um zu überprüfen, ob die *Zertifikate*, die zur Prüfung der Signatur, zur *Identifizierung* der Kommunikationspartner oder zur *Verschlüsselung* verwendet werden, gesperrt und damit bereits vor Ende ihres regulären Gültigkeitszeitraums ungültig wurden.
Online-Modus Konnektor		Im Online-Modus des *Konnektors* besteht eine VPN-Verbindung zur zentralen *Telematikinfrastruktur* oder es wird davon ausgegangen, dass diese Verbindung jederzeit aufgebaut werden kann.
Onlineprüfung und -aktualisierung		Gemäß § SGB V gesetzlich vorgegebene Prüfung auf Gültigkeit und Aktualität der Versichertenstammdaten, beinhaltet folgende Schritte: · Prüfung der Gültigkeit · Prüfung der Aktualität · Aktualisierung der Daten, wenn Änderungen vorliegen
Online-Rollout		Bezeichnet das Projekt zur Implementation einer *Telematikinfrastruktur*, welche es ermöglicht, die *Versichertenstammdaten* (*VSD*) auf der *eGK* im Feld aktualisieren zu können. Hierzu gehört die Bereitstellung der Netzverbindungen, des *Versichertenstammdatendienstes* (*VSDD*) und die Anbindung der Praxen, Krankenhäuser und Apotheken über *Konnektoren* an die *Telematikinfrastruktur*.
Online-Szenario		Anbindung des Primärsystems des Leistungserbringers an das Netz der Telematikinfrastruktur
Open Systems Interconnection	(OSI)	Kurzform für: Open Systems Interconnection Reference Model. Offenes Schichtenmodell für die Kommunikation informationsverarbeitender *Systeme* bestehend aus 7 Ebenen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Operation Level Agreement	Operational Level Agreement, (OLA)	Ein Operation Level Agreement (OLA) ist eine Vereinbarung mit einem internen Dienstleiter 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.
Organisationsanforderung	organisational requirement	Eine Organisationsanforderung fokussiert auf Belange ohne Bezug zu konkreten *Produkttypen* der gematik, z.B. Projektverfahren (wie Projektplanungsergebnistypen), Testvorgaben (wie [RVO 2009]) und aufbau- bzw. ablauforganisatorische Aspekte.
Organspendeerklärung		Vgl. "*persönliche Erklärungen des Versicherten*"
OSIG-Zertifikat		Das OSIG-Zertifikat identifiziert eine Institution, nicht eine natürliche Person oder eine technische Instanz. Im Regelfall wird es bei der Signatur als Datenbearbeiter von einer bestimmten Einheit oder Organisation des Gesundheitswesens (z. B. „Praxis Bülowbogen") verwendet. Da sich das OSIG-Zertifikat auf eine juristische Person bezieht, führt die Verwendung nach derzeitiger Gesetzeslage nicht zu einer elektronischen fortgeschrittenen oder elektronischen qualifizierten Signatur.
Over the Counter	(OTC)	Mit „Over the Counter"-Präparaten/-Medikamenten werden i.A. nicht verschreibungspflichtige und somit frei verkäufliche pharmazeutische Produkte (z.B. Aspirin) bezeichnet.
P		
Padding		Unter Padding versteht man allgemein das Ergänzen einer Zeichenfolge um zusätzliche Zeichen, damit eine bestimmte Gesamtlänge erreicht wird. Beispielsweise wird der *Hash-Wert* einer Nachricht beim RSA-Verfahren aus Sicherheitsgründen um bestimmte Füllzeichen ergänzt, bevor die Signaturerzeugung durch Exponentiation mit dem *privaten Schlüssel* vorgenommen wird.
Padding Random Number	(PRND)	Bei *Verschlüsselung* mit symmetrischen Blockchiffren und asymmetrischen Chiffren wird der Klartext in Blöcke geteilt und der Algorithmus darauf angewandt. Deshalb muss der letzte Block mit einer Zufallszahl auf die notwendige Größe aufgefüllt werden, wenn der letzte Block nicht lang genug ist.

Begriff	Synonym, (AK)	Definition/Erläuterung
Pairing		Bezeichnet den Prozess der logischen Verknüpfung zweier Komponenten durch den Austausch eindeutiger und geheimer Informationen. Das Pairing zwischen *Konnektor* und eHealth-*Kartenterminal* versetzt den *Konnektor* in die Lage, *Kartenterminals* zu erkennen, die für den Betrieb mit diesem *Konnektor* vorgesehen sind. Das Pairing ermöglicht es einem *Kartenterminal* und einem *Konnektor*, sich nach dem TLS-Verbindungsaufbau gegenseitig zu authentifizieren
Parallelsignatur		Parallelsignaturen sind mehrere voneinander unabhängige Signaturen in der Regel unterschiedlicher kryptographischer Identitäten bezogen auf einen identischen Inhalt.
Patches		Kleinere Korrekturen an ausgelieferter Software ohne darüber hinaus gehende Änderungen an Funktionalität oder Schnittstellen.“
Patient	patient	Natürliche Person, die medizinische Leistungen beansprucht.
Patientenakte, elektronische	(ePA)	Die elektronische Patientenakte soll geeignet sein „Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten“ (§ 291a Abs. 3, Satz 1, Nr. 4 SGB V/GMG) aufzunehmen. Hierbei handelt es sich um eine *freiwillige Anwendung* der eGK.
Patientenfach		Die Gesamtheit aller Patientenfachdaten eines *Versicherten*.
Patientenfach-daten	(PFD)	Einträge in dem Patientenfach des *Versicherten*, die vom *Versicherten* selbst oder für ihn zur Verfügung gestellt werden.
Patientenfach-datendienst	(PFDD)	Alle Einträge in die *Patientenfachdaten* (PFD) werden auf einem *Fachdienst* (PFDD) gespeichert.
Patientenfach-datenmanagement	(PFDM)	Managementsystem zur Verwaltung der Daten im *Patientenfach*
Patienten-information		Die Patienteninformation oder Aufklärung dient als Voraussetzung für eine wirksame Einwilligung zur Nutzung der *freiwilligen Anwendungen* der eGK. Die Patienteninformation muss objektiv und in einer für den Patienten verständlichen Form erfolgen.
Patienten-quittung		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 *Leistungserbringers*.
Patientenverfügung		Vgl. “*persönliche Erklärungen des Versicherten*”
Payload		Nutzlast an Daten, die durch ein Protokoll oder eine Nachricht transportiert wird.

Begriff	Synonym, (AK)	Definition/Erläuterung
Perform Security Operation	(PSO)	Berechnung der kryptographischen Prüfsumme bei zu verschlüsselnden Daten
Performance Management		Das Performance Management umfasst die beiden Prozesse *Availability Management* und *Capacity Management*.
Performance-Test		Der Performancetest (im Zusammenhang eines Leistungstests) hat zum Ziel, die Komponente und Systeme im erlaubten Grenzbereich auf Zuverlässigkeit zu testen (sind Performance- und Massentest bereits im Grenzbereich durchgeführt, ist der Lasttest für diese Prüfziele bereits enthalten). Dazu wird das Normalverhalten auch für folgende Situationen getestet: · Ausfall- von Hardware oder Softwarekomponenten mit denen das System kommuniziert · Betrieb mit der maximalen, gleichzeitigen Anzahl von kommunizierenden Web-Services (n Konnektoren, n Fachdienste) bzw. mit der maximalen gleichzeitigen Anzahl von parallelen Nutzern
Performanz	Performance	Als Performanz wird die Leistungsfähigkeit eines *Systemes* bezeichnet. In der gematik wird die Performanz der *Telematikinfrastruktur* anhand der Antwortzeiten von *Komponenten* und *Fachanwendungen* auf Anfragen beurteilt. Es wird unterschieden zwischen „wahrgenommene Performanz“ und „technischer Performanz“. Die wahrgenommene Performanz ist für den *Anwender* entscheidend, da sie die tatsächliche Wartezeit des *Anwenders* widerspiegelt. Hierbei werden z.B. auch Parallelisierungen im Prozess berücksichtigt. Die „technische Performanz“ misst die tatsächliche Leistungsfähigkeit der technischen *Komponenten* ohne Nutzerinteraktion.
Perimetergrenze		Bei einer Perimetergrenze handelt es sich um einen Begriff aus der Informationstechnologie. Die Perimetergrenze separiert ein Netzwerk in mehrere Teilsegmente. Die Absicherung von Informations- und Kontrollflüssen über die Segmentgrenzen, erfolgt durch Firewalls.
Personal Identification Number	(PIN)	Eine PIN ist eine in der Regel vier- bis achtstellige persönliche Geheimzahl, welche zur *Authentifizierung* ihres Inhabers bei der Nutzung elektronischer *Anwendungen* genutzt wird. So kann z.B. über eine PIN eine *Signaturerstellungseinheit* vor unberechtigtem Zugriff geschützt werden.
Personal Security Environment	(PSE)	Ein PSE ist ein Aufbewahrungsmedium für *private Schlüssel* und vertrauenswürdige Zertifikate. 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 Smart Card, realisiert sein.
Personal Unblocking Key	(PUK)	Die PUK ist ein persönlicher Entsperrungsschlüssel, der es erlaubt, ein durch PIN geschütztes Gerät nach mehrmaliger Falscheingabe zu entsperren und eine neue PIN zuzuordnen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Personalisierung	personalization	Vorgang der Zuordnung einer Karte zu einer Person. Dabei werden die optische Personalisierung (zum Beispiel Hochprägung, Lasergravur) und die elektrische Personalisierung (Laden der personenbezogenen Daten in den Speicher der *Chipkarte*) unterschieden.
persönliche Erklärungen des Versicherten		Die persönlichen Erklärungen sind Hinweise auf Willenserklärungen des Patienten im Kontext von Erklärungen zur Organ- und/oder Gewebespende, Vorsorgevollmacht und Patientenverfügung. Mit einem Organspendeausweis kann das Einverständnis zur Organ- und Gewebespende entweder generell oder auf bestimmte Organe oder Gewebe beschränkt erteilt oder einer Organ- und Gewebespende widersprochen werden. Darüber hinaus kann auf dem Organspendeausweis eine Person benannt werden, die im Todesfall benachrichtigt werden soll. Der Organspendeausweis wird an keiner offiziellen Stelle registriert oder hinterlegt; es ist sinnvoll, den Ausweis bei den Personalpapieren mit sich zu tragen. Hat sich die Einstellung zur Organ- und Gewebespende geändert, muss lediglich die alte Erklärung vernichtet und ein neuer Ausweis ausgefüllt werden. Mit der Vorsorgevollmacht wird vom Patienten selbst eine Vertrauensperson für den Fall seiner Geschäfts- und/oder Einwilligungsunfähigkeit für bestimmte Bereiche bevollmächtigt, z. B. für die gesundheitlichen Angelegenheiten. Der Patient kann eine Patientenverfügung (im Sinne der Definition des § 1901a Abs. 1 Satz 1 BGB) verfassen, mit der er selbst in bestimmte ärztliche Maßnahmen, die nicht unmittelbar bevorstehen, sondern erst in Zukunft erforderlich werden können, im Vorhinein einwilligt oder diese untersagt. (Quelle: Arbeitskonzept_BÄK)
Pharmazentralnummer	(PZN)	Bundeseinheitlicher Identifikationsschlüssel zur Kodierung von Arzneimitteln und Apothekenprodukten, die eine *Identifizierung* nach Warenzeichen, Wirkstoffstärken, Darreichungsform, Packungsgröße und pharmazeutischem Hersteller ermöglicht.
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: „Die Sekunde ist das 9 192 631 770-fache der Periodendauer der dem Übergang zwischen den beiden Hyperfeinstrukturniveaus des Grundzustandes von Atomen des Nuklids 133CS entsprechenden Strahlung.“ Die PTB verfügt über verschiedene Cäsium- und Cäsium-Fontänen Uhren.

Begriff	Synonym, (AK)	Definition/Erläuterung
Pilotbetrieb		Der Pilotbetrieb ist Teil der Erprobungsphase, in dem für eine größere Anzahl von Anwendern neue Funktionen bereit gestellt werden, die sie im gewohnten Umfeld und ohne besondere Vorkenntnisse in Anspruch nehmen. Ziel des Pilotbetriebs ist die Untersuchung des Betriebsverhaltens (z.B. Wartung) und Lastverhaltens (z.B. Antwortzeitverhalten und Stabilität) der neue Funktionen und der damit verbundenen Infrastruktur zu untersuchen. Voraussetzung für den Pilotbetrieb sind stabile Entwicklungen und Umsetzungen, deren Reife in Tests zuvor nachgewiesen werden konnten. Der Pilotbetrieb legt nicht den Schwerpunkt auf die Fehlerermittlung, wie z.B. im Feldtest noch teilweise vorgesehen, sondern soll Erkenntnisse zur Stabilität und der Betreibbarkeit unter realen Bedingungen liefern. Trotzdem können Erkenntnisse aus der Pilotbetriebsphase dazu führen, dass Anpassungen an Komponenten, Diensten und Anwendungen notwendig sind.
Pilotierung		Als Pilotierung wird die QS-Phase verstanden, in der erstmalig mit Echtdaten 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 Pad		Das PIN Pad ist eine Spezialtastatur zur sicheren Eingabe der unterschiedlichen PINs oder PUKs an einem *eHealth-Kartenterminal* in der *Telematikinfrastruktur*.
PIN.CH	PIN.Card Holder, *Praxis-PIN*	Diese PIN wendet der *Versicherte* an, um sich bei Inanspruchnahme medizinischer *Leistungen* über die *Telematikinfrastruktur* entweder explizit zu authentisieren oder jemand anderen für Zugriffe zu autorisieren. In technischen Dokumenten (eGK-Spezifikation) wird „PIN.CH“ verwendet.
PIN.home	*Privat-PIN*	Diese PIN kann der *Versicherte* in seiner häuslichen Umgebung nutzen, um genau definierte Geschäftsvorfälle in der *Telematikinfrastruktur* z. B. auf seinem PC durchzuführen. In technischen Dokumenten (eGK-Spezifikation) als „PIN.home“ bezeichnet.
PIN.QES	*Signatur-PIN*	Diese PIN wenden *Akteure* im Rahmen der *Telematikinfrastruktur* an, wenn sie *elektronische Signaturen* zur Durchführung von Geschäftsvorfällen benötigen. In technischen Dokumenten (eGK-Spezifikation) wird „PIN.QES“ verwendet.
Point	(pt)	Maß für die Größe einer Schrift. Für die eGK bezieht sich die Festlegung auf das DTP-Punkt-System (DTP von: Desktop Publishing), gelegentlich auch PostScript-Punkt genannt. Hierbei entspricht 1 pt: 0,3527 mm
Point-to-point Protocol	(PPP)	Das Point-to-point Protocol erlaubt es, verschiedene Protokolle über eine Punkt-zu-Punkt-Verbindung über Wählleitungen oder Festverbindungen zu übertragen.
Policy		Fachbegriff für eine *Richtlinie*

Begriff	Synonym, (AK)	Definition/Erläuterung
PPP over Ethernet	(PPPoE)	Protokoll zu Verwendung des PPP-Protokolls über Ethernet-Verbindungen.
Praxis PIN	PIN.CH	Diese PIN wendet der *Versicherte* an, um bei Inanspruchnahme medizinischer Leistung über die *Telematikinfrastruktur* sich entweder explizit zu authentisieren oder jemand anderen für Zugriffe zu autorisieren. In technischen Dokumenten (eGK-Spezifikation) wird „PIN.CH“ verwendet.
Praxis PUK	PUK.CH, PUK Card Holder	Diese PUK wendet der *Versicherte* an, um PIN-Änderungen oder das Zurücksetzen des Fehlbedienungszählers der PIN durchzuführen. Zugehörig zum *Praxis PIN*.
Praxisgemeinschaft		Kooperationsform von Vertragsärzten in Form eines Zusammenschlusses von zwei oder mehreren *Ärzten* zur Ausübung der Tätigkeit in gemeinsamen Praxisräumen. Im Gegensatz zur Gemeinschaftspraxis oder zum Medizinischen Versorgungszentrum wird die ärztliche Tätigkeit getrennt ausgeübt und abgerechnet. Es handelt sich also um mehrere rechtlich selbstständige Arztpraxen in gemeinsam betriebenen Räumen.
Primärsystem	(PSS)	Ein IT-System, das bei einem *Leistungserbringer* eingesetzt wird – z.B. eine Praxisverwaltungssoftware (PVS), ein Krankenhausinformationssystem (KIS) oder eine Apothekensoftware (AVS) – und sich unter dessen administrativer Hoheit befindet.
Primärsystemschnittstelle		Über diese vom *Konnektor* angebotene SOAP-Schnittstelle können *Primärsysteme* einerseits die *Fachanwendungen* der *Telematikinfrastruktur*, andererseits aber auch Funktionen der Basisdienste des *Konnektors* als so genannte Basisanwendungen aufrufen. Die cetp-Schnittstelle ist ebenfalls Bestandteil der PS-Schnittstelle. Die Primärsystemschnittstelle ist ein *Produkttyp*.
Privat PIN	PIN.home	Diesen PIN kann der Versicherte in seiner häuslichen Umgebung nutzen, um genau definierte Geschäftsvorfälle in der *Telematikinfrastruktur* z. B. auf seinem PC durchzuführen. In technischen Dokumenten (eGK-Spezifikation) als „PIN.home“ bezeichnet.
Privat PUK	PUK.home	Diese PUK wendet der *Versicherte* an, um PIN-Änderungen oder das Zurücksetzen des Fehlbedienungszählers der PIN durchzuführen. Zugehörig zum *Privat PIN*.
Probes		Testanfragen zur Prüfung von Diensten in der Telematikinfrastruktur
Problem		Begriff aus *ITIL*. Zusammenfassende Beschreibung von einem oder mehreren *Incidents*, deren Ursache unbekannt ist.

Begriff	Synonym, (AK)	Definition/Erläuterung
Problem Management		ITIL-basierter *Prozess*, der *Incidents* analysiert, um ihre Ursachen zu identifizieren. Aufgabe des Problem Management ist es ebenfalls, Workarounds zu erarbeiten und ggf. NfC zur Ursachenbehebung an das *Change Management* zu stellen. Zielsetzung des *Prozesses* ist die Vermeidung zukünftiger *Incidents*.
Produkt		Ein Produkt ist das konkrete Ergebnis eines geregelten Herstellungsprozesses auf der Grundlage einer spezifischen Vorgabe. Das Produkt der gematik ist die Spezifikation der Telematikinfrastruktur, Teilprodukte der gematik sind die Spezifikationen der Komponenten, Dienste und Verfahrensregelungen zur TI. Die Teilprodukte bilden gleichzeitig die Grundlage für die Zulassungsobjekte. Die aus diesen gematik-Produkten entwickelten Realisierungen der Hersteller und Betreiber sind ihrerseits ebenfalls Produkte. Sie setzen die an einen Produkttyp gestellten Anforderungen um und sind diesbezüglich testbar bzw. prüfbar. Wenn in den Spezifikationen und Verfahrensregelungen der gematik von Produkten oder Produkttypen die Rede ist, so bezieht sich das jeweils auf die Realisierungen der Hersteller und Betreiber. Dienstleistungen der gematik werden nicht als Produkte bezeichnet, sondern generell als Dienstleistung.
Produktbaustein		Wenn eine technische Zulieferung für die *Telematikinfrastruktur* alle Eigenschaften eines *Produktes* erfüllt, jedoch mit der Ausnahme, dass die *Anforderungen* an den *Produkttypen* nur teilweise umgesetzt werden, da für den Einsatz in der *Telematikinfrastruktur* noch dastere *Komponenten* ergänzt werden, dann heißt diese Zulieferung ein Produktbaustein. Zum Beispiel kann ein *Hersteller* einen *Netzkonnektor* (Produktbaustein) als eigenständigen Baustein entwickeln, der durch die gematik auch eigenständig testbar ist. Ein *Produkt* (*Einboxkonnektor*) würde aber erst entstehen, wenn jemand diesen Produktbaustein mit einem *Anwendungskonnektor* verbindet. Produktbausteine werden nicht zugelassen, da sie eigenständig nicht in der *Telematikinfrastruktur* eingesetzt werden können. Ihre Definition dient der Optimierung von Tests und der Förderung der Zusammenarbeit der Produkthersteller.

