gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Glossar

Version:	2.4.0
Revision:	\main\rel_main\15
Stand:	25.09.2008
Status:	freigegeben

Dokumentinformationen

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
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

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
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
	13.05.08	3	Formulierungsanpassungen	QM
	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

Inhaltsverzeichnis

1 Zusammenfassung

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

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

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

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

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

2.2 Zielgruppe

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

2.3 Geltungsbereich

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

2.4 Arbeitsgrundlagen

Die Grundlagen zu diesem Dokument bilden die 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

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

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

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

3 Glossar

Begriff	Synonym	Definition/Erläuterung
1st Level Support		Erste öffentliche Ansprechpartner im Support
2nd / 3rd Level Support		Nachgelagerte Supportabteilungen zur Lösung tiefer gehender Probleme
3DES	Triple-DES, TDES	Triple-DES (3DES) erhöht die Sicherheit des normalen *DES*, indem auf einen doppelten Schlüssel (112 Bit) der *DES*-Algorithmus dreifach durchlaufen wird.
3TDES	3 Key Triple-DES	Zusätzlich zu 3DES wird für jeden *DES*-Durchgang ein eigener Schlüssel verwendet.
A		
AB		1. Betriebliche *Anforderung* 2. Architekturboard
ABDA		Bundesvereinigung Deutscher Apothekerverbände
Ablaufdatum	expiration date	Datum, ab dem eine zugesicherte Leistung nicht mehr verfügbar ist (Synonym: gültig bis).
Abnahmetest	acceptance trial	Test eines Produktes, in dem geprüft wird, ob das Produkt die Anforderungen der *Spezifikation* erfüllt.
ABS	Acrylnitril-Butadien-Styrol	
ACI	Access Control Information	ACI bezeichnet Datensätze, in denen Informationen über Zugangsberechtigungen verschiedener *Identitäten* abgelegt sind
Administrative Hoheit		Verantwortlichkeit für das zweckorientiert und gesetzeskonforme Funktionieren eines *Systems*
Administrator		Fachpersonal zum Aufbau und Betrieb der *Telematikinfrastruktur* und der vorhandenen *Primär*- und Back-End-*Systeme*.
ADSL	Asymmetric Digital Subscriber Line	Übertragungsverfahren für die Hochgeschwindigkeitsdatenübertragung über eine normale Telefonleitung.
ADT		Abrechnungsdatenträger (Standard der *KBV*)
AE	Architekturentscheidung	
AES	Advanced Encryption Standard	Standard für ein symmetrisches Kryptosystem
AF	Funktionale *Anforderung*	

Begriff	Synonym	Definition/Erläuterung
AFO-ID	Anforderungs-Identifikation	Dient zur Identifizierung von Anforderungen im Anforderungsmanagement und wird als Referenzierungsmerkmal verwendet.
AHB	Anschlussheilbehandlung	
AID	Application Identifier	Kennung zur Identifikation einer Software
AkdÄ		Arzneimittelkommission der deutschen Ärzteschaft
Akkreditierung	accreditation	Prozess der Überprüfung bzw. Bescheinigung der erfolgreichen Überprüfung bzgl. der Erfüllung einer besonderen Eigenschaft. Die Akkreditierung ist gemäß § 2 Nr. 15 des *Signaturgesetzes* ein freiwilliges „Verfahren zur Erteilung einer Erlaubnis für den Betrieb eines Zertifizierungsdienstes, mit der besondere Rechte und Pflichten verbunden sind." 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 sind beispielsweise die Anwender des *Systems*. Bei den Akteuren werden jedoch nicht die konkreten beteiligten Personen unterschieden, sondern ihre *Rollen*, die sie im Kontext des *Anwendungsfalls* einnehmen.
Akteur, berechtigter		Als berechtigter *Akteur* in der *Telematikinfrastruktur* werden Personen oder Systeme bezeichnet, für die (z.B. in *Tickets*) Zugriffsrechte definiert sind.
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.
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).

Begriff	Synonym	Definition/Erläuterung
AlgRef.		Algorithmus Referenz
AM	Access Mode	Zugriffsmodus
AMD	Arzneimitteldaten	
AMDD	Arzneimitteldaten-dienst ~~Arzneimitteldokumen-tationsdienst~~	
AMDOK	*Arzneimittel-dokumentation*	
AMS	Application Manage-ment System	*Anwendungsmanagementsystem*, siehe auch *CAMS*
AMTS	*Arzneimitteltherapie-sicherheit*	
AN	Nicht-funktionale *Anforderung*	
Änderungsan-forderung	Change request	Schriftlich formalisierte Darstellung eines Änderungsbe-darfs an Ergebnistypen eines abgestimmten *Release* und/oder einer abgestimmten veröffentlichten Version. *Change Requests* sind immer entscheidungs- und be-wertungsrelevant.
AnF	Funktionale Annahme	
Anforderung	requirement	Vor der Entwicklung von Produkten werden die Eigen-schaften festgelegt, welche das Produkt erfüllen muss. Dabei wird nach fachlichen (welche Funktion muss das Produkt erfüllen), technischen (wie muss die Funktion umgesetzt werden), betrieblichen (was muss die das Produkt leisten) Aspekten und solchen der Sicherheit differenziert. Im Rahmen des Projektes zur Einführung der Gesund-heitskarte gilt aus Sicht des Anforderungsmanage-ments: Beschreibung einer gewünschten Eigenschaft des Pro-duktes „*Telematikinfrastruktur*“, die mindestens auf fol-gende konzeptionelle Ergebnistypen inhaltlich wirkt: * *Fachkonzept* * *Facharchitektur*, Gesamtarchitektur * *Spezifikation* * *Releasedefinition* Anforderungen werden klassifiziert und aus speziellen Sichten gruppiert. Abgegrenzte Begriffe, die nicht dieser Definition unter-liegen: * Testanforderung: Anforderungen an den Test der *Te-lematikinfrastruktur* * Betriebsanforderung, *Incident*-Meldung: Anforderun-gen an den Betrieb der *Telematikinfrastruktur* * *Sicherheitsanforderung*: *Sicherheitsanforderungen* mit Geheimhaltung * Risikobetrachtungen

Begriff	Synonym	Definition/Erläuterung
Anforderungs-meldung	Demand note	Schriftlich formalisierte Darstellung einer Anforderungs-idee als ausschließliches Kommunikationsmittel für den Entscheidungs- und Bewertungsprozess von *Anforde-rungen*. Datenhaushalt: * Anforderungssteller (Name, Organisationseinheit, E-Mail, Telefon) * Erstellungsdatum * Bezug (optional) * Anforderungstext * Anforderungserläuterung (optional) * Dringlichkeit, Zusammenhänge (optional)
Anmeldename	login, login name	Benutzername, mit dem sich ein Benutzer bei einem IT-System anmelden kann.
AnN	Nicht-funktionale Annahme	
Anonymisie-rung		Anonymisierung gemäß § 3 Abs. 6 BDSG (Bundesda-tenschutzgesetz): Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelanga-ben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer be-stimmten oder bestimmbaren natürlichen Person zuge-ordnet werden können.
AnS	Annahme zur Sicher-heit	
ANSI	American National Standards Institute	Amerikanisches Normungsinstitut, mehrere seiner Standards wurden in internationale Normen übernom-men (ANSI-ASCII, DES, X.9.31 (RSA). X9.53 (3DES), X9.62 (ECDSA))
Anwendertest		Anwendertests bilden die zweite *Teststufe* der Test-maßnahmen zur Einführung der *elektronischen Ge-sundheitskarte*. 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 ausge-gangen werden kann.
Anwendung	application, Applikati-on	System (Software-System) zur Unterstützung fachlicher Prozesse. Im Einsatzbereich der eGK gehören hierzu die über § 291a SGB V festgelegten Anwendungen, wie z. B. *eVerordnung* oder *freiwillige Anwendungen*. Zu den *Anwendungen* auf der *eGK* gehören Bereiche mit anwendungsspezifischen Daten und zugehörigen Zugriffsschutzregeln, hier jedoch kein ausführbarer Co-de.

Begriff	Synonym	Definition/Erläuterung
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.
Anwendungs-gateway		Anwendungsgateways sind Infrastruktur-Bestandteile, die spezifische Protokoll-Anfragen entgegen nehmen, diese auf syntaktische Korrektheit sowie Sicherheitsrisiken und potentiell Berechtigungen hin überprüfen und an eine Backend-Anwendung weiterleiten. Hierdurch wird ein direkter Zugriff aus einer unsicheren Zone auf eine schützenswerte Anwendung verhindert und somit ein erhöhtes Sicherheitsniveau erreicht
Anwendungs-management	application management, Applikationsmanagement	Betreuung von *Systemen* 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-management-system	application management system, AMS, Applikationsmanagementsystem	*System* für das *Anwendungsmanagement*.
API	Application Programming Interface	Ein Application Programming Interface ist eine dokumentierte Software-Schnittstelle, mit deren Hilfe ein Software-System bestimmte Funktionen eines anderen Software-Systems nutzen kann.
~~Apothekenteil~~		siehe Einlösedaten
Applikations-form		Darreichungsform eines Fertigarzneimittels oder einer Rezeptur. Eine normative Liste der Benennungen und Abkürzungen ist im [gemFK_VODM] (Beispiel: Tablette, Tab.) enthalten.
Approbierter Heilberufler		Eine natürliche Person (*Arzt*, Apotheker, Zahnarzt) mit gültiger Approbation (Zulassung der Ärzte-, Zahnärzte- oder Apothekerkammer), die diese Person berechtigt, entsprechende Heilbehandlungen durchzuführen.