Begriff	Synonym, (AK)	Definition/Erläuterung
Produktinstanz		Eine Produktinstanz ist ein konkretes Exemplar genau eines *Produkts*. Dabei kann es sich sowohl um einen physisch greifbaren Gegenstand – etwa eine *Chipkarte* – als auch um eine Dienstinstanz handeln, wobei letztere mehrere Server und ggf. auch redundante Lokationen umfassen kann. Produktinstanzen haben insbesondere die Eigenschaften: • Eine Produktinstanz repräsentiert einen eindeutigen Entwicklungsstand in einer Version des Herstellers (und damit eines Produkttyps in einer Version gemäß gematik-Vorgabe). • Eine Produktinstanz hat einen konkreten (ggf. verteilten) Standort und Betriebsverantwortlichen. Sie ist gekennzeichnet durch genau eine Produktversionsnummer und genau eine Produkttypversionsnummer. Produktinstanzen werden im Rahmen des *Betriebs* ihrer Einsatzumgebung gemanaged (d.h. z.B. für dezentrale *Komponenten* durch den Betriebsverantwortlichen der Umgebung des betroffenen *Leistungserbringers* oder *Kostenträgers*).
Produktions-referenz-umgebung	(PRU)	Bildet die identische Funktionalität der PU ab, insbesondere hinsichtlich des verwendeten *Releasestandes*, hat aber eine angepasst kleinere Skalierung. Die PRU dient hauptsächlich dem Nachstellen von Fehlerbildern aus der PU zur Problem- oder Fehlerbehebung. Aus Gründen des *Datenschutzes* und der Sicherheit werden hier nur Testdaten verwendet.
Produktions-testumgebung	(PTU)	Ist eine Testumgebung, die die Funktionalität der PU nachbildet. Die Skalierung ist den Testzwecken angepasst. Unterschiede zur PU bestehen insbesondere durch einen möglichen anderen *Releasestand*. Die PTU dient dem Testen von neuen *Releases* oder *Komponenten* zur Minimierung bzw. Vermeidung von Schadensrisiken bei Einbringen in die PU. Aus Gründen des *Datenschutzes* und Sicherheit werden nur Testdaten verwendet.
Produktions-umgebung	(PU)	Umgebung für den *Wirkbetrieb* der *Telematikinfrastruktur*, die u.a. die nach § 291a SGB V geforderten *Anwendungen* den Nutzern der *Telematikinfrastruktur* bereitstellt. In ihr werden ausschließlich Echtdaten verarbeitet.
Produktivphase		Die Produktivphase der TI ist die finale Phase des Wirkbetriebs, in der allen Anwendern die geplanten Anwendungen zur Verfügung gestellt werden und für die der vollständige uneingeschränkte Betrieb vorgesehen ist. Alle Komponenten und Dienste der TI und Fachanwendungen müssen in der Produktivphase vollständig zugelassen sein.
Produktiv-umgebung		Oberbegriff für die drei getrennten *Betriebsumgebungen*: • *Produktionsumgebung* (PU) • *Produktionsreferenzumgebung* (PRU) • *Produktionstestumgebung (PTU)*

Begriff	Synonym, (AK)	Definition/Erläuterung
Produkt-komponente		Die Produktkomponente beschreibt einen fachlichen bzw. funktionalen Bestandteil des Produktes, für den Service Levels festgelegt aber auch Monitoring-Daten erhoben werden können. Der *Broker* besteht unter anderem aus den Komponenten „Broker-ServiceS I.e.S“, „Trusted Service“, „MMS“, etc.
Produkttyp	(ProdT)	Ein Produkttyp beschreibt eine Gruppe gleichartiger *Produkte*, die von verschiedenen Unternehmen hergestellt bzw. bereitgestellt werden. Die Produkte eines Produkttyps decken den gleichen Funktionsbereich auf der Basis normativer Vorgaben ab und unterscheiden sich lediglich in ihrer Ausprägung. In der *Telematikinfrastruktur* werden Produkttypen • konzeptionell beschrieben und versioniert (normative Vorgaben, im Wesentlichen durch die gematik), • für die Infrastruktur konkret realisiert und • in der Regel als eine Einheit (d.h. von einem *Hersteller/Betreiber* verantwortet) umgesetzt. Jede Realisierung, die in diesem Rahmen bleibt, ist eine mögliche Realisierung des Produkttyps. Die Gesamtarchitektur der gematik [gemGesArch] legt fest, aus welchen Produkttypen die *Telematikinfrastruktur* besteht, die *Spezifikationen* definieren darauf basierend die Eigenschaften der Produkttypen.
Produkttyp-steckbrief	(PTStB)	Ein Produkttypsteckbrief (PTStB) ist ein Dokument, welches verbindlich eine Version eines *Produkttyps* (Produkttypversion) definiert. Dazu werden für die Produkttypversion u.a. folgende Festlegungen getroffen: • Zugrunde liegender Produkttyp und Produkttypversionsnummer • Liste von Spezifikationsdokumenten die normative Vorgaben zur technischen Realisierung von Produkten basierend auf der Produkttypversion enthalten. • Ggf. zusätzliche übergreifende normative Vorgaben für die Produkttypversion Produkttypsteckbriefe werden von der gematik veröffentlicht und dienen *Herstellern*, *Providern* und *Betreibern* als Basis für die Entwicklung von *Produkten*, die sich konform zu den Vorgaben der gematik verhalten. Für *Produkte* mit Zulassungsrelevanz dienen sie auch als eine Grundlage für die Zulassungsprüfung. Für jeden *Releasestand* definiert die gematik die Menge alle gültigen Produkttypversionen.
Professionelle endnutzernahe Dienstleister	(PED)	Dienstleister im Auftrag der *Leistungserbringer*, der für *Leistungserbringer* Dienste in *dezentralen Komponenten* betreibt.

Begriff	Synonym, (AK)	Definition/Erläuterung
Profilbildung		Eine Zusammenführung von getrennten und zu verschiedenen Zwecken erhobenen personenbezogenen oder –beziehbaren Daten und deren zweckfremde Verknüpfung, Verarbeitung oder Nutzung, die eine Registrierung und Katalogisierung der Persönlichkeit des Betroffenen ermöglicht und einen vollständigen bzw. auf einen Zweck bezogenen Überblick über Merkmale, das Verhalten oder die Lebensgewohnheiten des Betroffenen erlaubt.
Proof of Concept	*(PoC)*	Bei dem *Proof of Concept* handelt es sich um eine QS-Maßnahme, die das Ziel hat, durch eine prototypenhafte Entwicklung, die Machbarkeit eines Konzeptes zur Risikominimierung nachzuweisen. Dabei wird nicht die Gesamtheit aller geforderten Funktionen realisiert sondern der Fokus liegt auf den technisch innovativen und schwierigen Details.
Protection Profiles	*Schutzprofile*	*siehe dort*
Protocol Parameter Selection	(PPS)	Die Art eines ausgewählten Protokolls wird in einem Parameter, einem so genannten Protocol Parameter Selection codiert.
Protokollierung		In der *Telematikinfrastruktur* versteht man unter „Protokollierung“ sowohl das fachliche (*Audit*), als auch das technische Protokollieren (*Logging*) von Daten.
Provider	technischer Provider	Provider stellen einen *Dienst* im Auftrag eines *Betreibers* bereit. Sie sind gegenüber den *Betreibern* verantwortlich für die Einhaltung der definierten Betriebs- und Service Level. Provider beantragen eine *Zulassung* und erhalten von der gematik nach erfolgreicher Prüfung eine Dienstezulassung gemäß §291a 1b, z. B. eines *Fachdienstes*; sie können als mandantenfähige Provider auch für mehrere *Betreiber* den *Fachdienst* betreiben.
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 gerichteten Ablauf von Aktivitäten. 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).
Prüfungsnachweis		Datensatz, der zum Nachweis einer durchgeführten Onlineprüfung und -aktualisierung auf die eGK gespeichert und dem PVS übergeben wird.

Begriff	Synonym, (AK)	Definition/Erläuterung
Prüfvorschrift	(Pvo)	In einer Prüfvorschrift werden die *Anforderungen* an ein Prüfobjekt zusammengestellt, die zulassungs- oder abnahmerelevant sind. Die Pvo fasst die *Blattanforderungen* aus *Fachkonzept*, *Facharchitektur* und Spezifikationsdokumenten, bei betrieblichen Leistungen auch *Anforderungen* aus Leistungsbeschreibungen und SLAs zusammen. Sie ist die Grundlage für das Testdesign. Prüfvorschriften sind Teil des *Zulassungsverfahrens*.
Pseudonymisierung		Pseudonymisierung gemäß § 3 Abs. 6a BDSG: Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren. Re-Identifizierungsrisiken können sich aus dem Verfahren der Pseudonymgenerierung und / oder dem Umfang der Datensätze ergeben.
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)
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.
Public Key Infrastruktur	(PKI)	Eine PKI ist eine technische und organisatorische Infrastruktur, die es ermöglicht, kryptographische Schlüsselpaare (*private Schlüssel* in Form von PSEs und *öffentliche Schlüssel* in Form von *Zertifikaten*) auszurollen und zu verwalten. Zu den wesentlichen Kernkomponenten einer PKI zählen die *Registrierungsinstanz*, die *Zertifizierungsinstanz* und der *Verzeichnisdienst*. Unter Umständen umfasst eine PKI auch einen *Zeitstempeldienst* und *Attributbestätigungsinstanzen*.
Public Key Kryptographie		Bei der Public Key Kryptographie kommen für die *Verschlüsselung* und für die *Entschlüsselung* unterschiedliche Schlüssel zum Einsatz. Die beiden Schlüssel werden als Paar genutzt. Ein Schlüssel dieses Paares muss geheim gehalten werden und wird daher als *privater Schlüssel* bezeichnet. Der andere Schlüssel, der nicht geheim gehalten werden muss, wird auch *öffentlicher Schlüssel* genannt. Aufgrund der Ungleichheit der Schlüssel wird dieses Verfahren auch als asymmetrische *Verschlüsselung* bezeichnet.
Public Key Kryptosystem		Public-Key-Kryptosysteme verwenden asymmetrische Verschlüsselungsalgorithmen.
Public Key Zertifikat		Ein Public-Key-Zertifikat ist ein *Zertifikat*, das insbesondere den Namen des Zertifikatsinhabers und den *öffentlichen Schlüssel* enthält.

Begriff	Synonym, (AK)	Definition/Erläuterung
Pufferüberlauf	Bufferoverflow	Häufigste Sicherheitslücke in aktueller Software, die sich dazu eignet über Netzwerk unautorisiert die vollständige Kontrolle über Computersysteme zu erlangen oder deren *Verfügbarkeit* 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.
Q		
Quittung der Anforderungs-meldung	receipt	Schriftlich formalisierte Darstellung der Quittung des Eingangs einer *Anforderungsmeldung*. Sie gibt dem Anforderungssteller die Sicherheit, dass die *Anforderungs-meldung* in der gematik im Anforderungsmanagement eingegangen ist.
R		
Rahmen-architektur		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 *Service Level Agreements* (SLA) definiert.
Reaktionszeit		Eine Reaktionszeit beschreibt die Zeitspanne zwischen dem Eintreten eines Ereignisses und einer dadurch ausgelösten Reaktion. Reaktionszeiten für Systeme und Dienstleistungen der Telematikinfrastruktur sind u.a. in den jeweiligen Leistungsbeschreibungen definiert.
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.
Rechte-verwaltung	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 *Identität* des Benutzers/Subjekts.
Rechts-sicherheit		Rechtssicherheit wird erreicht, wenn der jederzeitige Nachweis der Einhaltung der relevanten Gesetze möglich ist.

Begriff	Synonym, (AK)	Definition/Erläuterung
Record Discovery Token	(RDT)	Das Record Discovery Token (RDT) ist wie das Access Right Instantiation Token (ARIT) ebenfalls ein eFA-Token (Offline-Token). Es dient im Gegensatz zum ARIT jedoch nicht der Erweiterung von Berechtigungen einer Fallakte. Vielmehr erleichtert es bereits berechtigten Leistungserbringern das Auffinden einer spezifischen Fallakte. Das RDT kann als Barcode auf Papier gedruckt (heutiges Modell) oder zukünftig auch direkt auf der eGK des Patienten gespeichert werden.
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. Im Sinne der Produktionsreferenzumgebung stehen zusätzlich die Aspekte der Fehlernachstellung bzw. Änderungstestung im Raum.
Regelbetrieb		Der Regelbetrieb ist die Phase, in welcher ein *System* oder Prozess seiner Bestimmung entsprechend genutzt wird. (siehe auch *Wirkbetrieb*)
Registered Application Provider Identifier	(RID)	Die RID ist der registrierte Bestandteil eines Application Identifiers (AID) zur Gewährleistung einer weltweit eindeutigen Namensvergabe für *Chipkarten-Anwendungen.*
Registrierung		Registrierung bezeichnet die Aufnahme eines Registrierungsgegenstandes in einem geordneten Verzeichnis verbunden mit der Feststellung definierter Rechte und Pflichten. Registriert werden können Organisationen und Personen aber auch *Dienste* und *Anwendungen*. Die Registrierung kann an Voraussetzungen wie z.B. eine Selbstverpflichtung gebunden sein, eine Auditierung oder Testung findet nicht statt. In der *Telematikinfrastruktur* werden z.B. Zertifikatsherausgeber registriert.
Registrierungsinstanz	Registration Authority, (RA)	Eine Registrierungsinstanz ist der Bestandteil einer PKI, bei dem ein Benutzer ein *Zertifikat* beantragen und ggf. dessen Sperrung veranlassen kann. Im Zuge des erstmaligen Registrierungsprozesses werden die *Identität* des Antragstellers und möglicherweise zusätzliche Attribute überprüft, so dass die Korrektheit der Angaben im *Zertifikat* gewährleistet ist.
Registrierungsstelle	Registration Authority, (RA)	Vertrauenswürdige Stelle, die die *Identität* eines Antragstellers für *Zertifikate* nach festgelegten Regeln prüft und die Daten an den ZDA weiterleitet

Begriff	Synonym, (AK)	Definition/Erläuterung
Regressions-test	regression test	Unter einem Regressionstest versteht man die wiederholte Ausführung von bereits erfolgreich getesteten Testfällen. Dies ist die Basis für entwicklungsbegleitende Tests, Projekte die ein iterativ, inkrementelles Vorgehensmodell umsetzen oder bei der Entwicklung eines neuen *Releases* oder Version einer Software. Mit der erneuten Ausführung der Testfälle soll die Fehlerfreiheit durch Änderungen nachgewiesen und unerwünschte Nebeneffekte durch Erweiterungen einer Software vermieden werden. Für die Durchführung der Testfälle ist entscheidend, dass die Vorbedingungen für den Testfall vor jeder Ausführung sichergestellt werden. Dies bedarf unter Umständen weiterer „Testfälle“, die nur dazu dienen einen entsprechenden Zustand im Testobjekt wiederherzustellen (bspw. Löschen eines Artikels in den Stammdaten). Um den Aufwand für die Testdurchführung zu minimieren werden die Testfälle eines Regressionstest meist automatisiert.
Release		Zusammenfassung mehrerer Changes zu einem gesamt auszurollenden Paket.
Release-definition	release definition	Beschreibung des geplanten Inhaltes mit Motivation durch *Auftragsanforderungen* jedoch ohne konzeptionelle Lösungsansätze, der zu einem *Release* führen soll.
Release-management	(RM)	ITIL-basierter *Prozess*, der für die operative Ausführung von Changes, die durch das *Change Management* beauftragt wurden, verantwortlich ist. Das Releasemanagement hat eine ganzheitliche Sicht auf die Veränderungen an einem IT-Service.
Releasepolicy		Gesammelte Regeln und Festlegungen, die alle Verfahren, Prozesse und Systeme des gesteuerten Einbringens von Releases (als Bündelung von Changes) in die Telematikinfrastruktur beschreiben.
Releasestand		Ein Releasestand bezieht sich immer auf ein *Release* und bezeichnet den Entwicklungsstand aller für das *Release* gültigen Vorgaben zu einem bestimmten Zeitpunkt. Der Releasestand wird in einer Dokumentenlandkarte bekanntgegeben. *Der* Releasestand wird durch eine innerhalb des Releases eindeutige Releasestandsversion in Form von „Vn.m.p“ gekennzeichnet. Dabei kennzeichnen die drei Stellen (n.m.p) die Version in der Fortschreibung der Dokumentenlandkarte in der Umsetzungs- und Wirkbetriebsphase.
Remote-PIN		Die Remote-PIN ist ein sicherer Mechanismus der es ermöglicht, für eine Karte, die in Kartenterminal A steckt, am Kartenterminal B eine PIN einzugeben.
Reporting		Das Reporting dient der Datenspeicherung, und –aufbereitung für den Zweck rückwirkend Aussagen über *Dienste*, *Services* und *Prozesse* machen zu können. Daraus abgeleitet können auch Trendanalysen erstellt werden.

Begriff	Synonym, (AK)	Definition/Erläuterung
Request for Change	(RfC)	ITIL-basierter Begriff zur formalisierten vollständigen Beschreibung eines Änderungsbedarfs. In der *Telematikinfrastruktur* wird der Begriff CR (*Change Request*) verwendet.
Request for Comment	(RFC)	Mit RFC werden „zur Diskussion“ gestellte organisatorische oder technische Dokumenten zum Internet bezeichnet. Hierbei handelt es sich um Dokumente, die sich aber durch allgemeine Akzeptanz und Gebrauch zum Standard entwickelt haben. http://www.ietf.org/rfc
Resolver		Programmsoftware, die – getrieben von Client Anfragen – Informationen aus dem Datenbestand von Name Servern extrahiert und an das anfragende Clientsystem zurückgibt.
Reverse Proxy		Ein Reverse Proxy dient wie ein Proxy 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.
Revisionsinformation	Revisionsnummer	Die Revisionsinformation stellt einen eindeutigen Bezeichner des Arbeitsstandes eines Dokumentes der gematik dar. Im Unterschied zur (logischen) Versionsnummer wird die Revisionsinformation bei jedem einzelnen Bearbeitungsschritt hochgezählt. Die Revisionsinformation stellt dabei sicher, dass verschiedene Arbeitsstände eines Dokumentes auch durch verschiedene Bezeichner eindeutig identifizierbar sind.
Revocation Status		Wird im Zusammenhang mit Digitalen *Zertifikaten* verwendet. Gibt an ob ein *Zertifikat* zu einem gegebenen Zeitpunkt gültig war oder ob die ausstellende Instanz dieses *Zertifikat* zurückgezogen hatte.
Rezept	prescription	Transportmittel zur Übermittlung ärztlicher Verordnungen über Arzneimittel, Heil- und Hilfsmittel und Therapien in der heutigen Form als Papierrezept, welches bis zu drei Verordnungen enthält, vom Arzt oder Zahnarzt ausgestellt wird und über den *Patienten* in der Apotheke oder *Versandapotheke* eingelöst wird. Unterformen: BtM-Rezept, Grünes Rezept, GKV-Rezept oder Privatrezept.
Rezept, elektronisches		verwendeter Begriff: *eVerordnung* (schließt das elektronische Rezept ein)
Richtlinie	Policy	Eine Richtlinie ist eine Handlungsvorschrift mit bindendem Charakter, aber nicht gesetzlicher Natur. Eine Richtlinie wird von einer Organisation ausgegeben, ist daher gesetzlich ermächtigt und hat so einen Geltungsbereich, der z. B. arbeitsrechtlich auch sanktionierbar ist. (Wikipedia)
Risiken, operationale	operational risks	Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und *Systemen* oder infolge externer Ereignisse eintreten.

Begriff	Synonym, (AK)	Definition/Erläuterung
Risiken, strategische	strategic risk	Strategische Risiken sind Gefährdungen der Zielerreichung, die aus den Veränderungen des Umfeldes eines *Systems* resultieren.
Rolle	role	Eine Rolle beschreibt die Verhaltensweise eines *Akteurs* in einer definierten Aufgabenstellung.
Rollout		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-CA		Oberste Zertifizierungsinstanz (CA) in einer Hierarchie einer PKI.
Router		Aktive Netzwerkkomponente, die gleiche oder verschiedene Protokolle zwischen mehreren Netzen mit unterschiedlichen Adressräumen vermittelt.
Routing		Weiterleitung von Paketen (z.B. IP-Paketen) auf der OSI-Schicht 3.
RSA-Algorithmus		Der nach seinen Erfindern (Rivest, Shamir und Adleman) benannte RSA-Algorithmus ist ein asymmetrischer Kryptoalgorithmus, der zur *Verschlüsselung* und zur Realisierung *digitaler Signaturen* verwendet werden kann. Die Sicherheit dieses Verfahrens basiert auf der kryptographischen Annahme, dass das Faktorisierungsproblem für große Zahlen nicht effizient gelöst werden kann.
S		
Schalenmodell		Das Schalenmodell ist ein so genanntes Gültigkeitsmodell für Zertifizierungspfade, bei dem alle *Zertifikate* im Pfad zu einem einheitlichen Prüfzeitpunkt gültig sind. Für *Authentisierungen* wird dabei der aktuelle Zeitpunkt betrachtet und für *elektronische Signaturen* der Erstellungszeitpunkt. Siehe auch *Kettenmodell*.
Schlüssel, geheimer		Geheime Schlüssel werden im Zusammenhang mit symmetrischen Kryptoalgorithmen verwendet. Im Gegensatz zu den bei asymmetrischen Kryptoalgorithmen eingesetzten *privaten Schlüsseln* ist das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt
Schlüssel, öffentlicher	public key, (PK)	Der öffentliche Schlüssel ist ein Bestandteil des Schlüsselpaares bei Public-Key-Kryptographie. Im Gegensatz zu dem *privaten Schlüssel* muss dieser nicht geheim gehalten werden und wird zum Beispiel im entsprechenden *Zertifikat* des Eigentümers verbreitet.
Schlüssel, privater	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 *digitale Signaturen* zu erstellen oder Daten zu entschlüsseln
Schlüssel, symmetrischer		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

Begriff	Synonym, (AK)	Definition/Erläuterung
Schlüsselableitung	derive Key	Dienst des *Schlüsselmanagements* (siehe [ISO 11770]): Der Dienst Schlüsselableitung erstellt eine potentiell große Anzahl von Schlüsseln unter Benutzung eines geheimen Originalschlüssels genannt Ableitungsschlüssel, nicht geheimen veränderlichen Daten und mit einem Transformationsprozess (der nicht immer geheim sein muss). Das Ergebnis dieses *Prozesses* ist der abgeleitete Schlüssel. Der Ableitungsschlüssel erfordert besonderen Schutz. Der Ableitungsprozess MUSS unumkehrbar und nicht-vorhersehbar sein um sicherzustellen, dass die Kompromittierung eines abgeleiteten Schlüssels nicht den Ableitungsschlüssel oder andere abgeleitete Schlüssel kompromittiert.
Schlüsselarchivierung	archive Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Schlüsselarchivierung ist der *Prozess*, Schlüssel nach Ablauf der Nutzung sicher und langfristig zu speichern. Für diesen Dienst ist die *Anwendung* des *Dienstes* "Schlüsselspeicherung" denkbar, es bestehen aber verschiedene *Anforderungen*, so dass auch verschiedene *Implementierungen* denkbar sind. So könnte z. B. die Schlüsselarchivierung offline realisiert werden. Archivierte Schlüssel können noch lange nach dem normalen Gebrauch der Schlüssel benötigt werden, um bestimmte Ansprüche abzuklären
Schlüsselderegistrierung	deregister Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Der Dienst zum Aufheben der Registrierung eines Schlüssels wird von einer Registrierungsinstanz angeboten, die die Verbindung des Schlüssels mit einer Entität aufhebt. Er ist Teil des Schlüssel-Zerstörungsprozesses. Wenn eine Entität die Registrierung eines Schlüssels aufheben lassen will, kontaktiert sie die Registrierungsinstanz.
Schlüsselerzeugung	generate Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Schlüsselerzeugung ist ein Dienst, der aufgerufen wird um auf sicherem Wege Schlüssel für einen bestimmten kryptographischen Algorithmus zu erzeugen. Dies erfordert, dass die Schlüsselerzeugung nicht manipulierbar sein darf und dass die Schlüssel nicht vorhersagbar und in der vorgeschriebenen statistischen Verteilung erzeugt werden müssen. Diese statistischen Verteilungen sind vom verwendeten kryptographischen Schlüssel erzwungen und von geforderten Niveau des kryptographischen Schutzes. Die Erzeugung mancher Schlüssel, z. B. Master-Keys, erfordert besondere Sorgfalt und besonderen Schutz, da die Kenntnis dieser Schlüssel Zugriff auf die verbundenen oder abgeleiteten Schlüssel ermöglicht.
Schlüsselinstallation	install Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Der Dienst Schlüsselinstallation ist immer vor dem Gebrauch eines Schlüssels notwendig. Bei der Schlüsselinstallation wird der Schlüssel in einer Art und Weise eingebracht, die den Schlüssel vor Kompromittierung schützt.
Schlüsselmanagement	Key Management	Verwaltung von Schlüsseln. Bezüglich des Kartensystems ist hier das Schlüsselmanagement für die eGK gemeint.
Schlüsselmanagementsystem	Key Management System	*System* (bzw. eine *Komponente* im gesamten Kartensystem) für das *Schlüsselmanagement*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Schlüsselregistrierung	Register Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Der Dienst Schlüsselregistrierung verbindet einen Schlüssel mit einer Entität. Er wird von einer Registrierungsinstanz angeboten und wird üblicherweise angewandt, wenn symmetrische Kryptographie benutzt wird. Wenn eine Entität einen Schlüssel registrieren lassen will, kontaktiert sie die Registrierungsinstanz. Schlüsselregistrierung beinhaltet eine Registrierungsanforderung und eine Bestätigung dieser Registrierung. Eine Registrierungsinstanz pflegt ein Register von Schlüsseln und die dazugehörigen Informationen in hinreichend sicherer Art und Weise.
Schlüsselspeicherung	Store Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Der Dienst Schlüsselspeicherung bietet sichere Speicherung für Schlüssel im laufenden oder kurz bevorstehenden Gebrauch oder auch für Backup-Schlüssel. Es ist üblicherweise von Vorteil, physikalisch getrennte Schlüsselspeicher vorzusehen. Zum Beispiel sichert ein Schlüsselspeicher die *Vertraulichkeit* und *Integrität* von Schlüsselmaterial oder die Integrität von *öffentlichen Schlüsseln*. Speicherung kann in allen Schlüsselzuständen im Lebenszyklus eines Schlüssels vorkommen.
Schlüsselsuspendierung	Revoke Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Wenn die Kompromittierung eines Schlüssels bekannt ist oder vermutet wird, stellt der Dienst Schlüsselsuspendierung die sichere Deaktivierung des Schlüssels sicher. Der Dienst ist auch für Schlüssel, deren Gültigkeit abgelaufen ist, notwendig. Schlüsselsuspendierung wird auch dann angewandt, wenn sich die Rahmenbedingungen beim Schlüsselinhaber ändern. Nach der Suspendierung kann der Schlüssel nur eingeschränkt benutzt werden (In der Regel nicht mehr um zu verschlüsseln oder zu signieren, aber der Schlüssel darf gebraucht werden um zu entschlüsseln oder zu verifizieren). Der Grad der Suspendierung MUSS genau beschrieben werden, wie auch die Umstände unter denen der Schlüssel wieder aktiviert werden kann. Der Dienst Schlüsselsuspendierung wird kaum bei zertifikatbasierten Schemata angewandt, wo der Lebenszyklus der Schlüssel durch die Gültigkeit der *Zertifikate* geregelt wird.
Schlüsselverteilung	Distribute Key	*Dienst* des *Schlüsselmanagements* (siehe [ISO11770]): Die Schlüsselverteilung ist eine Menge von *Prozessen*, um Schlüsselmanagement-Informationsobjekte (in der Regel Schlüssel) sicher zu autorisierten Entitäten zu verteilen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Schlüsselzerstörung	Destroy Key	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Der Dienst Schlüsselzerstörung bietet einen Prozess an, für die sichere Zerstörung von Schlüssel die nicht mehr gebraucht werden. Zerstörung eines Schlüssels heißt, alle Einträge des Schlüsselmanagement-Informationsobjekts zu löschen, so dass nach der Zerstörung keine Information übrig bleibt um den zerstörten Schlüssel wiederherzustellen. Dies wird gemacht um die Zerstörung aller archivierten Kopien sicherzustellen. Dennoch, bevor archivierte Schlüssel zerstört werden, sollte eine Prüfung gemacht werden um sicherzustellen, dass kein Material das durch diese Schlüssel geschützt wird jemals wieder gebraucht wird. NOTIZ: Es können Schlüssel außerhalb von elektronischen Geräte oder Systemen gespeichert sein. Das erfordert zusätzliche administrative Maßnahmen.
Schnittstellentest		Im Rahmen der *Schnittstellentests* sind die zur *Telematikinfrastruktur* exponierten Schnittstellen Testgegenstand. Dies sind z.B. VSDD, CMS, UFS, VODD.
Schutzbedarf		Der Schutzbedarf ist das Maß, in dem ein Objekt hinsichtlich eines oder mehrerer Schutzziele geschützt werden soll. Die Bestimmung des Schutzbedarfes ist erforderlich, um angemessene Sicherheitsmaßnahmen auswählen zu können.
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.
Schwachstelle	vulnerability	Von einer oder mehreren Bedrohungen ausnutzbare Schwäche eines Wertes oder einer Gruppe von Gütern (Quelle: [ISO/IEC27002]). Erläuterung: Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-*Systems* oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein *System* geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein *System*) anfällig für Bedrohungen (Quelle: [BSI_2005]).
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.
Secure Hash Algorithm	(SHA-1)	Der Secure Hash Algorithm (SHA-1) [FIPS180-2] ist ein von der US-amerikanischen Sicherheitsbehörde NSA entwickelter Hash-Algorithmus, der 160 Bit Hash-Werte produziert.
Secure Interoperable Chip Card Terminal	(SICCT)	Als Secure Interoperable Chip Card Terminals werden *Kartenterminals* bezeichnet, die der zugehörigen *Spezifikation* [SICCT] genügen.

Begriff	Synonym, (AK)	Definition/Erläuterung
Secure Messaging	(SM)	Secure Messaging bezeichnet in der Summe alle Algorithmen, Protokolle und Mechanismen zum Schutz sensitiver Daten bei der Übertragung über eine unsichere Schnittstelle. Im Allgemeinen werden mit SM-Verfahren zur Absicherung der Datenübertragung im Umfeld einer *Chipkarte* bezeichnet.
Secure Signature creation Device	(SSCD)	Ein Secure Signature Creation Device ist ein Hardware-Modul zum vertrauenswürdigen Erstellen von *digitalen Signaturen*. Der *private Schlüssel* 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 SmartCard mit Krpyto-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 Functional Requirement	Sicherheitsanforderungen, (SFR)	Begriff aus der *CommonCriteria* der die Menge der sicherheitstechnischen Funktionen beschreibt, die zur Durchsetzung der Sicherheitsziele des Produktes notwendig sind.
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.
Security Module Anwendungskonnektor	(SM-AK)	Physikalischer Träger der kryptographischen Geheimnisse des *Anwendungskonnektors*, insbesondere zu seiner *Identität*.
Security Module Card Typ A	Arbeitsplatzkarte, auch: Komponentenidentitätskarte (SMC-A)	Die SMC-A ist ein lokaler Schlüsselspeicher für eine fachliche *Identität* in *Kartenterminals*. Zur Vermeidung vieler Zugriffe über ein Netzwerk zu einer SMC-B mit Institutionsidentität erlaubt die in einem *Kartenterminal* hinterlegte SMC-A einen lokalen Zugriff auf die eGK. Die Security Module Card Typ A ist ein *Produkttyp*.
Security Module Card Typ B	Institutionskarte, (SMC-B)	Die SMC-B ist ein Schlüsselspeicher für die *privaten Schlüssel*, die eine Einheit oder Organisation des *Gesundheitswesens* (z.B. Praxis, Apotheke, Krankenhaus) ausweisen. Diese Schlüssel dienen als Ausweis gegenüber der eGK und gegenüber anderen *Komponenten* der TI. Die Security Module Card Typ B ist ein *Produkttyp*.
Security Module Card Typ K	(SMC-K)	Die SMC-K ist eine möglich Bauform des SM-K in Form einer *Chipkarte*. Die Security Module Card Typ K ist ein *Produkttyp*.
Security Module Card Typ KT	(SMC-KT)	Die SMC-KT ist eine mögliche Bauform des SM-KT in Form einer *Chipkarte*. Die Security Module Card Typ KT ist ein *Produkttyp*.

Begriff	Synonym, (AK)	Definition/Erläuterung
Security Module Card Typ RFID	(SMC-RFID)	Die SMC-RFID ist ein personengebundener Schlüsselspeicher zum Auslösen einer *Komfortsignatur*. Die Security Module Card Typ RFID ist ein *Produkttyp*.
Security Module Kartenterminal	(SM-KT)	Physikalischer Träger der kryptographischen Geheimnisse eines *Kartenterminals*
Security Module Konnektor	(SM-K)	Physikalischer Träger der kryptographischen Geheimnisse des *Konnektors*; der Begriff wird verwendet falls SM-NK und SM-AK in einem gemeinsamen physikalischen Modul umgesetzt sind oder *Anforderungen* für beide *Komponenten* gleichermaßen gelten.
Security Module Netzkonnektor	(SM-NK)	Physikalischer Träger der kryptographischen Geheimnisse des *Netzkonnektors*, insbesondere zu seiner *Identität*.
Sektor		Ein Sektor umfasst einen abgrenzbaren Bereich der *Leistungserbringer*, für den eine Spitzenorganisation zuständig ist.
Send Sequence Counter	(SSC)	Ein Mechanismus der zum sicheren Versenden von Nachrichten benutzt wird, wo es keinen eigenen Sicherheitsmechanismus gibt.
Serveranwendung		Die Serveranwendung ist eine spezielle Form einer *Anwendung*.
Service		Ausschnitt aus der von der *Telematikinfrastruktur* angebotenen Funktionalität. Die Funktionalität (Operation(en)) wird über ein Interface aufgerufen. Im Gegensatz zum *Dienst* muss das Interface nicht unbedingt über Netzwerkprotokolle adressiert werden. Beispiel ist die Ticketservice-Komponente des *Konnektors*. Im Sinne der *Gesundheitstelematik* kann ein Service auch eine Prozessunterstützung sein.
Service Consumer Tier		Schicht der *Telematikinfrastruktur*, welche die *Primärsysteme* der *Leistungserbringer* umfasst.
Service Continuity Management	(CtM)	ITIL-basierter Prozess, der gewährleistet, dass 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 Desk	(SD)	Der Service Desk nimmt zentral alle Anfragen und Störungsmeldungen einer Institution entgegen und leitet Sie an den entsprechenden Bearbeiter weiter.

Begriff	Synonym, (AK)	Definition/Erläuterung
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. Der Service Directory Service ist ein Produkttyp.
Service Katalog		Im Service Katalog werden die verfügbaren IT-Services zur Unterstützung der *Geschäftsprozesse* beschrieben. Er enthält u.a. die für den IT-Service zu erbringenden Service Level, ggf. Varianten des IT-Services und stellt dar, welche Bestandteile für die Erbringung des IT-Service relevant sind.
Service Level Agreement	(SLA)	Vereinbarung über die Qualität von IT-Dienstleistungen.
Service Level Management		ITIL-basierter Prozess, der die Qualität der IT-Services fokussiert. Aufgabe ist die Vereinbarung von SLA mit den Nutzern von IT-Services und deren Sicherstellung durch interne Vereinbarungen (OLA) und externe Verträge (UC).
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 Tier		Schicht der *Telematikinfrastruktur*, welche die *Fachdienste* umfasst, in denen *Versicherten-* und *Patientendaten* persistent gespeichert werden.
Servicespezifikation	Service Specification Sheet	Detaillierte technische Beschreibung einer Kundenanforderung (SLR), die als Informationsquelle für die Realisierung des IT-Services dient. (ITIL-basierter Begriff)
ServiceTicket		ServiceTickets werden durch das Berechtigungskonzept der gematik definiert. Im Gegensatz zu *ObjektTickets* enthält ein ServiceTicket immer nur die Referenz zu einem einzigen zugriffsberechtigten *Akteur*. Es kann nur ein ServiceTicket für eine bestimmte Kombination aus *Service*, *Dateneigentümer* und berechtigtem *Akteur* angelegt werden. Die dort hinterlegten Berechtigungsinformationen gelten für alle *medizinischen Datenobjekte* (MDOs) auf diesem Service.
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.