Begriff	Synonym	Definition/Erläuterung
Arbitration		Konfliktlösungsverfahren, bei dem ein neutraler Dritter den Vorsitz hat (Schlichtung).
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 Distriubuted Processing nach *SAGA* [SAGA]) verwendet: *Enterprise View, Computational View, Information View, Engineering View* und *Technology View*.
ARR	Access Rule Reference	Verwendung bei der Speicherung von Zugriffsregeln
Arzneimitteldokumentation	AmDok	Dabei handelt es sich um Daten zur Prüfung der *Arzneimitteltherapiesicherheit*. Die Arzneimitteldokumentation beinhaltet *Medikationsdaten*, *Arzneimittelverordnungsdaten* und Therapievorschlagsdaten.
Arzneimitteltherapiesicherheit	AMTS	Die Arzneimitteltherapiesicherheitsprüfung dient der Vermeidung von Risiken, die durch Wechselwirkungen von Arzneimitteln, mögliche Allergien des Versicherten, … entstehen können. Grundlage hierfür ist die *Arzneimitteldokumentation*.
Arzneimittelverordnungsdaten		Die Arzneimittelverordnungsdaten beinhalten Informationen über die vom *Arzt* ausgestellten *Verordnungen*.
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.
Ärztliche Verordnung		Durch einen *Arzt* signierte Verschreibung von *Leistungen* im Sinne des § 291 a und §73 Abs. 2 SGB V.
~~**Arztpraxispersonal**~~		ersetzt durch: *Mitarbeiter medizinische Institution*
~~**Arztteil**~~		ersetzt durch: *Verordnungsdaten*
AS	*Sicherheitsanforderung*	

Begriff	Synonym	Definition/Erläuterung
ASN.1	Abstract Syntax Notation One	Notation für Datenformate
AT	Authentication Template	
ATR	Answer to Reset	Reihe von Parametern, mit denen die Chipkarte dem Chipkartenleser mitteilt, wie diese miteinander kommunizieren können.
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.
Audit		Bezeichnet eine Überprüfung von Aufzeichnungen und Aktivitäten um festzustellen, ob bestehende Richtlinien und vorgegebene Verfahrensweisen eingehalten werden (z.B. Sicherheitsaudit). In der *Telematikinfrastruktur* bezeichnet Audit das fachliche *Protokollieren* durch den *Audit Service* bzw. die fachliche *Protokollierung* der letzten 50 Zugriffe auf die *eGK* zur Überprüfung durch den Versicherten. Da es um die *Protokollierung* von personenbezogenen Daten geht, dient das Audit ausschließlich Datenschutzzwecken.
Audit Service	AuditS Auditdienst	Der Audit Service protokolliert versichertenzentriert und den Fachdienst übergreifend alle Online-Zugriffe auf die Daten eines *Versicherten* innerhalb der *Telematikinfrastruktur*. Er ist Teil des *Broker Service* (im weiteren Sinne).
Auftragsanforderung	order requirement initial requirement	Klassifizierung von *Anforderung* *Anforderungen*, die im Sinne einer Weisung (verbindlich, bewertungsrelevant) oder im Sinne eines Auftrages (unverbindlich, entscheidungs- und bewertungsrelevant) an die gematik gehen.

Begriff	Synonym	Definition/Erläuterung
Augenschein und Augenscheinsbeweis		Augenschein ist jede unmittelbare sinnliche Wahrnehmung durch eine für ein Gericht oder eine Behörde tätige Person mit dem Ziel, beweiserhebliche Tatsachen festzustellen (z. B. durch Sehen, Hören, Riechen). Der Beweis durch Augenschein (Augenscheinsbeweis), der im Zivilprozessrecht in §§ 371 ff geregelt ist, umfasst alle Beweismittel, die nicht als Zeugen-, Urkunden-, oder Sachverständigenbeweis gesetzlich besonders geregelt sind
Ausgangsanforderung	output requirement	Anforderungssicht Eine Anforderung aus Sicht eines Konzeptes, die dieses Konzept für Folgekonzepte als Eingangsanforderung ermittelt hat
AUT	authentication, *Authentifizierung*	
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.
Auth	authentication *Authentisierung*	
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?
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.

Begriff	Synonym	Definition/Erläuterung
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.
AVS	Apothekenverwaltungssystem	*Primärsystem* der Apotheker
B		
B	Byte	digitales Speicherformat für 1 Zeichen
BA		Berufsausweis für Mitarbeiter im Gesundheitswesen (siehe auch *HBA*)
Backbone		Als Backbone wird ein zentrales Netzwerksegment mit hoher Bandbreite bezeichnet, dessen Aufgabe es üblicherweise ist, mehrere angeschlossene Netzwerke mit einander zu verbinden
BÄK	Bundesärztekammer	
BAND		Bundesvereinigung der Arbeitsgemeinschaften der Notärzte Deutschlands
Basic Input Output System	BIOS	Basis-Betriebssystem eines jeden x86 konformen Rechnersystems (unabhängig davon, ob es sich um einen PC oder einen Server handelt). Es ist die Software, die der Rechner direkt nach dem Einschalten lädt. Sie steuert den POST (Power On Self Test) und steht dem Steuerwerk der CPU direkt zur Verfügung. Es ist – wie eine Firmware auch – im Allgemeinen in einem nicht flüchtigen Speicher (Non volatile RAM) abgelegt.
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.
BCD	Binary Coded Decimal	Binär kodierte Dezimalzahldarstellung, bei der jede Ziffer einzeln durch 4 oder 8 Bit dargestellt wird
BDSG	Bundesdatenschutzgesetz	

Begriff	Synonym	Definition/Erläuterung
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.
Benutzbarkeit	chance of use	Die Benutzbarkeit eines Produktes definiert sich durch den Erfüllungsgrad aller *funktionalen Anforderungen, angelehnt an die Qualitätsmerkmale der DIN 66272.*
Benutzer	user	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.
Benutzerfreundlichkeit	ease of use	Die Benutzerfreundlichkeit eines Produktes definiert sich durch den Erfüllungsgrad aller *nicht-funktionalen Anforderungen.*
BER	Basic Encoding Rules	Basic Encoding Rules sind Grundregeln für die Kodierung von Daten, die in *ASN.1* beschrieben werden.
Berechtigter		Ein Berechtigter ist eine natürliche oder juristische Person, die durch eine befugte Person (im Kontext der Einführung der *elektronischen Gesundheitskarte*: der *Dateneigentümer*) die Erlaubnis für eine Aktivität (wie z.B. einen Zugriff auf Daten) erhalten hat. Der Zusammenhang zwischen *Dateneigentümer* und ähnlichen Begriffen ist in der Definition des *medizinischen Datenobjektes* enthalten.
Beschaffungskosten		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.
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.

Begriff	Synonym	Definition/Erläuterung
Betäubungsmittel	BtM	Narkotisierende, schmerzreduzierende oder sonstige verschreibungspflichtige Arzneimittel mit Hervorrufen einer Abhängigkeit im Sinne des Betäubungsmittelgesetzes (BtMG) nach Anlage I bis III (aufgeführte Stoffe und Zubereitungen, z.B. Morphin-N-oxid).
Betreiber		Betreiber sind Organisationen, welche *Dienste* der *Telematikinfrastruktur* bereitstellen. Die Betreiber der *Telematikinfrastruktur* sind im Dokument Betriebspolicy [gemPolicy] festgelegt. Betreiber können den *Dienst* selbst betreiben oder einen Provider mit dem Betrieb des *Dienstes* beauftragen. Sie verantworten die Einhaltung der zum *Dienst* gehörenden Betriebs- und Servicelevel gegenüber der gematik.
Betriebsumgebung		Die Betriebsumgebung beschreibt eine in sich geschlossene *Infrastruktur* zu einem bestimmten Zweck. Beispiele für Betriebsumgebungen sind: Anwendertestumgebung, *Referenzumgebung*, Produktionsumgebung. Diese sind physikalisch voneinander getrennt.
Bevollmächtigter		Eine natürliche Person, die im Fall einer nicht geschäftsfähigen Person bzw. bei Verhinderung die Rechte der Person durch Vorlage oder Nachweis einer Vollmacht wahrnimmt (autorisierter Vertreter).
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte	
BfDi	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit	
BG-Abrechnung	Berufsgenossenschaftliche Abrechnung	
Binary Large Object	BLOB	Binary Large Objects (BLOBs) sind große binäre und nicht weiter strukturierte Objekte beziehungsweise Felddaten. Diese werden üblicherweise dann verwendet, wenn für die speichernde oder empfangende Instanz die interne Struktur des Datenobjektes nicht relevant ist.
BinarySecurityToken		Ein BinarySecurityToken bezeichnet eine binär abgelegte Datenstruktur innerhalb des Webservice Security Standards. Diese Datenstruktur wird zum Speichern eines Security Tokens wie zum Beispiel eines *X.509-Zertifikates* verwendet und dient dazu, einen Benutzer zu authentifizieren
bindingTemplate		Element des *UDDI* Standards
Biometrisches Merkmal		Körpermerkmal, anhand dessen ein Mensch durch ein Biometrisches *System* identifiziert werden kann
BIOS	Basic Input Output System	

Begriff	Synonym	Definition/Erläuterung
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.
BLOB	Binary Large Object	
BMG	Bundesministerium für Gesundheit	
BNetzA	*Bundesnetzagentur*	
Boolean		Datentyp zum Speichern der zwei Zustände: Wahr und Falsch
BPtK	Bundespsychotherapeutenkammer	
Broker		Vermittelnde Infrastrukturkomponente für die Verbindung von dezentralen Komponenten und verschiedenen Fachdiensten.
Broker Service	BS	Der Broker Service integriert einzelne Telematik-Dienste in komplexere Ablauffolgen, Telematik-Sequenzen genannt, die vom *Konnektor* aufgerufen werden können. Zur Bereitstellung dieser Telematik-Sequenzen verwendet der Broker Service die anderen Dienste des Telematik Layers (z.B. zwecks Protokollierung, Anonymisierung, usw.) sowie die Dienste des *Service Provider Layers*.
BS7799		Der British Standard 7799 ist eine Norm für die Auditierung und *Zertifizierung* von IT-Systemen, die in der jetzigen Form der Öffentlichkeit im 1999-04 vorgestellt wurde. Der Standard BS 7799 ist ein international anerkannter Standard für *Informationssicherheit*, der Unternehmen bei der Definition und Umsetzung einer optimalen Sicherheitsstrategie unterstützt. Dieser wurde von der ISO als *ISO 17799* übernommen, welcher wiederum vom *ISO 27001* abgelöst wird.
BSI	Bundesamt für Sicherheit in der Informationstechnik	
BtM	*Betäubungsmittel*	
BtMDD	Betäubungsmitteldatendienst	