Begriff	Synonym, (AK)	Definition/Erläuterung
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.
Servicezeit		Zeiten, in denen Betriebsaspekte sowie Querschnittsaufgaben umfassend bearbeitet werden. Diese sind im Einzelnen in den Leistungsbeschreibungen definiert.
Sicherheit	Safety, Security	Objektiv ist Sicherheit eine Sachlage, bei der das Risiko nicht größer als ein identifiziertes Grenzrisiko 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.
Sicherheits-(grund)funktion	Security Function	Funktion zur Erfüllung der *Sicherheitsanforderungen* eines IT-Systems, die übergreifende Bedeutung haben. Sie besteht i.d.R. aus mehreren Sicherheitsmechanismen. Eine Sicherheitsgrundfunktion ist z.B. die *Vertraulichkeit* der Datenübertragung.
Sicherheits-analyse		Analyse der IT-Sicherheit durch festgeschriebene Methoden
Sicherheits-anforderung	Security/Safety Requirement	Sicherheitsanforderungen legen fest, gegen welche kritischen Bedrohungen eines IT-Systems bzgl. *Vertraulichkeit, Integrität, Verfügbarkeit* und *Authentizität* 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.

Begriff	Synonym, (AK)	Definition/Erläuterung
Sicherheits-audit	security audit	Es wird geprüft, ob ein *Provider* die Maßnahmen umgesetzt hat, die er in seinem individuellen Sicherheitskonzept beschrieben hat. Dies beinhaltet, ob sicherheitsrelevante Schnittstellen die festgelegten *Sicherheitsanforderungen* bei "ordnungsgemäßer" Nutzung erfüllen und ob sicherheitsrelevante Fehlerzustände erkannt und spezifikationsgemäß protokolliert werden.
Sicherheits-dienst	*Sicherheits-(grund)funktion*	*siehe dort*
Sicherheits-evaluierung		Bei der Sicherheitsevaluierung handelt es sich um einen Nachweis der Sicherheit und Stabilität des Systems (z.B. Konnektor, eHealth-KT). Die Sicherheitsevaluierung ist eine der Voraussetzungen für eine Zulassung.
Sicherheits-kontext		Gesamtheit aller (authentischen) sicherheitsrelevanten Informationen über einen Akteur. Diese Informationen können z. B. im Kontext einer Berechtigungsprüfung verwendet werden. Ein Sicherheitskontext kann u. A. aus Informationen zu ausgewählte Eigenschaften bzw. Attributen (Identität, Rollen, Rechte etc.) des adressierten Akteurs bestehen.
Sicherheits-konzept		Konzept, das die Sicherheit der Systemkomponenten sowie deren sicheren *Betrieb* festlegt
Sicherheits-konzeption		Eine Sicherheitskonzeption ist eine einheitlich strukturierte Vorgehensweise, gemäß der die für die Telematikinfrastruktur verbindlichen Methoden zur Informationssicherheit und zum Datenschutz angewendet werden. Ziel der Sicherheitskonzeption ist das Erreichen und Aufrechterhalten eines angemessenen Schutzniveaus für die Informationswerte in der Telematikinfrastruktur. Die Ergebnisse der Sicherheitskonzeption werden in Sicherheitskonzepten dokumentiert.
Sicherheits-modell	security modell	Formulierung bestimmter Regeln für die Zugriffskontrolle oder allgemein einer umfassenden *Sicherheitspolitik*.
Sicherheits-modul		Ein Sicherheitsmodul ist ein mechanisch und informationstechnisch abgesichertes Bauteil zur Aufbewahrung geheimer Daten und zur sicheren Ausführung kryptografischer Operationen.
Sicherheits-modul, institutionsbezogenes	Institutionsausweis	Ein institutionsbezogenes Sicherheitsmodul ist ein Sicherheitsmodul für eine Institution des Gesundheitswesens, das als Ausweis gegenüber Komponenten der TI dient. Beispiele für Ausprägungen von institutionsbezogenen Sicherheitsmodulen sind die SMC-B für Institutionen der Leistungserbringer und die SMC-KTR für Institutionen der Kostenträger.
Sicherheits-politik		Grundlegende Aussagen bzgl. Der Sicherheit für ein Unternehmen/*System*

Begriff	Synonym, (AK)	Definition/Erläuterung
sicherheits-relevant		(a) Eine *Komponente*/ein *Dienst*/ein *Prozess* ist sicherheitsrelevant, wenn diese/dieser korrekt arbeiten/funktionieren muss, um die *Sicherheit* (des *Systems*) zu gewährleisten. (b) Ein Informationsobjekt ist sicherheitsrelevant, wenn dessen *Vertraulichkeit*, *Integrität*, *Authentizität*, *Verfügbarkeit* oder *Nichtabstreitbarkeit* geschützt werden muss, um die *Sicherheit* (des *Systems*) zu gewährleisten.
Sicherheitstest		Nachweis der sicherheitstechnischen Eigenschaften der Komponenten und des Gesamtsystems Im Rahmen der Sicherheitstests erfolgt eine Überprüfung der geforderten Sicherheitsmaßnahmen für die Telematikinfrastruktur. Dies umfasst den Test des Systemverhaltens bei gezielten Systemabbrüchen und provozierten Ausfällen von Netzknoten. Darüber hinaus wird die Abwehr unerlaubter Eingriffe ins Netz getestet.
sicherstellen		"Sicherstellen" umfasst sowohl die Definition und Umsetzung von Maßnahmen, als auch die Prüfung auf deren Wirksamkeit.
Signatur		siehe *Digitale Signatur*
Signatur, digitale	digital signature	Die digitale Signatur ist auf dem Prinzip der Kryptographie aufgebaut. Es werden *Hash-Werte* verwendet, wodurch die *Integrität* der Daten gesichert und Veränderungen erkennbar werden.
Signatur, einfache elektronische		Elektronische Signatur ohne *Verschlüsselung*. Bsp.: Eingescannte Unterschrift
Signatur, elektronische	(eSign)	Gemäß § 2 Nr.1 SigG [SigG01] sind elektronische Signaturen Daten in elektronischer Form, die der Authentifizierung dienen. Die Bandbreite möglicher Ausprägungen reicht von einer digitalen Abbildung einer handschriftlichen Unterschrift (einfache elektronische Signatur) bis hin zur sehr vertrauenswürdigen qualifizierten elektronischen Signatur (unter Verwendung eines *qualifizierten Zertifikates*).
Signatur, fortgeschrittene elektronische		Eine fortgeschrittene *elektronische Signatur* ist gemäß § 2 Nr. 2 SigG [SigG01] eine *elektronische Signatur* mit besonderen Eigenschaften, durch die zumindest ein grundlegendes Maß an *Authentizität* und *Integrität* sichergestellt werden kann. Anders als bei der *qualifizierten elektronischen Signatur* kann aber eine lediglich fortgeschrittene *elektronische Signatur* nicht die Schriftform gemäß § 126 BGB ersetzen und hat geringere Beweiskraft vor Gericht Beispiel: S/MME mit Verwaltungs-PKI-Zertifikat
Signatur, qualifizierte elektronische	Qualified Electronic Signature; (QES)	Eine qualifizierte elektronische Signatur ist gemäß § 2 Nr. 3 SigG eine *fortgeschrittene elektronische Signatur*, die unter Verwendung einer sicheren *Signaturerstellungseinheit* erzeugt wurde und zum Zeitpunkt der Signaturerstellung auf einem gültigen *qualifizierten Zertifikat* beruht. Durch die qualifizierte elektronische Signatur kann die Schriftform ersetzt und somit auf kostenintensive Papierprozesse verzichtet werden.

Begriff	Synonym, (AK)	Definition/Erläuterung
Signatur-algorithmus		Ein Signaturalgorithmus ist ein asymmetrischer Kryptoalgorithmus, der zur Erzeugung *digitaler Signaturen* verwendet wird. Zu den populärsten Signaturalgorithmen zählen RSA, DAS und ECDSA.
Signaturanwendungskomponente	(SAK)	Signaturanwendungskomponenten sind gemäß § 2 Nr. 11 [SigG01] Software- und Hardwareprodukte, die dazu bestimmt sind, Daten dem *Prozess* der Erzeugung oder Prüfung *qualifizierter elektronischer Signaturen* zuzuführen oder *qualifizierte elektronische Signaturen* zu prüfen oder *qualifizierte Zertifikate* nachzuprüfen und die Ergebnisse anzuzeigen.
Signaturerstellungseinheit		Eine Signaturerstellungseinheit ist eine Hardware oder Software, in der *private Schlüssel*, die zur Erstellung von Signaturen erforderlich sind, wie in einem PSE, aufbewahrt und darüber hinaus auch angewandt werden können. Als Signaturerstellungseinheit kommen Smart Cards, HSMs oder Standard-Rechner-Systeme in Frage, wobei der *private Schlüssel* beispielsweise in einer mittels Passwort verschlüsselter Datei im PKCS #12-Format gespeichert wird. Zur Erstellung von *qualifizierten elektronischen Signaturen* sind sichere Signaturerstellungseinheiten nötig.
Signaturerstellungseinheit, sichere	(SSEE)	Eine sichere Signaturerstellungseinheit ist gemäß § 2 Nr. 10 SigG eine Signaturerstellungseinheit, die den anspruchsvollen *Anforderungen* des Signaturgesetzes, insbesondere § 17 Abs. 1 SigG und § 15 Abs. 1 SigV, genügt.
Signatur-PIN	(PIN.QES)	Diese PIN wenden *Akteure* im Rahmen der *Telematikinfrastruktur* an, wenn sie *elektronische Signaturen* zur Durchführung von Geschäftsvorfällen benötigen. In technischen Dokumenten (eGK-Spezifikation) wird „PIN.QES“ verwendet.
Signatur-PUK		Eine zur *Signatur-PIN* gehörige PUK wird als Signatur-PUK bezeichnet.
Signaturverordnung	(SigV)	Die Signaturverordnung ergänzt das Signaturgesetz um Einzelregelungen zu den *Anforderungen* an die *Zertifizierungsdiensteanbieter* sowie an die bei der Zertifikats- und Signaturerstellung einzusetzenden *Produkte* und Verfahren. Sie konkretisiert darüber hinaus die Kostenregelung in § 22 SigG. In der Anlage 1 macht sie zudem detaillierte Vorgaben für die Prüfung von *Produkten* für *qualifizierte elektronische Signaturen*.
Simple Mail Transfer Protocol	(SMTP)	Übertragungsprotokoll für E-Mails
Simple Network Management Protocol	(SNMP)	Leichtgewichtiges Protokoll für die Steuerung und Statusabfrage von Netzwerkkomponenten und Servern
Simple Network Time Protocol	(SNTP)	vereinfachte Version des NTP
Single Point Of Failure	(SPOF)	Nicht redundant ausgelegte technische *Komponente* bei deren Ausfall ein *Dienst* nicht mehr verfügbar ist.

Begriff	Synonym, (AK)	Definition/Erläuterung
Smoketest	smoke testing	Ziel des Smoketest ist es, festzustellen, ob die grundlegende Funktionalität des Testobjekts gegeben ist und das Testobjekt die Testeingangskriterien erfüllt. Es werden keine Details getestet. Die für den Smoketest verwendeten Testfälle sind eine Teilmenge aller für das jeweilige Testobjekt geplanten funktionalen Testfälle.
SNMP-Traps		Dezentral initiierte Statusmeldungen, Teil des SNMP
Specification related question	(SRQ)	Ein SRQ beschreibt verbindliche Ergänzungen und Hinweise zu den von der gematik veröffentlichten Dokumenten zur Einführung der *Gesundheitskarte*. Die SRQ haben das Ziel, für den Zeitraum bis zur Veröffentlichung einer Folgeversion des betroffenen Dokumentes Klarstellungen zu Formulierungen, Interpretationshinweise aber auch Korrekturen mitzuteilen. Die SRQ werden auf der Internetseite der gematik im Zusammenhang mit der zugrunde liegenden Version des betroffenen Dokumentes (Konzept, Architektur, *Spezifikation*) veröffentlicht.
Sperrliste		Eine Sperrliste wird durch eine *Zertifizierungsinstanz* erstellt und in einem *Verzeichnisdienst* veröffentlicht. Sie beinhaltet Informationen darüber, welche *Zertifikate* durch den Zertifikatsinhaber oder andere berechtigte Stellen gesperrt (revoziert) worden sind. Ein weithin akzeptiertes Format für Sperrlisten wurde in *X.509* spezifiziert und in [RFC3280] näher profiliert.
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 *Zertifizierung* durch die gematik.
Spoofing		Vortäuschen falscher *Identitäten*
Sprechstundenbedarf		Arznei-, Verband- und Hilfsmittel für den Praxisgebrauch des *Arztes*, die nicht auf Einzelrezept zu Lasten des *Patienten* verordnet werden.
Stammdaten	master data	Daten einer Person oder eines Gegenstandes, welche über längere Zeit unverändert bleiben. Bezogen z.B. auf die *Versicherten* handelt es sich um die Personenstammdaten wie Name, Geburtsdatum und Wohnort. Die Stammdaten sind Teil der Vertragsdaten nach §291a SGB V.
Stammzertifikat	Root Certificate	Das selbstsignierte *Zertifikat*, welches in einer PKI-Hierarchie an höchster Stelle steht und den Vertrauensanker (Wurzel) bildet.

Begriff	Synonym, (AK)	Definition/Erläuterung
Standalone-Szenario		Onlineprüfung und -aktualisierung ohne eine Netzanbindung des Praxisverwaltungssystems des Leistungserbringers an die Telematikinfrastruktur. In diesem Szenario wird ein zweiter vom Praxisverwaltungssystem getrennter Arbeitsplatz (Umgebung) zur Onlineprüfung und –aktualisierung genutzt. Die am Standalone-Arbeitsplatz auf der eGK aktualisierten VSD müssen durch erneutes Stecken der eGK in das Praxisverwaltungssystem des Leistungserbringers übernommen werden.
Stapelsignatur		Erstellung einer begrenzten Anzahl Signaturen nach den zeitlich unmittelbar aufeinander folgenden Prozessen der Anzeige der zu signierenden Daten und der einmaligen Authentisierung des Signaturschlüssel-Inhabers gegenüber der sicheren Signaturerstellungseinheit (SSEE).
Stateful Inspection		Eine dynamische Paketfiltertechnik von Firewalls, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird.
Stratum		Die Nähe einer Server-Zeit zu einer geeichten Normalzeit (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.
Subscription		Herstellungsanweisung für Rezepturen, Beispiel: Salbebeschreibung, die sich aus mehreren Bestandteilen zusammensetzt.
Switch		Verbindet mehrere Geräte in einem LAN
syslog		syslog-Protokoll, UDP 514
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.
Systeme, dezentrale		Dezentrale Systeme sind Komponenten mit Bezug zur TI, welche in den lokalen Netzen der Leistungserbringer und Kostenträger betrieben werden. Bestanteil sind hier auch Systeme, die für eine E2E-Betrachtung der Fachanwendungen benötigt werden. Ingesamt umfassen die dezentralen Systeme alle Fachmodule, die dezentralen Komponenten der TI-Plattform und die Clientsysteme.
Systemmanagement		Zusammenfassung aller Aufgaben, die den operativen Betrieb der IT-Infrastruktur technisch und organisatorisch unterstützen.
T		

Begriff	Synonym, (AK)	Definition/Erläuterung
Tag Length Value	(TLV)	Innerhalb der Datenübertragungsprotokolle können optionale Informationen als Tag Length Value codiert werden. Der Typ und die Länge sind feste Größe (typischerweise 1-4 Bytes). Der Wert ist von variabler Größe.
Target of Evaluation	(TOE)	*Evaluationsgegenstand* (EVG)
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 Verordnung (Beispiel: Massageverordnung oder Papierrezept) mehrere Einheiten beinhaltet, aber nicht alle Einheiten gleichzeitig eingelöst werden können, also nur Teile eingelöst werden, so spricht man von einer Teileinlösung.
Teilnehmerverzeichnis		Das Teilnehmerverzeichnis dient der Bereitstellung von Informationen zu den KOM-LE-Teilnehmern.
Teilzulassung (beschränkte Zulassung)		Für den Einführungszeitraum einer Komponente oder eines Dienstes der Telematikinfrastruktur können erleichterte Voraussetzungen zur Zulassung gelten. Liegen die Zulassungsvoraussetzungen beim Einsatz im Testverfahren noch nicht vollständig vor, kann die Zulassungsstelle eine befristete teilweise Zulassung erteilen. Teilzulassungen beziehen sich immer nur auf abgrenzbare Teilfunktionen/Teilbereiche einer gesamtheitlichen Komponente/Anwendung. Die Erteilung einer Teilzulassungen ist nur dann möglich, wenn die Zulassungskriterien für diese abgegrenzten Funktionen/Bereiche erfüllt werden, ohne dass die Erfüllung durch Abhängigkeiten zu anderen nicht zugelassenen Teilfunktionen/Teilbereichen beeinträchtigt werden kann. Der Ausschluss negativer Abhängigkeiten ist für eine erfolgreiche Teilzulassung nachzuweisen. Hinweis: Teilzulassungen müssen nicht zwangsläufig aufgrund von Problemen für eine Gesamtzulassung erfolgen, sondern können z.B. auch in frühen Phasen benutzt werden, wenn noch nicht alle Funktionen/Bereiche bereitgestellt werden können oder müssen. Die Teilzulassung ist mit der Freigabe das wichtigste Instrument, um iteratives Vorgehen zu ermöglichen. Generell ist der Einsatz von teilzugelassenen Objekten im Produktionsumfeld zwar nicht vorgesehen, kann aber unter bestimmten Auflagen erfolgen (hierzu ist das daraus resultierende Risiko für die Projektziele zu erheben und zwischen allen Stakeholdern abzustimmen).
Telematik		Telematik ist zusammengesetzt aus den Begriffen Telekommunikation und Informatik. Er beschreibt die Zusammenführung, Verarbeitung und Weitergabe verteilter, u.U. heterogener Datenbestände.

Begriff	Synonym, (AK)	Definition/Erläuterung
Telematik Tier		Der Telematik Tier verbindet den *Service Comsumer Tier* mit dem *Service Provider Tier*. Er stellt dazu vermittelnde Netzwerk- und Transportdienste sowie Sicherheitsdienste bereit und steuert die *Fachdienste* an.
Telematikinfra-struktur	(TI)	Die Telematikinfrastruktur ist die bevorzugte Informations-, Kommunikations- und Sicherheitsinfrastruktur des deutschen Gesundheitswesens mit allen technischen und organisatorischen Anteilen. Die Telematikinfrastruktur vernetzt alle Akteure und Institutionen des Gesundheitswesens miteinander und ermöglicht dadurch einen organisationsübergreifenden Datenaustausch innerhalb des Gesundheitswesens. Die Telematikinfrastruktur unterstützt die Anwendungen der Versicherten gemäß §291a SGB V und bildet darüber hinaus die Plattform für weitere interoperable und kompatible IT-Anwendungen im deutschen Gesundheitswesen. Die TI enthält die Komponenten und Dienste der TI-Plattform, die Fachdienste und die Fachmodule.
Telematik-infrastruktur, zentrale		Zur zentralen TI gehören Infrastrukturdienste und anwendungsunterstützende Dienste sowie das zentrale Netzwerk, an das alle Akteure und Dienste der Telematikinfrastruktur angebunden sind. Nicht Bestandteil der zentralen TI sind die Fachdienste, das Transportnetz und die dezentralen Systeme.
Telematik-zulassungs-infrastruktur	(TZI)	dient der Zuteilung von *Zertifikaten* für von der gematik freigegebene *Komponenten*
Terminal API		Schnittstelle für *Primärsysteme* zum *Kartenterminal*
Test		Im Test werden Betriebszustände simuliert oder ausgeführt mit dem Ziel, Fehler und Probleme zu identifizieren und die Fehlerrate auf ein Maß zu reduzieren, welches für einen stabilen Betrieb benötigt wird. Testziele sind demnach die Optimierung des Reifegrads, die Verringerung des Risikos zur fehlenden Nutzerakzeptanz und die Möglichkeit, Aussagen zu der Produktqualität zu erzielen, auf deren Basis das weitere Vorgehen bestimmt werden kann.
Test- und Entwicklungsphase		Die Test -und Entwicklungsphase ist ein Teil der Einführungsphase der Telematikinfrastruktur, in der zwar bereits Umgebungen und Dienste zur Verfügung stehen, diese jedoch aufgrund ihres Reifegrads noch nicht für den Wirkbetrieb eingesetzt werden können. Ziel dieser Phase ist die Bewertung und Verbesserung der frühen Spezifikationsergebnisse durch flexible Testmaßnahmen, so dass ein geeigneter Reifegrad für die anschließende Erprobungsphase ermöglicht wird. Die in der Test -und Entwicklungsphase benutzten Daten sind ausschließlich Testdaten, die nicht den Schutzbedarfsbestimmungen der Produktionsumgebungen des Wirkbetriebs unterliegen und somit eine flexible Auswertung im Rahmen der Testmaßnahmen erlauben.