Begriff	Synonym	Definition/Erläuterung
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.
BtMVV	Betäubungsmittel Verschreibungsverordnung	
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.
BVG	Bundesversorgungsgesetz	
BZÄK	Bundeszahnärztekammer	
C		
C	certificate	*Zertifikat*
C2C	card to card	Authentifizierungsverfahren zwischen zwei *Chipkarten*
C2S	card to server	Authentifizierungsverfahren zwischen einer *Chipkarte* und einem Server
CA	Certification Authority	*Zertifizierungsinstanz*
Cache, cachen		Der Cache bezeichnet in der EDV einen schnellen Puffer-Speicher, der zum Beschleunigen von Zugriffen eingerichtet wird. Ein Cache enthält lokale Kopien von Inhalten eines anderen (Hintergrund-)Speichers und erlaubt somit den Zugriff ohne auf externe Datenspeicher zurückgreifen zu müssen. cachen = in den Puffer-Speicher laden.
Cache-Miss		Ein Cache Miss bezeichnet einen nicht erfolgreichen Zugriff auf einen *Cache*. Dies bedeutet für das den Cache verwaltende *System*, dass die Existenz der Daten im Hintergrundspeicher überprüft und dann dem *Cache* hinzugefügt werden muss

Begriff	Synonym	Definition/Erläuterung
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.
CAMS	*Card Application Management System, Kartenanwendungsmanagementsystem*	
Capacity Management	CpM	*ITIL*-basierter *Prozess*, der sicherstellen soll, dass die notwendige und vereinbarte Kapazität zur Erbringung eines IT-Service zeitgerecht und kostenmäßig vertretbar bereitgestellt wird. Hierbei werden die notwendigen IT-Ressourcen aufgrund der geschäftlichen *Anforderungen* ermittelt, die Auslastung prognostiziert und ein Kapazitätsplan für die Planung der IT-Ressourcen erstellt. Darüber hinaus wird die Auslastung der Ressourcen überwacht und der Service gegen den SLA geprüft.
CAR	Certification Authority Reference	Referenz der *Zertifizierungsinstanz*
Card Management System	CMS, *Kartenmanagementsystem*	
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.
CBC	Cipher Block Chaining	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).
CC	1. Common Criteria 2. Cryptographic Checksum	1. Common Criteria for Information Technology Security Evaluation 2. kryptografische Prüfsumme
CCS	Card Communication Service	
CEN	Comité Européen de Normalisation	Europäisches Komitee für Normung
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.
CETP	Connector Event Transport Protocol	
CG	cryptogram	Kryptogramm
CH	cardholder	*Karteninhaber*

Begriff	Synonym	Definition/Erläuterung
CHA	Certificate Holder Authorization	Berechtigung des *Karteninhabers*
Change Management	CM	Verfahren zur 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 of Change.
Change Request	CR, *Änderungsanforderung*	
Chipkarte		Plastikkarten, die mit einem Mikrochip zu Rechen- und Speicherzwecken versehen sind. Die Informationen werden in einem Halbleiterchip abgelegt, der mit einem Chipkarten-Lesegerät ausgelesen wird. Sicherheit kann durch einen *PIN* und mit Kryptoverfahren erreicht werden. Anwendung als Telefonkarte, Krankenversicherungskarte, Cash-Karte
CHR	Certificate Holder Reference	Referenz des *Karteninhabers*
CIA	Cryptographic Information Application	kryptografische Informationsanwendung
CIO	Cryptographic Information Objects	kryptografische *Informationsobjekte*
CLA		Class-Byte eines Befehls
Client-Application	*Primärsystem*	
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.
CM	Change Management	
CMET	Common Message Element Type	
CMM	Cabability Maturity Model	Modell zur Bewertung des Reifegrades der Organisation eines Software-Herstellers bei der Entwicklung von *Anwendungen*
CMS	Card Management System, *Kartenmanagementsystem*	
CMYK		*System* zur Definition einer Farbe; CMYK steht für Cyan (Türkis), Magenta (Fuchsinrot), Yellow (Gelb) und Key/blacK (schwarz)
Commit		Der Begriff aus dem Bereich Datenbanken bestätigt den erfolgreichen Abschluss einer Transaktion. Hierdurch wird das endgültige Speichern von Daten angestoßen. Das Gegenteil wäre hierbei ein *Roll Back,* wodurch die temporär gespeicherten Informationen auf den Ursprungswert zurückgesetzt würden.

Begriff	Synonym	Definition/Erläuterung
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.
Computational View		Der Computational View nach RMODP (Reference Model for Open Distriubuted 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.
Computerwurm		Schadsoftware, die sich über Netzwerke selbständig ausbreitet
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 Dokumentation eines logischen Abbildes der physikalischen und logischen *Infrastruktur* zuständig ist. Wichtige Aufgabe dabei ist die Darstellung der Relationen zwischen den *Configuration Items*. Zielsetzung ist die Versorgung der Betriebsprozesse mit aktuellen zuverlässigen Informationen, welche häufig in einer Datenbank verwaltet werden.
Connector Event Transport Protocol	CETP	Übertragungsprotokoll für die Meldung von Ereignissen im *Konnektor*
Coordinated Universal Time	UTC	Koordinierte Weltzeit. Sie stellt die aktuelle Weltzeit dar und hat in dieser Funktion, die vielen geläufige Greenwich Mean Time abgelöst. Sie ist eine Kombination aus der internationalen Atomzeit TAI und der Universalzeit UT. Die Zeitzonen werden als positive oder negative Abweichung von UTC angegeben (z. B. UTC + 2 entspricht der MESZ). UTC ist unter anderem die Referenzzeit im Internet und auch vielfach in Computersystemen.
COS	Card Operating System	Kartenbetriebssystem
CoS	Class of Service	Gruppe von Verfahren zur Priorisierung in *TCP/IP*-basiserten Netzwerken

Begriff	Synonym	Definition/Erläuterung
CPI	Certificate Profile Identifier	Kennung des Zertifikatsprofils
CR	*Change Request, Änderungsauftrag*	
CRL	Certificate Revocation List	Zertifikatssperrliste
Cross-Zertifikat		Ein Cross-Zertifikat ist ein *Public-Key-Zertifikat*, das eine *Zertifizierungsinstanz* für eine andere *Zertifizierungsinstanz* ausstellt.
CRT	Control Reference Template	
CS	CertSign, Certificate-Signing	
CT	Confidentiality Template	
CV	card verifiable	Echtheitsprüfung von *Chipkarten*
CVC	Card Verifiable Certificate	*Zertifikat* für ein asymmetrisches Verfahren zur gegenseitigen Echtheitsprüfung von systemzugehörigen *Chipkarten*
D		
DALE-UV		Datenaustausch mit *Leistungserbringern* in der gesetzlichen Unfallversicherung
Datenautorität		Begriff aus der *Telematikinfrastruktur*. Die Datenautorität bezeichnet den Akteur innerhalb einer Telematiknachricht, über dessen kryptographische Identität der Zugriff auf ein Objekt autorisiert wird.
Datenbearbeiter		Begriff aus der *Telematikinfrastruktur*. Der Datenbearbeiter ist der Aktor innerhalb einer Telematik-Nachricht, durch dessen kryptographische Identität die Berechtigung auf eine Funktion eines *Fachdienstes* nachgewiesen wird
Dateneigentümer	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 Dateneigentümer ist eine spezielle Form eines *Berechtigten* für *medizinische Datenobjekte*. Der Zusammenhang zwischen Dateneigentümer und ähnlichen Begriffen ist in der Definition des *medizinischen Datenobjektes* enthalten.
Datenklasse		Eine Datenklasse ist eine Menge von Informationsobjekten mit gleichartigen Eigenschaften.

Begriff	Synonym	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.
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.
Datenzugriffs-auditservice	*Audit Service*	
DAV	Deutscher Apothekerverband e.V.	
DCF77		DCF77 ist das von der Physikalisch-Technischen Bundesanstalt (http://ptb.de) in Mainflingen – südöstlich von Frankfurt – ausgestrahlte Funksignal, das die gesetzlich festgelegte Zeit gemäß Zeitgesetz trägt. Dieses Signal wird insbesondere von *Zertifizierungsdiensteanbietern* genutzt, um die Aktualität der Systemzeit der von Ihnen betriebenen OCSP- und TSP-Responder zu gewährleisten.
DDoS	Distributed Denial of Service	Prinzipiell gleiches Verfahren wie bei *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.
DDV	Daten Direkt Verbindung	
DE	Data Element, Datenelement	
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 mit einer derart hohen Anzahl von Anfragen, dass der Server diese nicht mehr oder nur noch mit einer unzureichend langen Antwortzeit (Timeout) verarbeiten kann.

Begriff	Synonym	Definition/Erläuterung
DER	Distinguished Encoding Rules	Die Distinguished Encoding Rules sind eine Untermenge der *BER (Basic Encoding Rules)* und sind eine Codierung von *ASN.1*-Datenbeschreibungen, die auf Bitebene völlig eindeutig ist.
DES	Data Encryption Standard	Steht für Data Encryption Standard und ist 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.
DEÜV		Datenerfassungs- und Übermittlungsverordnung
DF	Dedicated File	Dateiverzeichnis einer Chipkarte
DFA	Differential Fault Analysis	
DHCP	Dynamic Host Configuration Protocol	Dient der Zuweisung der Netzwerkkonfiguration an Geräte durch einen Server.
Dienst	Service	Der Begriff wird in der IT verwendet zur Bezeichnung von technischen, in sich geschlossenen Funktionskomponenten, die einen *Prozess* unterstützen. Der Dienst wird dabei über eines oder mehrere Netzwerkprotokolle der *Anwendungsschicht* realisiert.
Differential Fault Analysis	DFA	Differential Fault Analysis 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 Orginaltext 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	Definition/Erläuterung
Digitale Signatur	digital signature	Mit dem Begriff Digitale Signatur werden Daten in elektronischer Form bezeichnet, die anderen zu schützenden elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind (z.B. durch kryptografische Umformung der zu schützenden Daten). Sie belegen die Herkunft und *Integrität* der zu schützenden Daten und schützen damit gegen Fälschungen.
DIMDI	Deutsches Institut für medizinische Dokumentation und Information	
DIN	Deutsches Institut für Normung	
DIR	Directory	Verzeichnis
Disease-Management-Programm	*DMP*	Disease-Management-Programme (*DMP*) werden auch strukturierte Behandlungsprogramme oder einfach Chronikerprogramme genannt. Im Rahmen eines *DMP* soll eine Krankheit (englisch: Disease) optimal behandelt (gemanaged) werden.
Dispensierdaten		Information über die erbrachte Leistung und den *Leistungserbringer*, die der einlösende *Leistungserbringer* der *eVerordnung* hinzufügt.
DIVI	Deutsche interdisziplinäre Vereinigung für Intensiv- und Notfallmedizin	
DKG	Deutsche Krankenhausgesellschaft	
DKR	Deutsche Kodierrichtlinien	
DM	Display Message	
DMP	*Disease Management Programm*	
DMZ	De-Militarized Zone	
DNS	Domain Name System, Domain Name Service	
DO	Datenobjekt	
Domain Name		Name (Label) eines Teilbaumes innerhalb des Domain Namespace; identisch mit dem Namen des Node-Eintrags an der Spitze des besagten Teilbaumes.
Domain Name System	DNS	(Bereichsnamensystem). Bezeichnung für das im Internet verwendete System von hierarchisch gegliederten Bereichsnamen. Über die Domain-Datenbanken wird eine Zuordnung von sprechenden Server-Namen in IP-Adressen vorgenommen. So wird z.B. aus einem logischen DNS-Namen wie www.vianetworks.de eine numerische Adresse wie 194.77.111.24.

Begriff	Synonym	Definition/Erläuterung
Domain Name-space		Spezifikation einer hierarchischen DNS Baumstruktur, in der jeder Node- und Leaf- Eintrag unterschiedlichen Typen von Informationssätzen (siehe Ressource Re-cords) beinhaltet.
DoS	Denial of Service	
DPA	Differential Power Analysis	
dpi	Dots per Inch	Punkte pro Zoll
DRG	Diagnosis Related Groups	Im Rahmen des ab 2003 eingeführten Fallpauschalen-systems zur Vergütung der einzelnen Krankenhausfälle entstandenes ökonomisch-medizinisches Klassifikati-onssystem basierend auf diagnosebezogenen Fallgrup-pen.
DSA	*Digital Signature Al-gorithm*	
DSI	Digital Signature In-put	
DSL	Digital Subscriber Line	Digitaler Teilnehmeranschluss
DST	Digital Signature Template	Vorlage für digitale Signaturen
DTA-Abrechnung		Abrechnung per Datenträgeraustausch zwischen *Arzt* und *KV*
DTD	Document Type Defi-nition	
Durchsetzungs-einheit	Access Control En-forcement Unit, Policy Enforcement Point	Die Durchsetzungseinheit stellt sicher, dass nur berech-tigte 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 Netz-werk
E		
eArztbrief	*elektronischer Arzt-brief*	
ebXML	Electronic Business XML	
ECB	Electronic Code Book	Blockverschlüsselung
ECDSA	Elliptic Curve Digital Signature Algorithm	
EDI	Electronic Data Inter-change	elektronischer Datenaustausch

Begriff	Synonym	Definition/Erläuterung
EDIFACT	Electronic Data Interchange For Administration, Commerce and Transport	EDIFACT ist ein branchenübergreifender internationaler Standard (*ISO9735*) für den automatisierten Austausch elektronischer Daten im Geschäftsverkehr. Er ist einer von mehreren gebräuchlichen Standards für *EDI*.
EDV	elektronische Datenverarbeitung	
eEHIC	elektronische Europäische *Krankenversicherungskarte*	
EEPROM	Electrical Erasable Programmable Read Only Memory	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.
EF	Elementary File	In einem Elementary File sind Schlüssel abgelegt, die einzelnen Berufsgruppen in unterschiedlicher Kombination den Zugriff auf die Datensegmente, die ebenfalls in elementary files organisiert sind, erlauben.
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
EFID		Short EF Identifier
eGK	*elektronische Gesundheitskarte*	
eHC	electronic Health Card, *elektronischer Heilberufsausweis*	
EHIC	Europäische *Krankenversicherungskarte*	
Eigenanteil		Zuzahlungsteil des *Versicherten* an den Kosten ärztlicher, zahnärztlicher oder Krankenhausleistung oder eingelöster Arznei- oder Hilfsmitteln.

Begriff	Synonym	Definition/Erläuterung
einfache elektronische Signatur		*Elektronische Signatur* ohne *Verschlüsselung*. Bsp.: Eingescannte Unterschrift
Eingangsanforderung	input requirement	Anforderungssicht Eine Anforderung aus Sicht eines Konzeptes, die dieses Konzept zu berücksichtigen hat.
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	~~**Verordnungseinlöser**~~	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*.
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
eKiosk		Umgebung zur Wahrnehmung der Rechte des Versicherten. Mit Hilfe des eKiosk kann der *Versicherte* z.B. *eVerordungungen* ausblenden.
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 wurden.
Electronic Data Interchange	EDI	EDI ist ein Sammelbegriff für alle elektronischen Verfahren zum vollautomatischen Versand von strukturierten Nachrichten zwischen Anwendungssystemen unterschiedlicher Institutionen. Zu den möglicherweise wichtigsten Standards für EDI zählen *EDIFACT* und *ebXML*.
elektronische Gesundheitskarte	eGK	Die elektronische Gesundheitskarte ist gemäß § 291 a 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 § 291 a SGB V Angaben, die für die Übermittlung elektronisch veranlasster ärztlicher Verordnungen geeignet sind.

Begriff	Synonym	Definition/Erläuterung
elektronische Patientenakte	ePA	Die elektronische Patientenakte beinhaltet „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). Hierbei handelt es sich um eine *freiwillige Anwendung* der *eGK*.
elektronische Signatur	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 sehr leicht fälschbaren digitalen Abbildung einer handschriftlichen Unterschrift (*einfache elektronische Signatur*) bis hin zur *qualifizierten elektronischen Signatur* als sehr sichere Form der *digitalen Signatur*.
elektronische Verordnung	eVerordnung	o eVerordnung Arzneimittel Spezifische eVerordnung, die die elektronische Verordnung von apothekenpflichtigen Arzneimitteln sowie Betäubungsmittel gemäß Muster 16 abbildet. o eVerordnung Krankenhausbehandlung Spezifische eVerordnung, die die elektronische Verordnung von Krankenhausbehandlung gemäß Muster 2 abbildet. o 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. o 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.
elektronischer Arztbrief	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.
elektronischer Heilberufsausweis	HBA	Der elektronische *Heilberufsausweis* ist ein personenbezogener Ausweis im Gesundheitswesen, der an *Heilberufler* ausgegeben wird. Er beinhaltet (neben einer visuellen Ausweisfunktion) die Dienste *Authentifizierung*, *Verschlüsselung* und *elektronische Signatur* und ermöglicht den Zugriff auf Daten der *elektronischen Gesundheitskarte*.

Begriff	Synonym	Definition/Erläuterung
elektronisches Rezept	eRezept	Durch *eVerordnung* (schließt das eRezept ein) ersetzt. Signierter elektronischer Datensatz des *Rezeptes*, welches vom *Arzt* oder Zahnarzt erstellt wird und in der Apotheke oder *Versandapotheke* eingelöst wird. Dient laut § 291a Abs. 2, Satz 1 SGB V/GMG zur „Übermittlung ärztlicher Verordnungen in elektronischer und maschinell verwertbarer Form“. Hierbei handelt es sich um die Pflichtanwendung der *eGK*.
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.
EMV	Europay Mastercard Visa	
ENC	Encryption	*Verschlüsselung*
ENC( )	Encrypted data	verschlüsselte Daten
Engineering View		Der Engineering View nach RMODP (Reference Model for Open Distriubuted 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 View		Der Enterprise View nach RMODP (Reference Model for Open Distriubuted 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.

Begriff	Synonym	Definition/Erläuterung
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.
EOF	End-of-File	Dateiende
ePA	*elektronische Patientenakte*	
ephemer		nur für kurze Zeit bestehend, flüchtig, ohne bleibende Bedeutung
eRezept	*elektronisches Rezept*	
eSign	*elektronische Signatur*	
Ethernet		Derzeit gebräuchlichste LAN-Technologie
ETSI	European Telecommunication Standards Institute	Europäisches Telekommunikationsstandardinstitut. Koordinierungsstelle für Kompatibilitätsfragen europäischer Telekommunikationsentwicklungen.
EU	Europäische Union	
Evaluation		Bezeichnet die Auswertung der Testergebnisse durch die gematik mit dem Ziel, den jeweiligen Testerfolg festzustellen. Die Evaluation der Testergebnisse erfolgt anhand gemeinsam abgestimmter, einheitlich definierter Kriterien.
Evaluationsgegenstand	EVG	Bei einer Evaluation gemäß *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
eVerordnung	*elektronische Verordnung*	Elektronisches Transportmittel zur Übermittlung ärztlicher Verordnungen auf der *eGK* oder über die *Telematikinfrastruktur*.
EVG	*Evaluationsgegenstand*	
Extensible Markup Language	XML	universelle Datenbeschreibungssprache
F		
FA	Funktionsabschnitt Fachanwendung *Facharchitektur*	Die Bedeutung des Kürzels wird durch den Kontext bestimmt.

Begriff	Synonym	Definition/Erläuterung
Facharchitektur		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		Bezeichnung für die technische Umsetzung von Fachanwendungen wie z.B. zur Bereitstellung der *Versichertenstammdaten*, Verarbeitung der Verordnungsdaten oder der *freiwilligen Anwendungen* des *Versicherten*.
Fachkonzept		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.
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.
FAQ	Frequently asked question	Ein FAQ behandelt eine Verständnisfrage zu einem Thema oder Dokument. Die Beantwortung erläutert die betroffene Festlegung, ohne sie inhaltlich zu verändern.
FCP	File Control Parameter	
Feldtest		Der Feldtest bildet die 3. und 4. *Teststufe* der Testmaßnahmen zur Einführung der elektronischen Gesundheitskarte. 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.
FI	Clock Rate Conversion Factor	Frequenzumsetzungsfaktor
FID	File Identifier	Dateikennung
File Transfer Protocol	FTP	Netzwerkprotokoll zur Datenübertragung
Filialapotheke		Durch das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (*GMG*) ist es seit 01.01.2004 möglich, dass Apotheker neben ihrer Hauptapotheke weitere Apotheken (Filialapotheken) betreiben können.