Begriff	Synonym, (AK)	Definition/Erläuterung
Test- und Migrationskonzept, übergreifendes (inkl. Regelung der Zulassungs- und Freigabeprozesse)		Zur Herbeiführung der TI-Wirkbetriebsreife liefert das Test- und Migrationskonzept Anforderungen und den Verfahrensrahmen, für die im Rahmen des Migrationspfades benötigten Test - und Zulassungsprozesse. Dies beinhaltet sowohl die Aufbau -und Entwicklungsphase, als auch den späteren Wirkbetrieb. Das Test- und Migrationskonzept wird initial in der Lastenheftphase unter der Verantwortung der Gesellschafter erstellt und soll in weiteren Phasen (Pflichtenheft-, Teststrategie-) durch den Auftragnehmer weiter verfeinert werden.
Testauswertung		Die Testauswertung ist die Tätigkeit der Auswertung der *Testprotokolle*. Im Zuge der Testauswertung wird ermittelt, ob Fehlerwirkungen vorliegen; ggf. wird eine Einteilung in Fehlerklassen vorgenommen. Die Ergebnisse der Testauswertung werden in Statistiken visualisiert und in *Testberichten* zusammengefasst.
Testbericht		Nach Abschluss der Tests werden die Testergebnisse im Testbericht dokumentiert. Ziel des Testberichtes ist, eine Entscheidung über Erfolg und Misserfolge einer Testung sowie die weiteren Maßnahmen bezogen auf das Testobjekt zu ermöglichen
Testbetrieb		Testbetrieb ist eine frühe Stufe im Lebenszyklus von *Diensten* und *Services* der *Gesundheitstelematik* vor dem *Wirkbetrieb* und dient der Erprobung der Implementation.
Testdesign		Aktivität im Testprozess zur Erstellung von *Testfällen*, *Testspezifikationen* und –szenarien
Testdurchführung		Aktivität im Testprozess, die die Tätigkeiten zum manuellen bzw. automatisierten Ausführen der freigegebenen *Testfälle* bzw. Testsuiten umfasst.
Testentwurf		Der Testentwurf (oder auch Testdetailkonzept genannt) wird aus den *Anforderungen* von *Fachkonzept* (FK), *Fachархitektur* (FA) und *Spezifikation* (SPEC) abgeleitet und hat einen direkten Bezug zur Prüfvorschrift. Der Testentwurf wird je Prüfobjekt aufgestellt und dokumentiert auf der Grundlage der Prüfvorschriften die detaillierte Testvorgehensweise und die zugeordneten logischen *Testfälle* einschließlich der Gründe für deren Auswahl. Darüber hinaus beschreibt er die Vorgehensweise zur Generierung bzw. Verwendung der Testdaten.

Begriff	Synonym, (AK)	Definition/Erläuterung
Testfall	test case	Ein Testfall beschreibt einen elementaren, funktionalen Softwaretest, der der Überprüfung einer z.B. in einer *Spezifikation* zugesicherten Eigenschaft eines Testobjektes (s.a. Modultest) dient. Ein Testfall wird mittels Testmethoden erstellt. Wichtige Bestandteile der Beschreibung eines Testfalls sind: 1. die Vorbedingungen, die vor der Testausführung hergestellt werden müssen, 2. die Eingaben/Handlungen, die zur Durchführung des Testfalls notwendig sind, 3. die erwarteten Ausgaben/Reaktionen des Testobjektes auf die Eingaben, 4. die erwarteten Nachbedingungen, die als Ergebnis der Durchführung des Testfalls erzielt werden. 5. die Prüfanweisungen, d.h. wie Eingaben an das Testobjekt zu übergeben und wie Sollwerte abzulesen sind.
Testimplementierung		Aktivität im Testprozess zur Realisierung einer lauffähigen *Testinfrastruktur* und des Testrahmens.
Testinfrastruktur		Bestandteile, die notwendig sind, um die geplanten Testaktivitäten erledigen zu können (Testarbeitsplätze, *Testumgebung*, Testwerkzeuge).
Testinstanz		Eine Testinstanz ist eine Instanz einer Betriebsumgebung, die speziell für Testmaßnahmen eingesetzt wird.
Testkonzept		Das Testkonzept (oft auch Testplan genannt) beschreibt, welche Testobjekte aufgrund welcher Grundlage und mit welchen Verfahren getestet werden. Das Testkonzept definiert darüber hinaus den Testumfang, die Vorgehensweise, die *Anforderungen* an die Prüfumgebung, die Ressourcen und die Zeitplanung der intendierten Tests.
Testkonzept, anwendungsspezifisches		Dokument, welches die spezifischen Testmaßnahmen einer Anwendung in der Telematikinfrastruktur auf Basis des übergeordneten Testkonzeptes beschreibt. Gilt als Grundlage für die Planung, Entwicklung und Durchführung der Testmaßnahmen durch eine testdurchführende Instanz.
Testmaßnahme		Eine Testmaßnahme ist die Bündlung von Testarten, deren Ergebnisse zur Verbesserung oder Sicherung der Produktqualität genutzt werden. Testmaßnahmen sind Teil eines Ablaufs (als Vorbereitung zur Migration oder im Rahmen von Teststufen), mit deren Hilfe die Produktqualität sichergestellt werden soll.
Testpaket		Ein Testpaket umfasst alle zu einem Test benutzten Anforderungen, *Testfälle*, Testdaten und Testergebnisse (*Testprotokolle* und *–berichte*) und steht in der Regel in direkter Beziehung zu einem Antrag auf Testung für eine *Komponente* oder zu einem zu testenden Problem. Ein Testpaket ist eine freigegebene Konfiguration und beschreibt einen Test vollständig.

Begriff	Synonym, (AK)	Definition/Erläuterung
Testplanung		Aktivität im Testprozess zur Erstellung und Fortschreibung des *Testkonzeptes*, der Testentwürfe und Prüfvorschriften
Testprotokoll		Ein Testprotokoll enthält die festgehaltenen Ergebnisse der Testausführung eines *Testfalls*. Im Testprotokoll werden je Testfall das angewendete *Testskript*, die Prüfergebnisse und die Abweichungen vom erwarteten Ergebnis festgehalten. Außerdem werden unter Bezugnahme auf die zugrunde liegenden *Testpakete*, das Datum und den verantwortlichen Tester die *Testfälle* einzeln aufgeführt. Das Testprotokoll dient dazu, die korrekte *Testdurchführung* zu dokumentieren.
Testrahmen		Sammlung aller Testtreiber, Platzhalter (Stubs), Testausgabewerkzeuge, Simulatoren, die notwendig sind, um *Testfälle* auszuführen, auszuwerten und *Testprotokolle* aufzuzeichnen.
Testregion		Eine Region, in der Teile der *Telematikinfrastruktur* vor dem *Rollout* in einem kontrollierten Testverfahren getestet werden.
Testskript		Ein Testskript ist eine Durchführungsanleitung zur schrittweisen automatisierten oder manuellen Ausführung eines *Testfalls*. Ein Testskript enthält detaillierte Informationen, welche Voraussetzungen vor dem Start des *Testfalls* geschaffen werden müssen und wie der *Testfall* auszuführen ist. Testskripte können für mehrere *Testfälle* gültig sein, die den gleichen Ablauf mit unterschiedlichen Inputdaten ausführen. Daher enthält das Testskript nicht die Eingabedaten selbst, sondern verweist auf die entsprechenden *Testfälle*. Ein Testskript muss so aufgebaut und kommentiert sein, dass die Benutzbarkeit des Testskripts durch einen vom Testskript-Ersteller abweichenden Prüfer einfach möglich ist.
Test-spezifikation		Die Testspezifikation umfasst die Auflistung der *Testfälle* für eine logische Gruppierung (z. B. zu testende *Komponenten* oder *Problem*).
Teststatus-bericht		Im Teststatusbericht wird der Status der Testaktivitäten zu einem bestimmten Stichtag umfassend dokumentiert. Der Teststatusbericht umfasst Abschnitte zu Testinhalten, Testorganisation als auch kaufmännische Aspekte. Zweck des Teststatusberichts ist die Vorlage bei der Testbereichsleitung, der Geschäftsführung oder anderen Testbeteiligten, um über den weiteren Fortgang der Testaktivitäten zu befinden. Der Teststatusbericht wird erstellt • zu Meilensteinterminen • zu vereinbarten (regelmäßigen) Terminen • auf besonderen Anlass hin (z.B. Testvorgehensanalyse)

Begriff	Synonym, (AK)	Definition/Erläuterung
Teststufe		Für die Durchführung der Testmaßnahmen zur Einführung der *elektronischen Gesundheitskarte* werden vier aufeinander aufbauende Teststufen definiert: • Labortest • Anwendertest • 10.000er-Feldtest • 100.000er-Feldtest
Testsuite		Kollektion von *Testfällen*, die logisch bzw. fachlich einem Thema zugeordnet werden können oder die in Ihrer Gesamtmenge einen bestimmten kompletten „*Use Case*“ abdecken. Eine Testsuite (auch Testszenario genannt) legt fest in welcher Reihenfolge *Testfälle* in der späteren *Testdurchführung* abgearbeitet werden. Die Nachbedingungen des einen Tests werden als Vorbedingungen des folgenden Tests genutzt.
Testteilnehmer		Ein Testteilnehmer ist ein Akteur (Leistungserbringer oder Versicherter) einer realen Arbeitsumgebung, der im Rahmen einer Erprobung neue Funktionen nutzt, so dass die Praxistauglichkeit nachgewiesen werden kann.
Testtiefe		Die Testtiefe leitet sich von den Testendekriterien ab und gibt Rahmenbedingungen vor, mit deren Hilfe der Umfang von Teststufen für eine Anwendungsklasse, unter Berücksichtigung der Änderungsarten (z.B. Neueinführung oder Optimierung), bestimmt werden kann. Indem die Testtiefe zu Beginn bestimmt wird, ist es möglich Testaufwände auf ein notwendiges Maß zu begrenzen.
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 (TOP).
Testumgebung, betriebliche		Eine betriebliche Testumgebung ermöglicht Tests, die im Rahmen der Zulassung und zur Vorbereitung von Migrationen erforderlich sind. Ihre Funktionsfähigkeit, Stabilität und Verfügbarkeit wird mit bedarfsgerechten Service Level Agreements sichergestellt.

Testung		Die Testung ist der Prozess des Testens, bestehend aus allen Aktivitäten, die sich, sowohl statisch als auch dynamisch, mit der Planung, Vorbereitung und Bewertung eines *Produkts* und damit verbundenen Arbeitsergebnissen befasst, um sicherzustellen, dass sie die festgelegten *Anforderungen* erfüllen, um zu zeigen, dass sie ihren Zweck erfüllen, und um Fehler zu finden.
		Testen umfasst die Phasen *Testplanung*, *Testdesign*, *Testimplementierung*, *Testdurchführung* und *–auswertung*.
		Im Rahmen des Testens werden nachfolgende Ergebnistypen erstellt:
		• *Testplanung*
		  ○ *Testkonzept*
		  ○ *Testentwurf*

Begriff	Synonym, (AK)	Definition/Erläuterung
		○ *Prüfvorschrift* • *Testdesign* ○ *Testfälle* ○ *Testspezifikation* ○ *Testsuite* • *Testimplementierung* ○ *Testrahmen* ○ *Testinfrastruktur* ○ *Testskripte* • *Testdurchführung* und *–auswertung* ○ *Testprotokoll* ○ *Testbericht* ○ *Teststatusbericht*
Testware	testware	Dazu gehören jegliche Art von Erzeugnissen, die für das Testen hilfreich sind. Vor allem Personen aus dem Testbereich produzieren diese: *Testkonzepte*, *Testfälle*, Testberichte, Fehlermeldungen, Eingabe-Dateien/Skripte für Testwerkzeuge,… Diese sollten alle wieder benutzbar sein und deshalb auch per Konfigurationsmanagement verwaltet werden.
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 *ServiceTicket*
Ticket Validation Service	(TVS)	Wird für die Überprüfung von *Tickets* genutzt.
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.
Tier		engl. Fachbegriff für Architekturebene Der Begriff wird in der Gesamtarchitektur [gemGesArch] verwendet, um die *Telematikinfrastruktur* bezüglich ihrer Aufgaben zu strukturieren.
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, Stratum-1-Server aufzubauen.
TI-Plattform		Die TI-Plattform als anwendungsunabhängiger Teil der TI dient der Unterstützung der Fachanwendungen mit allen nötigen technischen und organisatorischen Anteilen. Enthalten sind alle nötigen Schnittstellen- und Ablaufdefinitionen für die Fachanwendungen auf den Schichten Netzwerk, Infrastruktur und Anwendungsunterstützung. Die TI-Plattform besteht aus den dezentralen Komponenten der TI-Plattform, den zentralen Diensten der TI-Plattform und dem Zugangsnetz.
To be determined	(TBD)	Noch zu entscheiden

Begriff	Synonym, (AK)	Definition/Erläuterung
TOE Security Functionality	(TSF)	Begriff aus der *CommonCriteria* der die Menge der Entitäten beschreibt, die der EVG (*Evaluationsgegenstand*) zur Erfüllung seiner *Sicherheitsanforderungen* benötigt.
Token		Ein Token beizeichnet im Kontext dieses Dokuments sowohl Sicherheitsmerkmale (security token) im Sinne von WS-Trust, als auch Merkmale zum Referenzieren von Fallakten oder Berechtigungsverweisen (Offline-Token). Die Bedeutungsunterscheidung ergibt sich jeweils aus dem speziellen Kontext.
Token Management Service	(TMS)	Dient zur Steuerung der Authentifizierungsvorgängen
Transmission Control Protocol	(TCP)	Das in [RFC793] spezifizierte TCP ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Rechnernetzen, das auch im Internet zum Einsatz kommt.
Transportnetz		Das Transportnetz dient zur Anbindung der dezentralen TI-Plattformen an die zentrale TI-Plattform auf Netzwerkebene. Die konkreten Ausprägungen des Transportnetzes sind auf die Bedürfnisse des Anwenders angepasst und damit insbesondere bei der technischen Umsetzung sehr heterogen (z. B. Internet über ADSL, Festnetzverbindung). Das Transportnetz ist nicht durch die TI verantwortet und kontrolliert.
Transport-PIN		Ein bestimmter Status einer PIN einer *Chipkarte* im Auslieferungszustand. Vor der erstmaligen Nutzung der PIN muss die Transport-PIN in eine Echt-PIN geändert werden. Nach einer Änderung der Transport-PIN kann die Karte nicht wieder in diesen Status versetzt werden. Auf diese Weise kann der Anwender darauf vertrauen, dass ein Zugriff auf ein durch diese PIN geschützte Funktion der Karte bisher nicht möglich war, wenn er selbst die Änderung der Transport-PIN durchführt.
Transportsicherung der TI-Plattform		Die TI-Plattform stellt einen Mechanismus zur sicheren Kommunikation von Fachmodulen mit Fachdiensten auf Transportebene bereit. Über diesen Mechanismus können marktübliche verbindungsorientierte Anwendungsprotokolle (OSI Schicht 5-7) übertragen werden.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 *Telematikinfrastruktur* wird ein Treuhänder als *vertrauenswürdige* Instanz gesehen, welche treuhänderisch die Möglichkeit bietet, den Zugriff zu ausgewählten Daten eines *Versicherten* abzusichern, um diesem im Falle eines Verlusts des Zugangs(schlüssels) durch den *Versicherten* wieder Zugang zu den eigenen Daten zu ermöglichen. Nach LFDI Bayern: Ein Treuhänder ist eine neutrale Vertrauensstelle, die gewisse zentrale Aufgaben wahrnimmt und hierfür personenbezogene Daten erhält. Häufig übernimmt er die Aufgaben der pseudonymisierenden Stelle und / oder der Patientenliste. Dabei ist in der Regel die Sicherstellung des Beschlagnahmeschutzes erforderlich, weswegen häufig Notare zum Einsatz kommen.
Triple-DES	(TDES, 3DES)	Triple-DES (3DES) erhöht die Sicherheit des normalen DES, indem auf einen doppelten Schlüssel (112 Bit) der DES-Algorithmus dreifach durchlaufen wird.
Trust Service Provider	(TSP)	Organisation, welche einen oder mehrere (elektronische) *Trust Services* anbietet
Trustcenter		Institution, die *Zertifikate* im Zusammenhang mit der *digitalen Signatur* ausgibt, welche die *Identität* einer Person oder eines *Systems* bestätigen (*Zertifizierungsstelle*).
Trusted Channel	virtueller Kanal, vertrauenswürdiger Kanal	Trusted Channel ist ein Begriff aus der Common Criteria der den Übertragungsweg beschreibt über den ein Evaluationsgegenstand und ein entferntes vertrauenswürdiges IT-Produkt miteinander vertraulich kommunizieren. In der *Telematikinfrastruktur* werden die Trusted Channels z.B. zwischen eGK und *Fachdiensten* aufgebaut.
Trusted Computing Base	(TCB)	Die Trusted Comuting Base ist eine Menge, die die gesamte Hardware, Software und Firmware eines Assets umfasst, auf die Verlass sein muss, um die Sicherheit (des Assets) zu gewährleisten.
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.
Trusted Service	(TS)	Service der *Telematikinfrastruktur*, der für die Umsetzung eines Teils der Sicherheitspolicy zuständig ist
Trusted Viewer	SecureViewer, vertrauenswürdige Darstellungskomponente, (TV)	Vertrauenswürdige Benutzerschnittstelle einer *SAK* zur Anzeige des Inhalts zu signierender oder signierter Daten. Ein Trusted Viewer setzt die Anforderungen gemäß SigG/SigV und ggf. weitere, z.B. Stapel- und Komfortsignatur betreffende Anforderungen um.

Begriff	Synonym, (AK)	Definition/Erläuterung
Trust-Service Provider	(TSP)	TSPs sind Stellen, die innerhalb oder im Auftrag der Teilnehmerorganisationen Zertifikate für natürliche oder juristische Personen oder technische Komponenten ausstellen und/oder Verzeichnisdienste betreiben.
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. Der TSL Service ist ein *Produkttyp*.
Typ1-API		Schnittstelle des *Konnektors*, die den Zugriff auf dedizierte Funktionen ermöglichen, für deren Realisierung ausschließlich *dezentrale Komponenten* benötigt werden. Insbesondere die Nutzung der Signaturfunktion und Entschlüsselungsfunktion des HBAs und der SMC-B sowie das Lesen von Informationen auf einer Karte wird über dieses API angeboten.
Typ2-Netz		Das Typ2-Netz ist ein durch den *Konnektor* über eine separate VPN-Verbindung erreichbares Netz in den Anbieter von *Mehrwertdiensten* ihre *Mehrwertdienste* diskriminierungsfrei allen *Leistungserbringern* zur Verfügung stellen können. Das Typ2-Netz stellt die Summe der *Typ2-Zugangsnetze*, des zentralen Typ2-Netzes und der dezentralen Typ2-Netze dar. Das Typ2-Netz ist nicht Teil der *Telematikinfrastruktur*.
Typ2-Netz, dezentrales	(DT2N)	Unter einem dezentralen Typ2-Netz versteht man ein oftmals schon bestehendes Netz, in dem *Mehrwertdienste des Typ2* angeboten werden. Dieses Netz inklusive aller darin angebotenen *Mehrwertdienste* wird gegenüber der gematik durch einen einzigen Betreiber verantwortet, auch wenn die dort angebotenen *Mehrwertdienste* von Dritten betrieben werden sollten. Ein dezentrales Typ2-Netz ist mit dem *zentralen Typ2-Netz* oder einem *Typ2-Zugangsnetz* verbunden. Das dezentrale Typ2-Netz ist ein *Produkttyp*.
Typ2-Netz, zentrales	(ZT2N)	Das zentrale Typ2-Netz stellt das zentrale Segment des Typ2-Netzes dar, über das es möglich ist *Mehrwertdienste* und *dezentrale Typ2-Netze* diskriminierungsfrei in das *Typ2-Netz* zu integrieren. Das zentrale Typ2-Netz ist ein Produkttyp.
Typ2-Zugangsnetz		Das Typ2-Zugangsnetz stellt den äußeren Teil des *Typ2-Netzes* dar und bietet einen sicheren Zugang in das zentrale Typ2-Netz sowie in dezentrale Typ2-Netze. Hier terminiert der VPN-Kanal vom *Konnektor* in das *Typ2-Netz* (*transparenter Kanal).*

Begriff	Synonym, (AK)	Definition/Erläuterung
Typ3-API		Schnittstelle des *Konnektors*, die den Zugriff auf Funktionen ermöglichen, für deren Realisierung Komponenten der zentralen Telematikinfrastruktur benötigt werden. Dieses API ermöglicht nicht den transparenten Zugriff auf alle zentralen Infrastrukturdienste, sondern es werden ausgewählte Funktionen wie zum Beispiel das Überprüfen einer Signatur inklusive OCSP-Abfrage für die Nutzung durch *Mehrwertanwendungen* bereitgestellt.
Typ4-API		Generische Schnittstelle des *Konnektors*, die die Kommunikation mit einem *Mehrwertfachdienst* ermöglicht. Dazu werden alle Aufrufe gemäß vordefinierten Regeln gekapselt, mit spezifischen Typ4-Merkmalen versehen und unter Verwendung der Dienste der zentralen Infrastruktur der TI an den Mehrwertfachdienst übermittelt.
U		
Übergabedokument		Dokumente, die von einem *Leistungserbringer* zwecks Fortführung der Behandlung einem anderen *Leistungserbringer* übergeben werden.
Übersignatur		Gemäß Signaturverordnung [SigV, § 17] erhobene Anforderung, nach der Datensätze mit einer qualifizierten elektronischen Signatur erneut zu signieren sind, sobald diese für einen längeren Zeitraum in signierter Form benötigt werden, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und Parameter als geeignet bzw. sicher gelten.
UDDI Registry		Implementierung des UDDI Standards, siehe auch (UDDI, *Universal Description, Discovery and Integration*)
Umsetzungsanforderung	implementation requirement	Eine Umsetzungsanforderung entsteht aus den Dokumenten der gematik und beschreibt einen normativen (manchmal auch informativen) Aspekt des Dokumentes. Die Summe der Umsetzungsanforderungen eines Dokumentes müssen zusammen den vollständigen normativen Informationshaushalt des Dokumentes umfassen.
Underpinning Contract	(UC)	Ein Underpinning Contract (UC) ist eine Vereinbarung mit einem externen Dienstleiter 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.
Unified Modelling Language	(UML)	Die Unified Modelling Language (UML) ist eine Sprache zur *Spezifikation*, 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

Begriff	Synonym, (AK)	Definition/Erläuterung
Uniform Resource Locator	(URL)	Standard zur Adressierung beliebiger Objekte im Internet. Bsp.: Webseiten, PDF-Dokumente, Grafiken und Audiodateien
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.
Untersuchung, forensische	forensics	Untersuchung, ob und wie ein Angriff auf ein IT-*System* stattgefunden hat. (Allgemein: Suche nach Spuren eines Vergehens)
Update		Umfassendere Aktualisierung von Software ggf. auch mit Änderungen an Funktionalität oder Schnittstellen.
Update Flag Service	(UFS)	Der Update Flag Service (UFS) zeigt an, welche *Fachdienste* zum Zweck eines Updates 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. Der Update Flag Service ist ein *Produkttyp*.
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.
Use Case	*Anwendungsfall*	*siehe dort*
Use Case, technischer	(TUC)	Ein technischer Use Case (TUC) beschreibt eine zwingende Abfolge von Operationsaufrufen zwischen und innerhalb von *Komponenten* der *Telematikinfrastruktur*. Der technische Use Case wird durch einen *technischen Akteur* initiiert und bedient sich der *Dienste*, die von einzelnen *technischen Akteuren* (*Komponenten* der *Telematikinfrastruktur*) angeboten werden. *Fachliche Akteure* können durch Benutzereingaben involviert sein.
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 Incidents, die ein Diensteanbieter den Anwendern (Benutzer) als zentrale Kontaktstelle bereitstellt.
V		

Begriff	Synonym, (AK)	Definition/Erläuterung
Validierungs-dienst		Der Validierungsdienst dient zur Überprüfung der Gültigkeit von *X.509*-Zertifikaten In der Telematikinfrastruktur wird diese Funktion über einen *OCSP-Responder* durchgeführt.
Verbindlichkeit	Liability	Verbindlichkeit bezeichnet den Zustand, in dem die Eigenschaften der *Integrität*, *Authentizität*, *Nichtabstreitbarkeit* (Non-Repudiation) und *Zurechenbarkeit* gemeinsam erfüllt sind.
Verfügbarkeit, generell	Availability	Verfügbarkeit ist die Fähigkeit, bestimmte Informationen/*Dienste* in zugesicherter Form und Qualität innerhalb eines definierten Zeitraums am benötigten Ort zu liefern.
Verifikations-karte		Verifikationskarten sind Smartcards der Telematikinfrastruktur (eGK, HBA, etc.) mit Testidentitäten, deren Zertifikate und Schlüssel von einer im Wirkbetrieb eingesetzten Echt-CA abgeleitet wurden und somit die Durchführung von Testaktivitäten in der Wirkbetriebsumgebung ermöglichen (z.B. zur Fehlernachstellung).
Verordner		Zugelassener *Leistungserbringer*, der berechtigt ist, Verordnungen (und Überweisungen) auszustellen (z.B. *Arzt* oder Zahnarzt).
Verordnung	prescription	Leistungsbeschreibung, die von einem approbierten Heilberufler auf ein (elektronisches) Anforderungsformular aufgebracht den Empfänger zur Durchführung der Leistung legitimiert. Beispiel: Papierrezept mit mehreren Verordnungen (z.B. Arzneimitteln) oder *elektronische Verordnung.*
Verordnung, ärztliche		Durch einen *Arzt* signierte Verschreibung von Leistungen im Sinne des § 291 a und §73 Abs. 2 SGB V.
Verordnung, elektronische	(eVerordnung)	○ eVerordnung Arzneimittel Spezifische eVerordnung, die die elektronische Verordnung von apothekenpflichtigen Arzneimitteln sowie *Betäubungsmittel* gemäß Muster 16 abbildet. ○ eVerordnung Krankenhausbehandlung Spezifische eVerordnung, die die elektronische Verordnung von Krankenhausbehandlung gemäß Muster 2 abbildet. ○ eVerordnung Heilmittel Spezifische eVerordnung, die die elektronische Verordnung von Maßnahmen der physikalischen bzw. podologischen Therapie gemäß Muster 13, Maßnahmen der Stimm-, Sprech- und Sprachtherapie gemäß Muster 14 und Maßnahmen der Ergotherapie gemäß Muster 18 abbildet. ○ eVerordnung Hilfsmittel Spezifische eVerordnung, die die elektronische Verordnung von Sehhilfen und vergrößernden Sehhilfen gemäß Muster 8 bzw. 8A, Hörhilfen gemäß Muster 15 und sonstigen Hilfsmitteln gemäß Muster 16 abbildet.
Verordnungs-daten	(VOD)	Teil des Datensatzes *eVerordnung*, der vom *Arzt* erstellt wird. Enthält z.B. Daten des *Versicherten* und des *Arztes*, die Verordnung und die *Signatur* des Arztes.

Begriff	Synonym, (AK)	Definition/Erläuterung
Verordnungsdatendienst	(VODD)	Dienst zur Aufnahme und Bereitstellung von *Verordnungsdaten* in der *Telematikinfrastruktur.* Der Verordnungsdatendienst ist ein *Produkttyp*.
Versandapotheke		Zugelassene Apotheke, die in der Regel die Papierrezepte oder Zugriff auf die *eVerordnungen* erhält und nach erfolgreicher Prüfung die verordneten Arzneimittel an eine vom Patienten benannte Lieferadresse versendet.
Verschlüsselung	encoding, encryption	Bei der Verschlüsselung werden Informationen unter Verwendung eines symmetrischen oder asymmetrischen Kryptoalgorithmus mit geheimen bzw. öffentlichen Schlüsseln 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 *Krankenversichertennummer* zur Identifikation des *Versicherten*.
Versichertenstammdaten	(VSD)	Über die Versichertenstammdaten definieren sich Art und Umfang des Versicherungsverhältnisses zwischen *Kostenträger* und *Versichertem*. Die VSD sind inhaltlich normiert und von ihrer Struktur für alle *Kostenträger* einheitlich vorgegeben. Grundlage für den Dateninhalt der VSD sind die bei den *Kostenträgern* gespeicherten Sozialdaten des *Versicherten* (§§ 284, 288 SGB V). Die VSD liegen im Verantwortungsbereich des zuständigen *Kostenträgers*. Dieser ist verantwortlich für die Bereitstellung, kontinuierliche Pflege, bedarfsgerechte Aktualisierung und schließlich Löschung der Daten.
Versichertenstammdatendienst	(VSDD)	Auf dem Versichertenstammdatendienst werden die *Versichertenstammdaten* (VSD) gespeichert. Der Versichertenstammdatendienst ist ein *Produkttyp*.
Versichertenstammdatenmanagement	(VSDM)	Bereitstellung und Pflege der Stammdaten des *Versicherten* in der *Telematikinfrastruktur*.
Versicherter		Ein Versicherter ist eine natürliche Person, die von einem *Kostenträger* eine eGK erhalten hat. Er kann sich auf zwei Arten vertreten lassen: a) durch Übergabe der eGK an eine Person seines Vertrauens (organisatorisch). b) durch das Erteilen von Beauftragungen [gemFK_AdV] Der Versicherte selbst kann auf diese Weise ebenfalls andere Versicherte vertreten.
Versorgungszentrum, medizinisches		Unter medizinischen Versorgungszentren sind fachübergreifende, ärztlich geleitete Einrichtungen zu verstehen, in denen Ärzte, die in das Arztregister eingetragen sind, als Angestellte oder Vertragsärzte tätig sind.
Vertragsarztnummer		Eindeutige alphanumerische Nummer für einen Arzt, der an der GKV-Versorgung teilnimmt. Die Nummer wird auf Antrag durch den Zulassungsausschuss der Kassenärztlichen Vereinigung zugeteilt.

Begriff	Synonym, (AK)	Definition/Erläuterung
Vertragsdaten		Die Daten, die in § 291 SGB V aufgeführt sind. Sie setzen sich zusammen aus Stammdaten und Daten bezogen auf den Krankenversicherer.
Vertragsverhältnis, primäres		Das Vertragsverhältnis eines *Versicherten* mit demjenigen *Kostenträger*, welcher in erster Instanz die Behandlungskosten trägt.
Vertrauensraum	Common Trust Domain	Der Vertrauensraum bezeichnet einen Teilbereich innerhalb der *Telematikinfrastruktur*, in welchem alle PKI-relevanten Objekte (z.B. *geheime Schlüssel*, *Zertifikate*, Gültigkeitsinformationen) ein zumindest gleichwertiges Sicherheitsniveau besitzen. Die Vorgaben ergeben sich aus dem [gemSiKo] und der relevanten Certification Policy [gemTSL_SP_CP], realisiert wird der Vertrauensraum durch die Aufnahme der TSP-Zertifikate in eine *Trust Service Status List*.
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 *Zertifizierung* 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 PKI und wird zur Veröffentlichung von *Zertifikaten* und Zertifikatstatusinformationen in Form von Sperrlisten oder OCSP-Antworten verwendet. In einem Verzeichnisdienst werden die *öffentlichen Schlüssel* aller zertifizierten Teilnehmer online zur Verfügung gestellt um die *Authentizität* des Absenders einer verschlüsselten Nachricht feststellen zu können. OCSP, LDAP und X.500 sind die bekanntesten Protokolle für Verzeichnisdienste. Der Verzeichnisdienst ist ein *Produkttyp*.
VPN-Konzentrator	(VPN-K)	Der VPN-Konzentrator ist ein Sammelpunkt für mehrere VPN-Verbindungen. Der VPN-Konzentrator ist ein *Produkttyp*.
W		
Wartungsrelease		Ein Wartungsrelease enthält dringende Änderungen zu einem Major oder Minor Release. Das Wartungsrelease ist vollständig kompatibel zur Vorversion und nicht geplant. Es ist gekennzeichnet durch die Änderung der letzten Stelle der Releaseversion.

Begriff	Synonym, (AK)	Definition/Erläuterung
White-Box-Test	white box test	Der Begriff White-Box-Test bezeichnet eine Methode des Software-Tests, bei der die Tests mit Kenntnissen über die innere Funktionsweise des zu testenden *Systems* entwickelt werden. Im Gegensatz zum *Black-Box-Test* ist für diesen Test also ein Blick in den Quellcode gestattet, d. h. es wird am Code geprüft.
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.
Wirkbetrieb		Der Wirkbetrieb ist die reguläre Betriebsphase, in der für Anwender die geplanten Funktionen zur Verfügung gestellt werden und der Einsatz von Echtdaten erfolgt. Voraussetzung für den Wirkbetrieb ist der Abschluss von Testmaßnahmen, in dem ein geeigneter Reifegrad der Komponenten, Dienste und Anwendungen nachgewiesen werden konnte.
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.
Workaround		Übergangslösung eines Known Error mit dem Ziel der schnellen Wiederherstellung eines Services. (ITL basierter Begriff)
Wurzel-Zertifizierungsinstanz	Root-CA	Eine Wurzel-Zertifizierungsinstanz (engl. Root-CA) ist eine Zertifizierungsinstanz, deren Zertifikat als vertrauenswürdig gilt.
X		
X.500		X.500 ist eine von der ITU entwickelte Empfehlung für einen (globalen) *Verzeichnisdienst*, 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 Appliance		Hardware-Modul für die performante Verarbeitung von XML-Daten.

Begriff	Synonym, (AK)	Definition/Erläuterung
XML Digital Signature	XML-Dsig	Für die *digitale Signatur* von Daten im XML-Format wurde von einer Arbeitsgruppe des W3C ein spezifisches Signaturformat entwickelt. Im Vergleich zum generischen Signaturformat PKCS #7, mit dem Daten beliebigen Formats signiert werden können.
XML Encryption		Standard des W3C zur *Verschlüsselung* digitaler Inhalte einschließlich Teilen von XML-Dokumenten und Protokoll-Nachrichten
XML Signature		Standards des W3C zur Verarbeitungsregeln und Syntax von *digitalen Signaturen* im Kontext von XML
Z		
Zahlungs-beteiligung		Eine Kostenbeteiligung des Patienten. Sie kann u.a. in einer vollen Kostenübernahme des Patienten unabhängig von einer Kostenerstattung bzw. einer Zuzahlungsverpflichtung gem. § 61 SGB V bestehen.
Zeitdienst		Der Zeitdienst stellt eine NTP-basierte Zeitsynchronisation zur Verfügung. Der Zeitdienst ist ein *Produkttyp*.
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 *digitaler Signaturen* erstellt. Somit sind Zeitstempel elektronische Bescheinigung darüber, dass die mit dem Zeitstempel signierten Daten zum Zeitpunkt der *Signatur* in der signierten Form vorgelegen haben.
Zeitstempel, qualifizierter	Qualified Time Stamp	Ein qualifizierter Zeitstempel ist gemäß § 2 Nr. 14 SigG ein Zeitstempel, der von einem *Zertifizierungsdiensteanbieter* 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“.
Zeitstempel-dienst		Ein Zeitstempeldienst stellt *Zeitstempel* aus. Oft wird hierbei das in der IETF spezifizierte Time Stamp Protocol verwendet.
Zeitsynchronisation	time synchronization	Verfahren zum Sicherstellen einer einheitlichen Zeitbasis in verteilten *Systemen*, dass eine maximale Abweichung der verteilten Uhren voneinander sicherstellen soll.
Zertifikat	certificate	Zertifikate sind elektronische Bescheinigungen, die von einer *Zertifizierungsinstanz* ausgestellt (signiert) werden, mit denen dem Zertifikatsinhaber bestimmte Informationen zugeordnet werden. Hierbei unterscheidet man zwischen *Public-Key-Zertifikaten*, bei denen dem Zertifikatsinhaber insbesondere ein *öffentlicher Schlüssel* zugeordnet wird und *Attributzertifikaten*. Das gebräuchlichste Format für *Zertifikate* ist X.509v3.