Begriff	Synonym	Definition/Erläuterung
Financial Management	FM	*ITIL*-basierter *Prozess*, der die Kosten im Rahmen der Erbringung von IT-Services identifiziert, analysiert und eine realistische Methode für die Verrechnung der Kosten anwendet. Hierbei umfasst das Financial Management drei Unterprozesse, IT Service Budgeting, IT-Accounting und Leistungsverrechnung.
Firewall		Ein Firewall ist ein System aus Hardware und/oder Software, das den Zugriff zwischen zwei Systemen beschränkt und somit ein Regelwerk erzwingt.
Firmware		"Fest eingebrannte" Betriebssoftware eines Gerätes
Forensische Untersuchung	forensics	Untersuchung, ob und wie ein Angriff auf ein IT-System stattgefunden hat. (Allgemein: Suche nach Spuren eines Vergehens)
Fortgeschrittene elektronische Signatur		Eine fortgeschrittene elektronische Signatur ist gemäß § 2 Nr. 2 SigG [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
FPU Erweiterung	Floating Point Unit	Eine physische Erweiterung eines Systems, die zur schnelleren Verarbeitung von Gleitkommazahlen dient.
Framework		Der Begriff Framework stammt aus dem Bereich der Software-Entwicklung und bezeichnet ein Rahmenwerk. Diese Rahmenwerk schreibt vor, wie bestimmte *Systeme* zu implementieren sind, um Interoperabilität zu anderen *Systemen* zu gewährleisten
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 liegt nicht in der Verantwortung der gematik, deshalb erteilt sie hierfür eine Freigabe.
Freiwillige Anwendung		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*.
FTP	File Transfer Protocol	
Fully-Qualified Domain Name	FQDN	Ein absoluter Domain Name innerhalb eines *DNS* Namensraumes, der ausgehend vom Knoten, den er kennzeichnet, die Labels aller darüber liegenden Hierarchiestufen bis zum Wurzelverzeichnis (root) enthält.

Begriff	Synonym	Definition/Erläuterung
funktionale Anforderung	functional requirement	Eine funktionale *Anforderung* wird beschrieben durch einen Funktionsauslöser, eine erwartete Aktion und ein Ergebnis und definiert die Benutzbarkeit. WAS muss das Produkt erfüllen. Beispiele: Vollständigkeit, Angemessenheit, Korrektheit, Konsistenz, Robustheit, Fehlertoleranz, Betriebsprozessansprüche, Reife, Effizienz, Effektivität
Funktionale Eignung		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. Zur Durchführung der Prüfung hat das Testlabor der gematik eine Prüfvorschrift „Prüfung der funktionalen Eignung der eGK“ erstellt und wendet diese einheitlich an. Diese Prüfvorschriften können auf Anforderung zugesandt werden. 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 "nichtfunktionale" Eigenschaften sowie Aspekte der Sicherheit.
G		
Gateway	Protokollumsetzer	Ein Gateway erlaubt es Netzwerken, die auf völlig unterschiedlichen Protokollen basieren, miteinander zu kommunizieren.
GDO	Global Data Object	
Gebrauchstauglichkeit	usability	Gebrauchstauglichkeit eines Produktes definiert das Ausmaß, in dem es von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Kontext unter den Aspekten der Software-Ergonomie zu erreichen (IDIN EN ISO 9241). Sie unterteilt sich in die Bereiche *Benutzbarkeit* und *Benutzerfreundlichkeit.*
Geheimer Schlüssel		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
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*.)
Gesamtsystemtest		Im Rahmen des Gesamtsystemtests wird das Systemverhalten des Gesamtsystems unter Einbeziehung aller relevanten Komponenten getestet.

Begriff	Synonym	Definition/Erläuterung
Geschäfts-prozess		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.
Gesetzliche Krankenkasse		Körperschaft des öffentlichen Rechts, die Leistungen der *gesetzlichen Krankenversicherung* für ihre *Versicherten* gewährt.
Gesetzliche Kranken-versicherung	*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.
Gesundheits-karte	*eGK*, *elektronische Gesundheitskarte*	Wird im Rahmen des Projekts verwendet.
Gesundheitste-lematik		Der Begriff bezeichnet die Telematik im Gesundheitswesen und umfasst im Unterschied zu *Telematikinfrastruktur* nicht nur die technischen Komponenten, sondern auch die betrieblichen Aspekte und Dienstleistungen (siehe hierzu auch: Richtlinie für den Betrieb der Gesundheitstelematik [gemPolicy]).
GKV	*Gesetzliche Kranken-versicherung*	
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung	
GOÄ	Gebührenordnung für *Ärzte*	
goTOP	gematik offene Testorganisations-Plattform	
GP	Global Plattform	
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*)

Begriff	Synonym	Definition/Erläuterung
GSHB		IT-Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik
gSP	gematik-Standardisierungs-Prozess	
H		
Hacker		Unauthorisierte Person, die sich Zugang zu oder Zugriff auf ein IT-System verschaffen will (Anm: dies trifft noch keine Aussage darüber, ob diese Person auch tatsächlich böswillige Absichten hat!)
Halbleiterhersteller		Der Halbleiterhersteller hat (neben der eigentlichen Herstellung des Chips, der in die Karte implantiert wird) im Kontext der *eGK* zwei wesentliche Aufgaben, die für die Sicherheit des gesamten *Systems* von großer Bedeutung sind: 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*.
HARP	Harmonization for the security of web technologies and applications	
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.
HB	Historical Bytes	Die Historical Bytes sind eine Kette von maximal 15 Bytes, deren Inhalt nicht festgelegt ist.
HBA	*Heilberufsausweis*	

Begriff	Synonym	Definition/Erläuterung
HCA	Health Care Application, Gesundheitsanwendung	
Health Level 7	HL7	Health Level 7 ist ein internationaler Standard für den Austausch von Daten zwischen Computersystemen im Gesundheitswesen. Die 7 des Namens bezieht sich auf die Schicht 7 des ISO/OSI-Referenzmodell für die Kommunikation (ISO7498-1) und drückt damit aus, dass hier die Kommunikation auf Applikationsebene beschrieben wird.
Health Professional Card	HPC	HPC ist der englische Begriff für *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.
Heilberufsausweis	*Health Professional Card, HBA, HPC*	Heilberufsausweis ist eine personenbezogene Mikroprozessorchipkarte mit kryptographische Funktionen, mit dem sich Angehörige der Heilberufe (z.B. *Ärzte* und Apotheker) gegenüber der *Telematikinfrastruktur* ausweisen und vertraulich (verschlüsselt) kommunizieren können. Außerdem enthält er eine *qualifizierte elektronische Signatur* des entsprechenden *Leistungserbringers*.
Heim-PC		Bezeichnung für den privaten Computer eines Versicherten. Ähnlich wie der *eKiosk* ist grundsätzlich auch der Heim-PC des *Versicherten* ein mögliches *Primärsystem*, sofern dieser u. a. über ein Kartenlesegerät und einen Internetanschluss verfügt. Da der Heim-PC als unsicheres *System* anzusehen ist, müssen allerdings vor einer Nutzung für die *eGK* insbesondere Sicherheitsaspekte berücksichtigt werden.
HL7	*Health Level 7*	
HP	Health Professional, *Heilberufler*	
HPC	Health Professional Card, *Heilberufsausweis*	
HSM	Hardware Security Module	
http	Hypertext Transfer Protocol	

Begriff	Synonym	Definition/Erläuterung
Hybridschlüssel	hybridkey	Ein symmetrischer kryptographischer Schlüssel, der durch den öffentlichen Schlüssel eines Public-Key-Schlüsselpaares verschlüsselt wurde und somit nur durch den Besitzer des privaten Schlüssels des Schlüsselpaares lesbar ist.
Hypertext Transfer Protocol	http	HTTP ist ein Protokoll zur Übertragung von Daten, das insbesondere im Rahmen des World Wide Web zum Einsatz kommt und sich meist auf das verbindungsorientierte TCP stützt.
I		
IANA	Internet Assigned Numbers Authority	
ICC	Integrated Circuit Card	
ICCSN	Integrated Circuit Card Serial Number	
ICM	IC Manufacturer, IC-Herstellerkennung	
ID	Identifier	eindeutiger Schlüssel zur *Identifizierung* von Objekten
ID des verordneten Mittels		Mit der Identifikationsnummer (ID) eines Arzneimittels ist derzeit die 7-stellige Pharmazentralnummer (PZN) gemeint, die zukünftig durch die Europäische Arzneimittelnummer (EAN) ersetzt wird. Arzneimittel oder sonstige Heil- und Hilfsmittel, die per se keine *PZN* haben werden gruppenweise einer *PZN* zugewiesen.
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.
IEC	International Electrotechnical Commission	
IEEE	Institute of Electrical and Electronics Engineers	
IETF	Internet Engineering Task Force	

Begriff	Synonym	Definition/Erläuterung
IFD	Interface Device	
IFSC	Information Field Size Card	
IFSD	Information Field Size Device	
IIN	Issuer Identification Number	Kennung des Kartenanbieters
IK		*Institutionskennzeichen*: Ordnungsbegriff für Teilnehmer am Telematikprozess
Implementierung		Integration neuer Elemente in bestehende Strukturen. 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 eine Störung, Anfrage oder Aufträge qualifiziert und formalisiert beschreibt.
Incident Management	IM	*ITIL*-basierter Prozess, der alle *Incidents* registriert, kategorisiert, priorisiert und verfolgt. Die primäre Zielsetzung ist eine schnellstmögliche Bearbeitung der *Incidents*.
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*.
Information View		Der Information View nach RMODP (Reference Model for Open Distriubuted Processing nach SAGA [SAGA]) beschreibt die Ausprägung und Semantik der verarbeiteten Daten, sowie die detaillierten Prozesse zur Datenverarbeitung. Diese Sicht legt die Struktur und Semantik der Informationen des Systems fest. Weitere Punkte sind die Definition von Quellen und Senken von Information sowie die Verarbeitung und Transformation von Information durch das System. Hierzu gibt es Integritätsregeln und Invarianten.
Informationsmodell		Das Informationsmodell gibt die fachliche Beschreibung (eindeutige Bezeichnung und Definition) der benötigten *Informationsobjekte* in einem definierten Kontext wieder (z.B. die der *Versichertenstammdaten* auf der Grundlage des §291 Abs. 2 SGB V).

Begriff	Synonym	Definition/Erläuterung
Informationsobjekt		Logisches Element des *Informationsmodells*. Für das Informationsobjekt sind Anforderungen festgelegt wie z.B. Sicherheitsziele, welche wiederum nach bestimmten (Sicherheits-)Eigenschaften der die Informationsobjekte verarbeitenden Komponenten verlangen.
Informationssicherheit	IT- Security	Die Informationssicherheit schafft auf der Ebene der Informationstechnik (*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.
Informative Anforderung	informative requirements	Informative Anforderungen werden an Beteiligte der *Telematikinfrastruktur* gestellt, dabei liegt die Umsetzung dieser *Anforderungen* jedoch nicht im Hoheitsgebiet der gematik. Bsp. Anforderungen an *Primärsysteme*
Infrastruktur		System von Einrichtungen, Ausrüstungen und Dienstleistungen, welches für den Betrieb einer Organisation erforderlich ist.
Installation		Funktionsfähige Bereitstellung von Hardware und Software in einer definierten Umgebung.
Institute of Electrical and Electronics Engineers	IEEE	IEEE (sprich ei trippel i) ist ein weltweiter Verband von Ingenieuren und Informatikern. Eine der Aufgaben des IEEE ist die Definition von Standards wie zum Beispiel des WLAN Standards (IEEE 802.11)
Institution (medizinische)		In der Telematikinfrastruktur handelt es sich bei der Institution des Leistungserbringers [Leistungserbringer] 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		Die Institutionskarte entspricht technisch weitgehend der *Health Professional Card*, ist jedoch institutionsbezogen und wird lediglich bei Systemstart mit einer *PIN* freigeschaltet. In diesem Fall wird sie auch als *Security Module Card (SMC)* bezeichnet. Die Institutionskarte funktioniert nur in Verbindung mit einem *HBA*.
Institutionskennzeichen	IK	Das Institutionskennzeichen ist ein eindeutiges Merkmal für die *Identifizierung* von *Kostenträgern* und bestimmten *Leistungserbringern* (z.B. Apotheken)

Begriff	Synonym	Definition/Erläuterung
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. Ziel des Integrationstests ist die *Identifikation* von Fehlern in der Interaktion zwischen Komponenten. 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 bezeichnet den Zustand der Korrektheit und Unverfälschtheit von Daten. Es sind nur erlaubte und beabsichtigte Veränderungen zugelassen und möglich. Datenintegrität bezeichnet die Integrität von gespeicherten und übertragenen Daten. Systemintegrität bezeichnet die Unverfälschtheit von Programmen und 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 eines *Systems*, auf die durch andere *Systeme* zugegriffen werden kann
InterKom		Sicherstellung der Interoperabilität und Kompatibilität
Intermediär		Vermittler zwischen zwei *Systemen*, wobei beide *Systeme* jeweils dem Intermediär vertrauen, nicht jedoch zwangsweise einander.
International Organization for Standardization	ISO	Die ISO (http://www.iso.org) ist eine internationale Vereinigung der Standardisierungsgremien von 151 Ländern. Sie verabschiedet internationale Standards in allen technischen Bereichen. Deutschland ist durch das Deutsche Institut für Normung (*DIN*) (http://www.din.de) und die USA durch *ANSI* in der *ISO* vertreten.
International Telecommunication Union	ITU	Die ITU ist eine weltweite Organisation, die sich mit technischen Aspekten der Telekommunikation beschäftigt. In ihrem Telecommunication Standardization Bureau (ITU-T) werden technische Normen erarbeitet und als Empfehlung veröffentlicht.

Begriff	Synonym	Definition/Erläuterung
Internet Assigned Numbers Authority	IANA	Diese nicht-kommerzielle Organisation ist unter anderem für die Zuweisung von im Internet Protokoll verwendeten Portnummern zuständig.
Internet Engineering Task Force	IETF	Die Internet Engineering Task Force (IETF) ist eine große, offene, internationale Gemeinschaft, die sich um den reibungslosen Betrieb und die Weiterentwicklung der Internet-Architektur bemüht. Die in der IETF entwickelten Standards und Empfehlungen werden als Request for Comments (*RFC*) mit einer bestimmten laufenden Nummer unter http://www.ietf.org veröffentlicht.
Internet Protocol Security	IPSec	IPsec ist eine von der *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.
Interoperabilität		Zusammenarbeit in einem offenen *System* (gemäß dem Client/Server-Modell). Unabhängig von der verwendeten Hardware, den eingesetzten Betriebssystemen, der verwendeten Netzwerktechnologie und der Realisierung einer *Anwendung* kann eine Zusammenarbeit zwischen diesen *Anwendungen* erfolgen.
Interoperabilitätstest		Nachweis der Austauschbarkeit von einzelnen Komponenten unterschiedlicher Hersteller/Betreiber
IP	Internet Protokoll	
IPSec	Internet Protocol Security	
ISDN	Integrated Services Digital Network	
ISIS-MailTrusT	ISIS-MTT	ISIS-MTT ist eine gemeinsame Spezifikation von TeleTrusT e.V. (http://www.teletrust.de) und T7 e.V. (http://www.t7-isis.de) für *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.
ISIS-MTT	Intermediate System – Intermediate System MailTrusT-Standard	Spezifikation international verbreiteter und anerkannter Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen.
ISO	International Organization for Standardization	die internationale Vereinigung der Standardisierungsgremien von derzeit 148 Ländern
ISO 17799		vollständige Bezeichnung: ISO/IEC 17799:2000 (Information technology - Code of practice for information security management); entspricht inhaltlich dem British Standard Nr. 7799, Teil 1 (BS 7799-1:1999)

Begriff	Synonym	Definition/Erläuterung
ISO 27001		vollständige Bezeichnung: ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements); spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation.
ISO/IEC 7816		Normenreihe für *Chipkarten*
IT		Informationstechnik
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.
ITIL	IT Infrastructure Library	ITIL ist ein in Großbritannien entwickelter Leitfaden zur Unterteilung der Funktionen und Organisation der Prozesse, die im Rahmen des Betriebs einer IT-Infrastruktur eines Unternehmens entstehen (*IT Service Management*).
ITSEC	Information Technology Security Evaluation Criteria	Die Kriterien für die Bewertung der Sicherheit von *Systemen* in der Informationstechnik sind ein europäischer Sicherheitsstandard
ITU	International Telecommunication Union	
IV	Initial Value	
K		
Kartenanwendung	card application	Die Kartenanwendung ist eine spezielle Form einer *Anwendung*.
Kartenanwendungsmanagement	*Card Application Management, CAM*	Verwaltung der *Kartenanwendungen* einer *eGK* – im Rahmen der Festlegungen zur *Telematikinfrastruktur* wird dieser Funktionsbereichung unter *Kartenmanagement* (*CM*) subsumiert.
Kartenanwendungsmanagementsystem	*Card Application Management System, CAMS*	System für das *Kartenwendungsmanagement* – im Rahmen der Festlegungen zur *Telematikinfrastruktur* wird dieser Funktionsbereichung unter *Kartenmanagementsystem* (*CMS*) subsumiert.
Kartenherausgeber		Der Kartenherausgeber ist i.d.R. Eigentümer der Karte. Er ist verantwortlich für die Zuordnung einer Karte zu einer Person und veranlasst Ausstellung und Einzug von Karten. Der Begriff „Kartenherausgeber“ wird im Rahmen des Projekts *eGK* als *Akteur* verwendet.
Karteninhaber		Der Karteninhaber ist die Person, welche die Entscheidungsbefugnis über den Einsatz einer *eGK* im Gesundheitswesen hat. Im Allgemeinen ist dies der *Versicherte* selbst.

Begriff	Synonym	Definition/Erläuterung
Kartenlebens-zyklus		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.
Karten-management	Card Management, CM	Vom *Kartenherausgeber* zur Verwaltung der *eGK* über den gesamten Lebenszyklus benötigte Anwendung. Das Kartenmanagement umfasst dabei die Ausgabe und Verwaltung von Karten und kartenbezogenen Daten. Es besteht aus den Einzelanwendungen Lebenszyklusmanagement, Validitätsmanagement, Anwendungsmanagement, *Kartenanwendungsmanagement*, Datenerhalt- und Schlüsselmanagement.
Karten-management-system	Card Management System, CMS	System für das *Kartenmanagement*
Karten-personalsierer		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.
Kartensystem	Card System, CS	Gesamtsystem aller zur Verwaltung der *eGK* erforderlichen *Komponenten*. Dieses umfasst neben dem eigentlichen *Kartenmanagementsystem* zum Beispiel auch die *Komponenten* zur Verwaltung der zur *eGK* zugehörigen Schlüssel und *Zertifikate*.
Kartenterminal		Technische Einrichtung zum Kontaktieren der im *System* verwendeten *Chipkarten*
Kartenversen-der		Der Kartenversender übernimmt das Mailing der Karte. Dies umfasst im Allgemeinen das Personalisieren eines Anschreibens, das Aufbringen der personalisierten Karte auf das Anschreiben, das Kuvertieren und die Übergabe an ein Zustellunternehmen. Der Begriff „Kartenversender“ wird im Rahmen des Projekts *eGK* als *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 *Lebenszyklus der Karte* zu koordinieren.
KB		Kilo Byte
KBSt		Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KBV		Kassenärztliche Bundesvereinigung
KD	Key derivation Data	dient der Sicherung elektronischer Nachrichten