Begriff	Synonym, (AK)	Definition/Erläuterung
Zertifikat, digitales		Digitale Zertifikate sind strukturierte Daten, die den Eigentümer eines öffentlichen Schlüssels bestätigen. Durch ein digitales Zertifikat können Vertraulichkeit, Authentizität und Integrität von Daten bei der Anwendung von öffentlichen Schlüsseln gewahrt werden.
Zertifikat, qualifiziertes		Ein qualifiziertes Zertifikat ist gemäß § 2 Nr. 7 SigG ein *Zertifikat*, das von einem *Zertifizierungsdiensteanbieter* 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 Identifizierung des Signaturschlüsselinhabers anhand eines amtlichen Ausweises erfolgen.
Zertifikats-Erzeugung	Create Key Certificate	Dienst des *Schlüsselmanagements* (siehe [ISO11770]): Erzeugung eines Schlüsselzertifikats: Der Dienst zur Registrierung der Erzeugung eines Schlüsselzertifikats verbindet einen *öffentlichen Schlüssel* mit einer Entität und wird von einer *Zertifizierungsinstanz* betrieben. Wenn eine *Anforderung* zur Schlüsselzertifizierung akzeptiert wird, erzeugt die *Zertifizierungsinstanz* ein Schlüsselzertifikat.
Zertifikatsherausgeber		Der Zertifikatsherausgeber ist verantwortlich für die Herausgabe und Sperrung von Zertifikaten von Personen, Institutionen und Geräten der TI. Er handelt üblicherweise im Auftrag eines Kartenherausgebers. Zertifikatsherausgeber kann sowohl ein Anbieter (bspw. bei eGK-Zertifikaten die Kostenträger), wie auch ein Betreiber (bspw. bei HBA-Zertifikaten der Zertifizierungsdiensteanbieter (ZDA)) sein. Ist der Zertifikatsherausgeber ein Anbieter, so ist er auch für die Registrierung von Personen, Institutionen und Geräten der TI verantwortlich.
Zertifikatsnehmer		Zertifikatsnehmer sind natürliche oder juristische Personen, für die ein TSP innerhalb des gematik-Vertrauensraums Zertifikate ausstellt. Zertifikate der Zertifikatsnehmer werden als Endnutzerzertifikate bezeichnet. Zertifikatsnehmer im Kontext Komponentenzertifikate sind zugelassene Dienste und/oder Geräte, für die ein TSP innerhalb des gematik-Vertrauensraums Zertifikate ausstellt.
Zertifikatsnutzer		Zertifikatsnutzer sind alle Personen, Organisationen und Systeme, die die Zertifikate der im gematik-Vertrauensraum enthaltenen TSPs nutzen können.
Zertifikatsprüfdienst		Der Zertifikatsprüfdienst dient der Prüfung der Gültigkeit eines Zertifikats via OCSP bei *elektronischen Signaturen*.
Zertifikatssuchdienst		Ein Zertifikatssuchdienst dient der Suche nach Adressinformationen, insbesondere zur asymmetrischen Verschlüsselung. Diese Funktionalität ist derzeit in der TI nicht übergreifend umgesetzt. (Siehe auch *Verzeichnisdienst/Directory Service*) Für die *Mehrwertanwendung* MWK-LE wurde eine vergleichbare Funktionalität durch den MWK-LE *Verzeichnissuchdienst* umgesetzt.

Begriff	Synonym, (AK)	Definition/Erläuterung
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 *Spezifikation*. Die Zertifizierung wird durch ein dazu legitimiertes Institut vorgenommen. In der Telematikinfrastruktur werden Zertifizierungen als Zulassungsvoraussetzung verwendet, bei der der Zulassungsnehmer nachweisen muss, dass sein Produkt erfolgreich zertifiziert wurde (z.B. Sicherheitszertifizierungen durch das BSI).
Zertifizierungsdiensteanbieter	Certification Authority, (ZDA)	Ein Zertifizierungsdiensteanbieter ist gemäß § 2 Nr. 8 SigG eine natürliche oder juristische Person, die *qualifizierte Zertifikate* oder *qualifizierte Zeitstempel* ausstellt. Ein ZDA muss die Aufnahme des Betriebes bei der BnetzA anzeigen oder sich akkreditieren lassen. Synonym: Trust Center
Zertifizierungsinstanz	Certification Authority	Eine Zertifizierungsinstanz stellt *Zertifikate* aus, indem sie die Zertifikatsinhalte mit einer *digitalen Signatur* versieht. Meist stellt eine Zertifizierungsinstanz auch Sperrlisten aus, die in ähnlicher Art und Weise signiert werden.
Zertifizierungsstelle	Certification Authority	Der Begriff der Zertifizierungsstelle war in § 2 Abs. 2 SigG97 definiert als eine „natürliche oder juristische Person, die die Zuordnung von öffentlichen Signaturschlüsseln 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 *Zertifizierungsdiensteanbieters* ersetzt.
Zielplattform		Eine Zielplattform bezeichnet ein Zielsystem, für das eine Anwendungssoftware entwickelt wird. Sie beschreibt die Kombination aus Hardware, Betriebssystem und ggf. eingesetzte Middleware.
Zugangskontrolle	Admission Control	Die Zugangskontrolle soll den unbefugten Zugang zu einem IT-System verhindern und führt hierzu eine Identifikation und eine Überprüfung der angegebenen *Identität* (*Authentifizierung*) des Benutzers (Subjekt) durch, bevor der Zugang gewährt wird. Sie umfasst die Verwaltung der Benutzerkennungen (Benutzerverwaltung) und die Rechteprüfung beim Zugangsversuch, einschließlich der Beweissicherung.
Zugangsnetz	(TI-ZGN)	Über das Zugangsnetz erfolgt die kontrollierte und sichere Anbindung der dezentralen Systeme der Leistungserbringer und Kostenträger an die zentrale TI. Es handelt sich um eine logische Bezeichnung für alle hierfür notwendigen Netzwerksegmente und Komponenten und stellt somit kein echtes physisch getrenntes und homogenes Netzwerk dar.
Zugriffskontrolle	Access Control	Die Zugriffskontrolle eines IT-Systems soll den unbefugten Zugriff auf Objekte (z.B. Daten, *Anwendungen*) verhindern. Sie umfasst die Rechteverwaltung, die Rechtezuweisung und die Rechteprüfung beim Zugriffsversuch, einschließlich der Beweissicherung.

Begriff	Synonym, (AK)	Definition/Erläuterung
Zugriffs-kontrolle, rollenbasierte	role based access control	Die Zugriffskontrolle eines IT-Systems ist nicht unmittelbar auf ein Objekt (Person, *Anwendung*) bezogen, sondern wird je *Rolle* festgelegt.
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.
Zugriffsrecht	permission	Der Begriff Zugriffsrecht wird im Zusammenhang mit der Rechteverwaltung gebraucht und dient als Oberbegriff für alle Rechte, die (z.B. in Tickets) für einen *Akteur* definiert werden können. Hierzu zählen Zugriffsberechtigungen für *Leistungserbringer* und Beauftragungen für andere *Versicherte*.
Zugriffsrecht, institutsbezogenes		Berechtigung, die einer Institution (z.B. Arztpraxis, Krankenhaus) für Zugriffe auf Daten der eGK mittels einer Institutionskarte (SMC) durch den Eigentümer der Daten erteilt wurde.
Zugriffsrecht, personenbezogenes		Berechtigung, die direkt einer Person (Leistungserbringer oder Versicherten) für Zugriffe auf Daten der elektronischen Gesundheitskarte mittels einer persönlichen Chipkarte der Telematikinfrastruktur (z.B. HBA) durch den Eigentümer der Daten erteilt wurde.
Zulassung		Für den Einsatz im Wirkbetrieb der Telematikinfrastruktur müssen sämtliche Komponenten, Dienste und Prozesse wie auch die Anbieter von Diensten zugelassen sein. Die Zulassung wird durch die Zulassungsstelle der TI auf Antrag erteilt, wenn der Nachweis erbracht wird, dass die zugrunde liegenden Anforderungen aus den Spezifikationen hinsichtlich Funktionsfähigkeit, Interoperabilität und Sicherheit erfüllt werden. Demzufolge wird unterschieden in Anbieter-, Dienst-, Komponenten- und Prozesszulassung. Die Zulassungsstelle der TI veröffentlicht Prüfkriterien und überprüft diese in Rahmen von Zulassungstests. Die Zulassung wird durch einen Zulassungsbescheid und eine Zulassungsurkunde festgestellt. Die Zulassung kann vollständig oder teilweise erteilt werden. Eine teilweise Zulassung beschränkt den Einsatz der Komponenten oder des Dienstes auf einen Zeitraum oder eine Umgebung, in der diese eingesetzt werden dürfen. Im Produktivbetrieb jedoch, dürfen nur vollständig zugelassene Komponenten, Dienste der TI und Fachanwendungen eingesetzt werden.
Zulassung, beschränkte		siehe *teilweise Zulassung*

Begriff	Synonym, (AK)	Definition/Erläuterung
Zulassung, teilweise	beschränkte Zulassung	Für den Einführungszeitraum einer *Komponente* der *Telematikinfrastruktur* können erleichterte Voraussetzungen zur *Zulassung* gelten. Liegen die Zulassungsvoraussetzungen beim Einsatz im Testverfahren noch nicht vollständig vor, kann die gematik eine bis zum Ende der dritten Teststufe befristete teilweise *Zulassung* erteilen. Die *Zulassung* wird dann als Teilzulassung durch einen entsprechenden Zulassungsbescheid und eine Zulassungsurkunde erteilt. Eine teilweise *Zulassung* wird bescheinigt für *Komponenten*, die für den freien Markt mehrfach entwickelt/produziert werden und in der Einführungsphase sind.
Zulassungskriterien		Zulassungskriterien sind die Summe aller für die Zulassung benötigten Voraussetzungen. Die Zulassungskriterien haben ihren Ursprung in Spezifikationen, Konzepten und Policies.
Zulassungsstelle		Zulassungsstelle der gematik
Zulassungsverfahren		Gemäß § 291a Abs. 7 S. 2 SGB V [SGB V] wurde die gematik gesetzlich verpflichtet sicherzustellen, dass die angebotenen *Produkte* und Dienstleistungen den definierten *Anforderungen* insbesondere im Hinblick auf Interoperabilität und Sicherheit entsprechen. Hierzu wurden von ihr Zulassungsverfahren erstellt, die den Ablauf sowie die Prüfungen und alle erforderlichen Nachweise beschreiben, die zur Zulassung notwendig sind.
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 *Patient* bereits Zuzahlungen geleistet hat.
Zuzahlungsstatus		Die Information innerhalb der Vertragsdaten, ob der *Patient* prinzipiell eine *Zuzahlung* leisten muss. Der prinzipielle Status kann unterjährig durch einen tatsächlichen Status überlagert werden, bspw. Wenn ein *Patient* aufgrund des Erreichens der Belastungsgrenze für den Rest des Jahres von weiteren *Zuzahlungen* befreit wird.

4 Abkürzungsverzeichnis

Abkürzung	Langform
3DES	Triple-DES, TDES
3TDES	*3 Key Triple-DES*
A	
AA	Ausgangsanforderung
AAL	Ambient Assisted Living
AB	1. Betriebliche *Anforderung* 2. Architekturboard
ABDA	Bundesvereinigung Deutscher Apothekerverbände
ABS	Acrylnitril-Butadien-Styrol
ACI	*Access Control Information*
ADF	1. Access-Control Enforcement Facility 2. Access-Control Decision Facility
ADI	Access-Control Decision Information
ADSL	*Asymmetric Digital Subscriber Line*
ADT	Abrechnungsdatenträger (Standard der *KBV*)
AdV	*Anwendungen des Versicherten*
AE	Architekturentscheidung
AES	*Advanced Encryption Standard*
AF	*Funktionale Anforderung*
AFO-ID	Anforderungs-Identifikation
AH	*Authentication Header*
AHB	*Anschlussheilbehandlung*
AID	*Application Identifier*
AK	*Anwendungskonnektor*
AkdÄ	Arzneimittelkommission der deutschen Ärzteschaft
AM	Access Mode, Zugriffsmodus
AMD	*Arzneimitteldaten*
AMDD	*Arzneimitteldatendienst*
AMS	*Application Management System, Anwendungsmanagementsystem*
AMTS	*Arzneimitteltherapiesicherheit*
AN	*Nicht-funktionale Anforderung*
AnF	*Funktionale Annahme*

Abkürzung	Langform
AnN	*Nicht-funktionale Annahme*
AnS	Annahme zur Sicherheit
ANSI	*American National Standards Institute*
APDU	Application Protocol Data Unit
API	*Application Programming Interface*
ARIT	*Access Rights Instantiation Token*
ARR	*Access Rule Reference*
AS	*Sicherheitsanforderung*
ASN.1	*Abstract Syntax Notation One*
AT	*Authentication Template*
ATR	*Answer to Reset*
AUT	authentication, *Authentifizierung*
Auth	authentication, *Authentisierung*
AvM	*Availability Management*
AVS	*Apothekenverwaltungssystem*
B	
B	*Byte*
BA	Berufsausweis für Mitarbeiter im Gesundheitswesen
BÄK	Bundesärztekammer
BAND	Bundesvereinigung der Arbeitsgemeinschaften der Notärzte Deutschlands
BCD	*Binary Coded Decimal*
BDSG	Bundesdatenschutzgesetz
BE-Netz	Backend-Netz
BER	*Basic Encoding Rules*
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BfDi	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
BIOS	*Basic Input Output System*
BLOB	*Binary Large Object*
BLZ	*Betriebsleitzentrale*
BMG	Bundesministerium für Gesundheit
BnetzA	*Bundesnetzagentur*
BPtK	Bundespsychotherapeutenkammer
BS	*Broker Service*
BSI	Bundesamt für Sicherheit in der Informationstechnik
BtM	*Betäubungsmittel*
BtMDD	*Betäubungsmitteldatendienst*

Abkürzung	Langform
BtMVV	Betäubungsmittel Verschreibungsverordnung
BVG	Bundesversorgungsgesetz
BZÄK	Bundeszahnärztekammer
C	
C	certificate, *Zertifikat*
C2C	*card to card*
C2S	*card to server*
CA	*Certification Authority*, *Zertifizierungsinstanz*
CAB	*Change Advisory Board*
CAMS	Card Application Management System, *Kartenanwendungsmanagementsystem*
CAR	Certification Authority Reference, Referenz der Zertifizierungsinstanz
CA-Zertifikat	Certification Authority Certificate
CBC	*Cipher Block Chaining*
CC	1. *Common Criteria* 2. *Cryptographic Checksum*
CCS	*Card Communication Service*
CEN	Comité Européen de Normalisation, Europäisches Komitee für Normung
cetp	*Connector Event Transport Protocol*
CfM	*Configuration Management*
CG	cryptogram, Kryptogramm
CH	cardholder, Karteninhaber
CHA	Certificate Holder Authorization, Berechtigung des Karteninhabers
CHAP	*Challenge Handshake Authentication Protocol*
CHR	Certificate Holder Reference, Referenz des Karteninhabers
CI	*Configuration Item*
CIA	Cryptographic Information Application, kryptografische Informationsanwendung
CIO	Cryptographic Information Objects, kryptografische Informationsobjekte
CLA	Class-Byte eines Befehls
CM	Change Management
CMDB	*Configuration Management Database*
CMET	*Common Message Element Type*
CMM	Cabability Maturity Model
CMS	*Card Management System, Kartenmanagementsystem*
CMYK	Cyan (Türkis), Magenta (Fuchsinrot), Yellow (Gelb) und Key/blacK (schwarz)
COS	Card Operating System, Kartenbetriebssystem
CoS	*Class of Service*

Abkürzung	Langform
CP	*Certificate Policy*
CPI	Certificate Profile Identifier, Kennung des Zertifikatsprofils
CpM	*Capacity Management*
CR	*Change Request, Änderungsanforderung*
CRL	Certificate Revocation List, Zertifikatssperrliste
CRM	*Customer Relationship Management*
CRT	Control Reference Template
CtM	*Service Continuity Management*
CV	*card verifiable*
CVC	*Card Verifiable Certificate*
D	
DA	Datenautorität
DALE-UV	Datenaustausch mit *Leistungserbringern* in der gesetzlichen Unfallversicherung
DAV	Deutscher Apothekerverband e.V.
DB	Datenbearbeiter
DdoS	*Distributed Denial of Service*
DDV	*Daten Direkt Verbindung*
DE	1. *Dateneigentümer* 2. Data Element, *Datenelement*
DER	*Distinguished Encoding Rules*
DES	*Data Encryption Standard*
DEÜV	Datenerfassungs- und Übermittlungsverordnung
DF	*Dedicated File*
DFA	*Differential Fault Analysis*
DFT	*Dienst-Funktionstest*
DHCP	*Dynamic Host Configuration Protocol*
DIMDI	Deutsches Institut für medizinische Dokumentation und Information
DIN	Deutsches Institut für Normung
DIR	Directory, Verzeichnis
DIT	*Dienst-Interoperabilitätstest*
DIVI	Deutsche interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin
DKG	Deutsche Krankenhausgesellschaft
DKR	Deutsche Kodierrichtlinien
DLT	*Dienst-Leistungstest*
DM	Display Message
DMP	*Disease Management Programm*

Abkürzung	Langform
DMT	*Dienst-Monitoring- und Systemmanagementtest*
DMT-I	Dienst-Monitoring-Interoperabilitätstest
DMZ	De-Militarized Zone
DNS	*Domain Name System*, Domain Name Service
DNSSEC	Domain Name System Security Extensions
DO	Datenobjekt
DoS	*Denial of Service*
DPA	*Differential Power Analysis*
DPD	Dead Peer Detection
dpi	Dots per Inch, Punkte pro Zoll
DRG	*Diagnosis Related Groups*
DSA	*Digital Signature Algorithm*
DSI	Digital Signature Input
DSL	Digital Subscriber Line, Digitaler Teilnehmeranschluss
DST	1. *Dienst-Sicherheitsrobustheitstest* 2. Digital Signature Template, Vorlage für digitale Signaturen
DT	*Diensttest*
DT2N	*Dezentrales Typ2-Netz*
DTD	*Document Type Definition*
E	
EA	1. Enterprise Architect 2. Eingangsanforderung
eArztbrief	*elektronischer Arztbrief*
ebXML	*Electronic Business XML*
ECB	Electronic Code Book, Blockverschlüsselung
ECDSA	Elliptic Curve Digital Signature Algorithm
EDI	*Electronic Data Interchange*, elektronischer Datenaustausch
EDIFACT	*Electronic Data Interchange For Administration, Commerce and Transport*
EDV	*elektronische Datenverarbeitung*
eEHIC	elektronische Europäische Krankenversicherungskarte
EEPROM	*Electrical Erasable Programmable Read Only Memory*
EF	*Elementary File*
EFID	Short EF Identifier
eGK	*elektronische Gesundheitskarte*
eHC	electronic Health Card, elektronischer Heilberufsausweis
EHIC	Europäische Krankenversicherungskarte