Begriff	Synonym	Definition/Erläuterung
Kettenmodell		Das Kettenmodell ist ein so genanntes Gültigkeitsmodell für Zertifizierungspfade, bei dem alle *Zertifikate* im Pfad genau dann gültig sind, wenn der zugehörige *Zertifizierungsschlüssel* zum Zeitpunkt der Erstellung (des *Zertifikats*) auf einem gültigen *Zertifikat* beruht.
Key Performance Indikator	KPI	Eine Messgröße, die einen Prozess, 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 Berichtserstellung in Bezug auf den Prozess, den IT Service oder die Aktivität eingesetzt. Bei der Auswahl der KPIs sollte die Sicherstellung von Effizienz, Effektivität und Wirtschaftlichkeit berücksichtigt werden.
KGK	Key Generation Key	Ein Key Generator ist ein Programm welches zum einen automatisch nach einem Algorithmus Seriennummern oder Freischaltungscodes erstellt und zum anderen Passwörter für Verschlüsselungsmechanismen erzeugt.
KIS	Krankenhausinformationssystem	*Primärsystem* der Krankenhäuser
Kiss-'o-death		Mit Hilfe dieses Verfahrens kann der *NTP-Server* die Anzahl der an ihn gerichteten Anfragen von korrekt implementierten und hierarchisch untergeordneten *NTP-Servern* beeinflussen. Das Verfahren ist in Abschnitt 5.1.1.16 des Dokumentes „Spezifikation Infrastrukturkomponenten: Zeitdienst" beschrieben.
KK	Krankenkasse	
KM	CM	*Kartenmanagement*
KMS	CMS	*Kartenmanagementsystem*
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)
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. Die Verwendung des Begriffes in der *Telematikinfrastruktur* orientiert sich an der Verwendung des Begriffes Komponente in der Unified Modelling Language (UML).
Komponentenleistungstests		Im Rahmen der *Komponententests* finden auch Leistungstests statt (Lastverhalten (Lasttest), Antwortzeit- und Durchsatzverhalten (Performanztest), Verhalten in Abhängigkeit von Datenmengen (Massentest) sowie Verhalten bei Überlast (Stresstest).

Begriff	Synonym	Definition/Erläuterung
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*).
Komponenten-test		Im Rahmen der Komponententests werden funktionale Aspekte (inkl. funktionaler Sicherheit) in der Labortest- bzw. zukünftig Komponententestumgebung
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.
Konkatenation		Die Konkatenation (auch Verkettung) ist der Vorgang und das Ergebnis der regelhaften linearen Aneinanderreihung von sprachlichen Elementen oder linguistischen Kategorien. Konkatenationen verknüpfen mindestens zwei Elemente (z.B. NP + VP), deren Reihenfolge durch die Verkettungsoperation festgelegt ist. In der generativen Transformationsgrammatik werden Konkatenationen durch Ersetzungsregeln im Basisteil erzeugt.
Konnektor		Der Konnektor koordiniert die Kommunikation zwischen *Primärsystem, eGK, HBA/SMC* und *Telematikinfrastruktur*. Er stellt damit das Bindeglied zwischen diesen Komponenten auf Leistungserbringerseite bzw. *eKiosk* und *Telematikinfrastruktur* dar.
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.
Kostenerstattungsverfahren	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	Eine Person oder Institution, die für eine erbrachte Leistung die entstandenen Kosten ganz oder teilweise übernimmt. Im Kontext der *eGK* wird hiermit die Gruppe der (*privaten und gesetzlichen) Krankenversicherungen* bezeichnet. Der Begriff „Kostenträger" wird im Rahmen des Projekts *eGK* als *Akteur* verwendet.
Kostenträger-kennung		Institutionskennzeichen der *Krankenversicherung*
KPI	*Key Performance Indikator*	

Begriff	Synonym	Definition/Erläuterung
Krankenversichertenkarte	KVK	*Chipkarte*, welche seit 1995 den Krankenschein ersetzt hat. Die Karte enthält reine Verwaltungsdaten (*Krankenkasse*, Name, Geburtsdatum und Anschrift des *Versicherten*, *KVNR* und *Versichertenstatus*).
Krankenversichertennummer	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)
Krankenversicherung		Die Krankenversicherung umfasst die *Gesetzliche und Private Krankenversicherung.*
Krypto Subsystem		Funktionsfeld zur Verarbeitung von *PKI* Anwendungen (Signaturerstellung, -prüfung, Datenverschlüsselung, -entschlüsselung)
KV		Kassenärztliche Vereinigung
KVK		*Krankenversichertenkarte*
KVNR		*Krankenversichertennummer*
KZBV		Kassenzahnärztliche Bundesvereinigung
KZV		Kassenzahnärztliche Vereinigung
L		
L2TP	Layer 2 Tunneling Protocol	L2TP kommt als Protokoll bei Virtuellen Privaten Netzwerken zum Einsatz. Es dient zum Aufbau einer abgesicherten Verbindung zwischen zwei Netzwerken über ein ungesichertes Medium wie zum Beispiel das Internet.
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 Laborbedinungen mit Testdaten durch. Die Ziele der Labortests sind: - *Komponententests* - *Integrationstests* - *Interoperabilitätstests* - *Sicherheitstests*
LAN	Local Area Network	Lokales Netzwerk (z. B. innerhalb einer Arztpraxis oder Apotheke)
Lasttest	performance test	Test des Systemverhaltens in Abhängigkeit einer ansteigenden Zahl an Benutzern/Transaktionen oder des Datenvolumens.

Begriff	Synonym	Definition/Erläuterung
LDAP	Leightweight Directory Access Protocol	
LE	*Leistungserbringer*	
Lebenszyklus		Im Zusammenhang mit dem *Kartenmanagement* ist der Lebenszyklus der Karte gemeint. Siehe *Kartenlebenszyklus*.
Leistung		Jede in Verbindung mit der medizinischen Versorgung durch einen *Leistungserbringer* durchgeführte oder auch erbrachte Handlung. Eine Leistung kann aus mehreren Einzelleistungen bestehen. Eine Leistung ist ein Synonym für eine *medizinische Maßnahme*.
Leistungsanforderung	performance requirement capacity requirement benefit requirement	Leistungsanforderungen beziehen sich immer auf andere *Anforderungen*. In Bezug zu *funktionalen Anforderungen* werden Erfüllungsgrad (Abdeckung z.B. in %), Performance (Reaktionszeit in der Mensch-Maschine-Schnittstelle) oder Skalierungsangaben benötigt, im Bereich der *nicht-funktionalen Anforderungen* sind beispielhaft Durchlaufzeiten eines Standard-Workflows, aber auch Vorgaben zu Kosten-Nutzen-Verhältnissen nicht unüblich. WIE GUT muss das Produkt erfüllen. Beispiele: Schnelligkeit, Skalierbarkeit, Maßangaben zu *funktionalen Anforderungen* im Sinne von Messeinheit, Messwert, Messgrenzen
Leistungserbringer	LE	Ein Leistungserbringer gehört zu einem zugriffsberechtigten Personenkreis nach §291a Abs. 4 SGB V und erbringt Leistungen des Gesundheitswesens für Versicherte. Der Personenkreis umfasst abschließend: Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Apothekenassistenten, Pharmazieingenieure, deren berufsmäßige Gehilfen, Psychotherapeuten, sonstige Erbringer ärztlich verordneter Leistungen, Angehörige eines anderen Heilberufs mit staatl. geregelter Ausbildung. Der Begriff „Leistungserbringer“ wird im Rahmen des Projekts eGK als Akteur verwendet.
Leistungserbringerorganisation		Standesorganisation von Leistungserbringern (KBV, BÄK, DAV, DKG etc.)
Leistungsniveau	Service Level	Im Rahmen eines *Leistungsvertrags* definierte *Leistung*.

Begriff	Synonym	Definition/Erläuterung
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*).
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*)
Leonardo		Symbolfigur im deutschen Gesundheitswesen ist die von Leonardo da Vinci in den Jahren um 1490 geschaffene Skizze "Proportionsschema der menschlichen Gestalt nach Vitruv". Auf der *eGK* ist diese Figur in einer gematik-spezifischen Fassung als verpflichtendes Erkennungsmerkmal dargestellt. Umgangssprachlich und auch in der eGK-Spezifikation Teil 3 wird sie als "Leonardo" bezeichnet
Lightweight Directory Access Protocol	LDAP	Mit dem Lightweight Directory Access Protocol (Spec. RFC2251) können Informationen, die in einem Verzeichnisdienst gespeichert sind, abgerufen oder modifiziert werden.
Linux		Populäres, quelloffenes UNIX Betriebssystem
Load Balancing		Lastenverteilung zwischen zwei Systemen, die den gleichen Dienst anbieten.
Logdaten, Logs		Daten über Ereignisse, z.B. Störungen
Logging		In der *Telematikinfrastruktur* wird mit Logging die technische *Protokollierung* bezeichnet, dabei werden technische Daten, wie z. B. der Systemstatus eines Servers, protokolliert.
Lösungs-architektur	solution outline	Ergebnisdokument des Vorprojektes *biT4health*: Darin wurde an Hand der in der *Rahmenarchitektur* vorgegebenen Regeln die *Telematikinfrastruktur* weiter detailliert.

Begriff	Synonym	Definition/Erläuterung
Low-Level-Signaturformat		Bei Low-Level-Signaturformaten ist bitgenau spezifiziert, wie die zu signierenden Daten, oder ein *Hash-Wert* derselben, vor der eigentlichen *Anwendung* des asymmetrischen Kryptoalgorithmus, z.B. durch Füllmechanismen (*Padding*), aufzubereiten sind.
M		
MAC	Message Authentication Code	
MAC Adresse		eindeutige Hardware Adresse einer Netzwerkkarte
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 *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.
Materialtechnische Eignung		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.
MB	Mega Byte	
MDO	*Medizinisches Datenobjekt*	
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.