Abkürzung	Langform
eH-KT	eHealth-Kartenterminal
eKiosk	Umgebung zur Wahrnehmung der Rechte des Versicherten
EMV	*Europay Mastercard Visa*
ENC	1. Encryption, *Verschlüsselung* 2. Encrypted data, verschlüsselte Daten
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
EOF	End-of-File, Dateiende
eFA	*elektronische Fallakte*
ePA	*elektronische Patientenakte*
~~**eRezept**~~	
eSign	*elektronische Signatur*
ESP	*Encapsulating Security Payload*
ETSI	*European Telecommunication Standards Institute*
EU	Europäische Union
eVerordnung	*elektronische Verordnung*
EVG	*Evaluationsgegenstand*
F	
FA	1. Funktionsabschnitt 2. *Facharchitektur*
FAQ	*Frequently asked question*
FCP	File Control Parameter
FD	*Fachdienst*
FE-Netz	Frontend-Netz
FES	*Fortgeschrittene elektronische Signatur*
FI	Clock Rate Conversion Factor, Frequenzumsetzungsfaktor
FID	File Identifier, Dateikennung
FK	*Fachkonzept*
FM	*Financial Management* Fehlermeldung
FMEA	Failure Mode Effect Analysis, Methode zur Abschätzung und Bewertung von Risiken
FPU	Floating Point Unit
FQDN	*Fully Qualified Domain Name*
FTP	*File Transfer Protocol*
G	
GDO	Global Data Object

Abkürzung	Langform
GKV	*Gesetzliche Krankenversicherung*
GKV-SV	GKV-Spitzenverband
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GOÄ	Gebührenordnung für *Ärzte*
goTOP	gematik offene Testorganisations-Plattform
GP	Global Plattform
GSHB	IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informations-technik
gSP	gematik-Standardisierungs-Prozess
GT	Gesundheitstelematik
GVD	Geschützte Versichertendaten auf der eGK
H	
HARP	Harmonization for the security of web technologies and applications
HB	*Historical Bytes*
HBA	*Heilberufsausweis*
HL7	*Health Level 7*
HP	Health Professional, Heilberufler
HPC	*Health Professional Card, Heilberufsausweis*
HSM	Hardware Security Module, *Hardware Sicherheits Modul*
http	*Hypertext Transfer Protocol*
I	
IANA	*Internet Assigned Numbers Authority*
ICC	*Integrated Circuit Card*
ICCSN	*Integrated Circuit Card Serial Number*
ICM	IC Manufacturer
ICMP	*Internet Control Message Protocol*
ID	*Identifier*
IDA	Identität Datenautorität
IDB	Identität Datenbeauftragter
IDS	*Intrusion Detection System*
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

Abkürzung	Langform
IIN	*Issuer Identification Number*
IK	*Institutionskennzeichen*
IKE	*Internet-Key-Exchange*
IM	*Incident Management*
IP	Internet Protokoll
IPCP	*Internet Protocol Control Protocol*
IPsec	*Internet Protocol Security*
ISAKMP	*Internet Security Association and Key Management Protocol*
ISDN	*Integrated Services Digital Network*
ISIS-MTT	*Intermediate System – Intermediate System MailTrusT-Standard*
ISO	*International Organization for Standardization*
IT	Informationstechnik
ITIL	*IT Infrastructure Library*
ITSEC	*Information Technology Security Evaluation Criteria*
ITSM	*IT Service Management*
ITU	*International Telecommunication Union*
IV	Initial Value
K	
KB	Kilo Byte
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informations-technik in der Bundesverwaltung
KBV	Kassenärztliche Bundesvereinigung
KD	Key derivation Data
KFT	*Kompontenten-Funktionstest*
KIS	Krankenhausinformationssystem
KIT	*Komponenten-Interoperabilitätstest*
KK	Krankenkasse
KLT	*Komponenten-Leistungstests*
KM	Kartenmanagement
KMS	Kartenmanagementsystem
KOM-LE	*Kommunikation für Leistungserbringer*
Konn	Konnektor
KPI	*Key Performance Indikator*
KT	1. *Kartenterminal* 2. *Komponententest*
KTR	*Kostenträger*

Abkürzung	Langform
KV	Kassenärztliche Vereinigung
KVK	*Krankenversichertenkarte*
KVNR	*Krankenversichertennummer*
KZBV	Kassenzahnärztliche Bundesvereinigung
KZV	Kassenzahnärztliche Vereinigung
L	
L2TP	*Layer 2 Tunneling Protocol*
LAN	Local Area Network
LDAP	*Leightweight Directory Access Protocol*
LE	*Leistungserbringer*
LEO	*Leistungserbringerorganisation*
LS	*Leitstand-Service*
LTANS	*Long Term Archive Notary Services*
M	
MAC	*Message Authentication Code*
MB	Mega Byte
MDO	*Medizinisches Datenobjekt*
MF	Master File
Mgmt-	
Mgmt-Netz	*Management-Netz*
MII	Major Industry Identifier
Mkonn	Mehrkomponentenkonnektor
MKT	*Multifunktionales Kartenterminal*
mob-KT	*Mobiles Kartenterminal*
MPLS	*Multi Protocol Label Switching*
MSB	Most Significant Byte
MSE	Manage Security Environment
MTU	Maximum Transmission Unit
MWA	*Mehrwertanwendung*
MWA Typ1	*Mehrwertanwendung des Typs 1*
MWA Typ2	*Mehrwertanwendung des Typs 2*
MWA Typ3	*Mehrwertanwendung des Typs 3*
MWA Typ4	*Mehrwertanwendung des Typs 4*
MWC	*Mehrwertclient*
MWD	*Mehrwertdienst*

Abkürzung	Langform
MWD2	*Mehrwertdienst Typ2*
MWD4	*Mehrwertdienst Typ4*
MWFD	*Mehrwertfachdienst*
MWK-LE	*Mehrwertkommunikation Leistungserbringer*
MWM	*Mehrwertmodul*
MWN	*Mehrwertnetz*
N	
NAT	*Network Adress Translation*
NfC	Need for Change
NFD	Notfalldaten
NFDM	Notfalldatenmanagement
NIST	*National Institute for Standards and Technology*
NK	*Netzkonnektor*
NS	Name Server
NTP	*Network Time Protocol, The*
NTP-DdoS	Distributed Denial of Service-Angriff (DdoS) auf den NTP-Dienst.
NTP-DoS	Denial of Service (DoS)-Angriff auf den NTP-Dienst
NVRAM	*Non Volatile Random Access Memory*
O	
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	*Online Certificate Status Protocol*
OCSP-eGK	*OCSP-Responder eGK*
OCSP-HBA-SMCB	*OCSP-Responder HBA-SMC*
OCSP-Komp	*OCSP-Responder Komponenten PKI*
OID	Object Identifier, Objektkennung
OLA	*Operational Level Agreement*
OP	Offene Punkte
OSI	*Open Systems Interconnection*
OSIG	*Organizational Signature*
OT	*ObjektTicket*
OTC	*Over the Counter*
P	
PA	Prozessanleitung
PAP	Password Authentication Protocol
PassG	Passgesetz

Abkürzung	Langform
PassV	Passverordnung
PassVwV	Passverwaltungsvorschrift zur Durchführung des Passgesetzes
PB	Projektbüro
PC	*Polycarbonat*
PC/SC	Interoperability Specification for ICCs an Personal Computer Systems (References)
PCS	Procedure Coding System
PED	*Professionelle endnutzernahe Dienstleister*
PET	Polyethylenterephthalat
PFD	*Patientenfachdaten*
PFDD	*Patientenfachdatendienst*
PFDM	*Patientenfachdatenmanagement*
PHB	Projekthandbuch
PI	Padding Indicator
PICS	Protocol Implementation Conformance Statement
PIN	*Personal Identification Number*, persönliche Identifikationsnummer
PIN.CH	PIN.Card Holder (Praxis PIN)
PIN.QES	PIN.Qualified Electronic Signature (Signatur-PIN)
PIP	*Post Issuance Processing, Nachladeprozess*
PK	Public Key, *Öffentlicher Schlüssel*
PKCS	*Public Key Cryptography Standards*
PKI	*Public Key Infrastructure*
PKV	1. Private Krankenversicherung 2. Verband der privaten Krankenversicherungen e.V.
PL	Projektleiter / Projektleitung
PL-API	Plattform-API
PLZ	Postleitzahl
PMP	Projektmanagementplan
PoC	*Proof of Concept*
PP	Protection Profile, Schutzprofil
PPP	*Point-to-Point Protocol*
PPPoE	*PPP over Ethernet*
PPS	*Protocol Parameter Selection*
PrA	Projektauftrag
PrK	Private Key, *Privater Schlüssel*
PRND	*Padding Random Number*
PRU	*Produktionsreferenzumgebung*

Abkürzung	Langform
PSE	*Personal Security Environment*
PSO	*Perform Security Operation*
PSS	*Primärsystem*
pt	*point*
PTA	Pharmazeutisch-Technischer Assistent
PTB	*Physikalisch Technische Bundesanstalt*
PTSB	*Produkttypsteckbrief*
PTU	*Produktionstestumgebung*
PU	*Produktionsumgebung*
PUK	*Personal Unblocking Key*
PuK	Public Key, *Öffentlicher Schlüssel*
PUK.CH	*Praxis PUK*
PUK.home	*Privat PUK*
PUK.QES	*Signatur PUK*
PVC	Polyvinylchlorid als Kartenmaterial
Pvo	*Prüfvorschrift*
PVS	Praxisverwaltungssystem
PZN	*Pharmazentralnummer*
Q	
QES	*Qualified Electronic Signature*
QoS	Quality of Service
QS	Qualitätssicherung
R	
RA	*Registration Authority*
RADIUS	Remote Authentication Dial-In User Service
RAID	*Redundant Array of Inexpensive Disks*
RBAC	Role Based Access Control
RC	Retry Counter
RCA	Root CA, Wurzelinstanz
RD	Reference Data, Referenzdaten
RDT	*Record Discovery Token*
RegTP	ehemalige Regulierungsbehörde für Telekommunikation und Post; Nachfolger ist die Bundesnetzagentur (BnetzA)
RF	Radio Frequency
RfC	*Request for Change*
RFC	*Request for Comment*

Abkürzung	Langform
RFID	Radio Frequency Identification
RID	*Registered Application Provider Identifier*
RM	1. Risikomanagement 2. Releasemanagement
RND	Random Number, Zufallszahl
RVO	Rechtsverordnung
S	
SAGA	Standards und Architekturen für eGovernment-Anwendungen des Bundesministerium des Inneren
SAK	*Signaturanwendungskomponente*
SAVeD	Sicherer Anbindungs- und Vermittlungsdienst
SC	1. Security Condition, Sicherheitsbedingung 2. Smart Card
SD	*Service Desk*
SDS	*Service Directory Service*
SE	Security Environment, Sicherheitsumgebung
SeM	*Security Management*
SFID	Short EF Identifier
SFR	*Security Functional Requirement*, Sicherheitsanforderungen
SGB	Sozialgesetzbuch
SGB V	Sozialgesetzbuch Fünftes Buch
SHA-1	*Secure Hash Algorithm*
SICCT	*Secure Interoperable Chip Card Terminal*
SIG	Signature, Signatur
SigG	Signaturgesetz
SigV	*Signaturverordnung*
SK	Secret Key, geheimer Schlüssel
SL	Stationäre Leistungen
SLA	*Service Level Agreement*
SLO	Service Level Objective
SLR	*Service Level Requirement*
SM	*Secure Messaging*
SM-AK	*Security Module Anwendungskonnektor*
SMC	Security Module Card, Sicherheitsmodulkarte
SMC-A	*Security Module Card Typ A*, Arbeitsplatzkarte bzw. Komponentenidentitätskarte
SMC-B	*Security Module Card Typ B*, Institutionenkarte

Abkürzung	Langform
SMC-K	*Security Module Card Typ K*
SMC-KT	*Security Module Card Typ KT*
SMC-RFID	*Security Module Card Typ RFID*
SMK	SM key, SM-Schlüssel
SM-K	*Security Module Konnektor*
SM-KT	Security Module Kartenterminal
SM-NK	*Security Module Netzkonnektor*
SMTP	*Simple Mail Transfer Protocol*
SN	Serial Number, Seriennummer
SNMP	*Simple Network Management Protocol*
SNTP	*Simple Network Time Protocol*
SOAP	Standard für die Kommunikation innerhalb der WEB-Services
SP	Service Provider
Spec.	Specification
SPOF	*Single Point Of Failure*
SRQ	*Specification related question*
SSC	*Send Sequence Counter*
SSCD	*Secure Signature Creation Device*
SSEE	*Sichere Signaturerstellungseinheit*
SSL	*Secure Socket Layer*
SVA	Sozialversicherungsabkommen (der EU)
SVR	Server
SW	1. Software 2. Status Word
T	
TBD	1. *To be determined*, noch nicht festgelegt 2. To be done, fertigzustellen
TC	1. Trusted Channel 2. Trust Center
TCB	Trusted Computing Base
TCL	Trusted Component List
TCP MSS	TCP Maximum Segment Size
TCP/IP	*Transmission Control Protocol*/Internet Protocol
TCS	Test Case Specification
TDS	*Time Distribution System*
TI	*Telematikinfrastruktur*

Abkürzung	Langform
TI-ZGN	Telematikinfrastruktur-Zugangsnetz
TLS	Transport Layer Security
TLV	*Tag Length Value*
TMS	*Token Management Service*
TOE	*Target of Evaluation*, E*valuationsgegenstand* (EVG)
TOP	Testorganisationsplattform
TPM	*Trusted Platform Module*
TS	*TrustedService*
TSF	*TOE Security Functionality*
TSL	*Trust-service Status List*
TSP	*Trust Service Provider*
TTD	Telematik Transport Details
TUC	*Technischer Use Case*
TV	*Trusted Viewer*
TVS	*Ticket Validation Service*
TZI	*Telematikzulassungsinfrastruktur*
TZP	Telematikzugangsprovider
U	
UC	1. Use Case, Anwendungsfall 2. *Underpinning Contract*
UDDI	*Universal Description, Discovery and Integration*
UDP	*User Datagram Protocol*
UFS	*Update Flag Service*
UHD	*User Help Desk*
UML	*Unified Modelling Language*
UQ	Usage Qualifier, Karteninhaberauthentifikation
URI	*Uniform Resource Identifier*
URL	*Uniform Resource Locator*
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UTF8	8-bit Unicode Transformation Format
UUID	Universal Unique ID
V	
VdAK/AEV	Verband der Angestellten-Krankenkassen e.V./Arbeiter-Ersatzkassen-Verband e.V.
VDAP	Verband deutscher Arztpraxis-Softwarehersteller e.V.

Abkürzung	Langform
VDDS	Verband Deutscher Dental-Software Unternehmen
VhitG	Verband der Hersteller von IT-Lösungen für das Gesundheitswesen
VHK	Verein patientenorientierter Informations- und Kommunikationssysteme
VNM	Virtual Machine Monitor
VOD	*Verordnungsdaten*
VODD	Verordnungsdatendienst
VODM	Verordnungsdatenmanagement
VPN	*Virtual Private Network*
VPN-K	*VPN-Konzentrator*
VSD	*Versichertenstammdaten*
VSDD	*Versichertenstammdatendienst*
VSDM	*Versichertenstammdatenmanagement*
W	
WAN	*Wide Area Network*
WOP	*Wohnortprinzip*
WSDL	WebService Description Language
X	
XAdES	XML Advanced Electronic Signatures
XML	Extensible Markup Language
XSD	Extensible Schema Definition
xTV	Extended Trusted Viewer
Z	
ZDA	*Zertifizierungsdiensteanbieter*
ZI	Zentralinstitut für die Kassenärztliche Versorgung
ZIS	Zugangs- und Integrationsschicht
ZPVS	Zahnarztpraxisverwaltungssystem
ZS	Zuzahlungsstatus
ZT2N	Zentrales Typ2-Netz

Anhang

A1 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CNTS]	CRC Press Taylor & Francis Group (März 2006): Computer Network Time Synchronization The Network Time Protocol, David L. Mills (ISBN: 0-8493-58051)
[FIPS180-2]	Federal Information Processing Standards Publication 180-2 (August 2002) – Secure Hash Standard, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (zuletzt geprüft am 14.12.2006)
[FIPS186-2]	NIST: FIPS Publication 186-2: Digital Signature Standard (DSS), Januar 2000 und Change Notice 1, Oktober 2001.
[gemFK_ADV]	gematik: Einführung der Gesundheitskarte - Fachkonzept Anwendungen des Versicherten (ADV)
[Haas_2006]	Springer Verlag (P. Haas) (2006): Gesundheitstelematik: Grundlagen, Anwendungen, Potenziale
[gemBetr_Qu]	gematik: Einführung der Gesundheitskarte - Anforderungen an die Betriebsunterstützung und Querschnittsaufgaben
[gemBetr_SLA]	gematik: Einführung der Gesundheitskarte – Service Level Agreements
[gemBetr_LB]	gematik: Einführung der Gesundheitskarte – Leistungsbeschreibungen
[gemFK_VODM]	gematik: Einführung der Gesundheitskarte - Fachkonzept Verordnungsdatenmanagement
[gemPolicy]	gematik: Einführung der Gesundheitskarte - Betrieb der Gesundheitstelematik - Policy
[gemSpec_KT]	gematik: Einführung der Gesundheitskarte - Spezifikation eHealth-Kartenterminal
[gemSiKo]	gematik: Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept
[ISO11770]	ISO/IEC 11770: 1996 Information technology - Security techniques - Key management Part 3: Mechanisms using asymmetric techniques
[Oestereich]	B. Oestereich (2001): Objektorientierte SW-Entwicklung, Analyse und Design mit der UML, 5. Auflage
[RVO2009]	Bundesgesetzblatt I (2009) vom 02.10.2009, Seite 3162 ff.: Zweite Verordnung zur Änderung der Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte in der Fassung vom 23.09.2009
[SAGA]	Bundesministerium des Innern (2005): Standards und Architekturen für E-Government-Anwendungen
[SigG01]	Bundesgesetzblatt I (2001), S.876: Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz - SigG)
[UDDI]	OASIS (19.10.2004): UDDI Spec Technical Committee Draft Version 3.0.2 http://uddi.org/pubs/uddi_v3.htm
[WuV]	WUV Werbe- und Vetriebsgesellschaft Deutscher Apotheker mbH (31.10.2006): Glossar rund um die Telematik im Gesundheitswesen; http://www.wuv-gmbh.de/1377_1416.htm (zuletzt geprüft am 14.12.2006)

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[RFC2251]	RFC2251 (Dezember 1997): Lightweight Directory Access Protocol (v3) http://www.ietf.org/rfc/rfc2251.txt
[RFC2401]	RFC 2401 (November 1998): Security Architecture for the Internet Protocol http://www.ietf.org/rfc/rfc2401.txt
[RFC3280]	RFC 3280 (April 2002): Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile http://www.ietf.org/rfc/rfc3280.txt
[RFC3647]	RFC 3647 (November 2003) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://www.ietf.org/rfc/rfc3647.txt
[RFC4301]	RFC 4301 (Dezember 2005): Security Architecture for the Internet Protocol http://www.ietf.org/rfc/rfc4301.txt
[RFC793]	RFC 793 (September 1981): Transmission Control Protocol http://www.ietf.org/rfc/rfc793.txt
[RFC959]	RFC 959 (Oktober 1985) File Transfer Protocol (FTP) http://www.ietf.org/rfc/rfc959.txt
[BSI-TR-03114]	BSI (22.10.2007): Technische Richtlinie – Stapelsignatur mit dem Heilberufsausweis; Version 2.0 https://www.bsi.bund.de/cae/servlet/contentblob/477234/publicationFile/30605/BSI-TR-03114_pdf.pdf