Begriff	Synonym	Definition/Erläuterung
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.
Medizinische Daten		Medizinische Daten sind im Kontext der *eGK* ein Synonym für „*Klinische Daten*“.
Medizinische Maßnahme		Generisch für verschiedene Behandlungsarten (Diagnostik, operativer Eingriff, pflegerische Maßnahme, Rehabilitationsmaßnahme), unabhängig von der Art der durchführenden Einrichtung und der Dauer. Eine Maßnahme kann aus mehreren Einzelmaßnahmen bestehen. Eine medizinische Maßnahme ist ein Synonym für eine Leistung.
Medizinisches Datenobjekt	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 ist. 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.
Mehrwertanwendung		Eine Mehrwertanwendung im Sinne der *Telematikinfrastruktur* ist eine Fachapplikation, die für mindestens eine Nutzergruppe der *Telematikinfrastruktur* einen – wie auch immer gearteten – Nutzwert darstellt, selbst nicht Teil der durch die *Telematikinfrastruktur* spezifizierten Komponenten, Dienste oder Funktionalitäten ist und Teile der *Telematikinfrastruktur* (Karten, dezentrale oder zentrale Komponenten) nutzt. Der *HBA* wird hier nicht als Teil der *TI* gesehen, die Nutzung außerhalb der *TI* ist hier ohne weiteres möglich. Daneber werden Unterstützungsfunktionen der *TI* (z.B. Signieren mit dem *Konnektor*) nicht als Mehrwertanwendungen bezeichnet, sondern erst die *Fachanwendung*, die diese Funktionen nutzt.
Mehrwertanwendung des Typs 1		Lokale Mehrwertanwendungen In diese Kategorie fallen *Mehrwertanwendungen*, die die durch die dezentralen Komponenten der *Telematikinfrastruktur* beim *Leistungserbringer* lokal angebotenen Funktionen nachnutzen.
Mehrwertanwendung des Typs 2		Informationstechnisch von der *TI* getrennte *Mehrwertanwendungen* Mehrwertanwendungen, die Dienste außerhalb der *Telematikinfrastruktur* nutzen (in eigenen Netzen – Mehrwertnetze), wobei die dezentralen Komponenten der *Telematikinfrastruktur* einen transparenten Zugang zu diesen Netzen schaffen.

Begriff	Synonym	Definition/Erläuterung
Mehrwertan-wendung des Typs 3		Nachnutzung von Infrastruktur durch Mehrwertanwen-dungen Bestimmte Infrastrukturdienste sind auch für die Nut-zung durch Anwendungen außerhalb der Telemati-kinfrastruktur interessant, beispielsweise der Zugriff auf die Verzeichnisse von Leistungserbringern. Die Mehr-wertanwendungen, die diese zentrale Infrastruktur nachnutzen, selbst aber keine zentralen Bestandteile haben, werden als Typ 3 - Mehrwertanwendungen be-zeichnet.
Mehrwertan-wendung des Typs 4		Mehrwertanwendungen als Fachanwendungen in der TI Analog zu den gesetzlich geregelten Anwendungen können auch Mehrwertanwendungen zentrale Dienste umfassen und die technischen Mechanismen der ge-setzlichen Anwendungen in vollem Umfang nachnutzen. Diese Mehrwertanwendungen werden als Typ 4 - Mehrwertanwendungen bezeichnet.
Mehrwertclient		Ein Mehrwertclient ist eine Client-Komponente einer Mehrwertanwendung außerhalb der Telematik-infrastruktur, die über die Primärsystemschnittstelle des Konnektors Funktionen nutzt, die die TI für Mehrwert-anwendungen anbietet.
Mehrwertdienst		Als Mehrwertdienst wird eine zentrale Anwendungs-komponente einer Mehrwertanwendung bezeichnet. Dies kann sich sowohl auf einen Server in einem Mehr-wertnetz beziehen als auch auf einen Fachdienst einer Typ-4 Mehrwertanwendung.
Mehrwertfach-dienst		Ein Mehrwertfachdienst ist ein Mehrwertdienst innerhalb der Telematikinfrastruktur, d.h. Server einer Typ-4 Mehrwertanwendung.
Mehrwertmodul		Ein Mehrwertmodul ist eine Client-Komponente einer Mehrwertanwendung auf dem Konnektor (als Gerät). Diese Komponente nutzt vom Konnektor aus die glei-chen Funktionen wie ein Mehrwertclient.
Message Au-thentication Code	MAC	Ein Message Authentication Code (MAC) dient zur Si-cherung 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 ent-hält, 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 auszuse-hen hat. Ein Metamodell ist somit ein Modell auf einer höheren Abstraktionsebene.
MF	Master File	
Migration		Übergang einer *Betriebsumgebung* von einem *Release* oder Versionsstand (bspw. Funktionsabschnitt) auf den Nächsten.

Begriff	Synonym	Definition/Erläuterung
Migrationspfad		Der Migrationspfad beschreibt die Einführung der *eGK* in mehreren abgesicherten und beherrschbaren Stufen
MII	Major Industry Identifier	
Mikroprozessorchipkarte	SmartCard	Ist eine *Chipkarte* mit einer kleinen CPU und arbeitet wie ein kleiner Computer. Enthält außerdem einen ROM mit Betriebssystem und RAM. Zum Beispiel Kryptoverfahren können so auf der Karte implementiert werden.
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.
MKT	*Multifunktionales Kartenterminal*	
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		Laufende Überwachung bestimmter kritischer Informationen, z.B. verfügbare Bandbreite, CPU-Auslastung, Anzahl fehlgeschlagener Verbindungsversuche aber auch nicht technischer Aspekte wie Rechtslage.
MPLS	Multi Protocol Label Switching	Netzwerk-Transportprotokoll zur performanten Weiterleitung von (No Suggestions), besonders effizientes Verfahren zur Bildung von VPNs auf WANs
MSB	Most Significant Byte	
MSE	Manage Security Environment	dient zur Zertifikatsverifikation

Begriff	Synonym	Definition/Erläuterung
Multiapplikative Chipkarte		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.
Multifunktionales Kartenterminal	MKT	Zum Lesen und Beschreiben von Karten werden *Kartenterminals* benötigt. Für das Gesundheitswesen wurde in den vergangenen Jahren ein „Multifunktionales Kartenterminal (MKT)" entwickelt, das auch in europäischen Projekten internationale Anerkennung gefunden hat. Das MKT ist für alle *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. Höherwertige Terminals können auch mit Zahlungsfunktionen ausgestattet werden. Die *Spezifikation* ist im Internet unter der Adresse http://sit.gmd.de/SICA/mkt.html verfügbar (Quelle: [WuV])
Musterpraxis		Die Musterpraxis bildet die technische Infrastruktur einer Arztpraxis einschließlich Apotheke musterhaft nach. Sie dient der frühzeitigen Demonstration der Funktionsweise und Praktikabilität geplanter Lösungen. Im Sinne einer *QS* hat sie keine definierte *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 Gesundheitskartenanwendung bereit. Dabei wird ein *Primärsystem* oder Primärsystemsimulator mit *Konnektor* und *Kartenterminal* so verbunden, dass die Fachanwendungen durchgeführt werden können. Die Musterumgebung dient zum *Anwendertest*.
N		
Nachladeprozess	Post Issuance Process, PIP	Nachladen von *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 (siehe Ressource Records) für anfragende Resolver bereitstellt.
NAT	Network Adress Translation	
National Institute for Standards and Technology (NIST)		Das NIST ist ein staatliches Standardisierungsinstitut in den USA. Zu den vom NIST publizierten Standards zählt beispielsweise *DSA* und *SHA-1*.

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

Begriff	Synonym	Definition/Erläuterung
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. In ihm wird in einem Rechnersystem das *BIOS* oder die Firmware abgelegt.
Notfalldaten		Elektronischer Datensatz auf der *eGK* mit den Daten zu notfallrelevanten Informationen wie z.B. Allergien.
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*..
NTP-Server		Serversysteme, die mittels NTPd (*NTP* deamon) 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.
NVRAM	Non Volatile Random Access Memory	NVRAM ist eine Speichertechnologie in der Elektronik, die auch ohne Aufrechterhaltung der Energieversorgung die Information halten kann.
O		
OASIS	Organization for the Advancement of Structured Information Standards	*OASIS* (http://www.oasis-open.org) ist ein nichtkommerzielles, globales Konsortium für die Entwicklung und Umsetzung von Standards für eBusiness und *XML*.
ObjektReferenz		Eindeutiger Verweis auf ein Objekt innerhalb eines Fachdienstes, bestehend aus Diensttyp, Dienstinstanz und Objekt ID des Objektes. Durch die Objekt Referenz kann jedes Objekt innerhalb der *Telematikinfrastruktur* eindeutig adressiert werden.
ObjektTicket		Ein ObjektTicket bezeichnet Berechtigungsinformationen zu einem Objekt. In einem ObjektTicket sind sowohl die Informationen über die Zugriffsrechte einer Identität auf ein Objekt als auch der *Hybridschlüssel* für eine zugelassene *Identität* enthalten.

Begriff	Synonym	Definition/Erläuterung
OCSP	Online Certificate Status Protocol	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.
Öffentlicher Schlüssel	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.
OID	Object Identifier	Objektkennung
Online Certificate Status Protocol	OCSP	*OCSP* ist ein in RFC2560 von der *IETF* standardisiertes Client-Server-Protokoll zur Abfrage des Status von *Zertifikaten*. Mittels dieser Online Abfrage kann beispielsweise geprüft werden, ob ein *Zertifikat* durch den *Benutzer* gesperrt worden ist.
OP	Offene(r) Punkt(e)	
Open Systems Interconnection	OSI	kurz für: Open Systems Interconnection Reference Model. Offenes Schichtenmodell für die Kommunikation informationsverarbeitender *Systeme* bestehend aus 7 Ebenen.
Operation Level Agreement		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.
Operational Level Agreement	OLA	Nach innen gerichtete Vereinbarung über die Erbringung definierter Services. Ziel ist die Gewährleistung eines mit Kunden vereinbarten *SLA*. (ITIL-basierter Begriff)
Operationale Risiken	operational risks	Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und *Systemen* oder infolge externer Ereignisse eintreten.
OSI	Open Systems Interconnection	
OTC	Over the Counter	OTC steht für „over the counter“. Mit OTC-Präparaten/-Medikamenten werden i.A. nicht verschreibungspflichtige und somit frei verkäufliche Präparate/Medikamente (wie z.B. Aspirin) bezeichnet.

Begriff	Synonym	Definition/Erläuterung
P		
Packungsgröße		Menge und Einheit der Packung eines Arzneimittels, z.B. N2
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.
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
PassG	Passgesetz	
PassV	Passverordnung	
PassVwV	Passverwaltungsvorschrift zur Durchführung des Passgesetzes	
Patches		Kleinere Korrekturen an ausgelieferter Software
Patient	patient	Natürliche Person, die medizinische Leistungen beansprucht.
Patientenfach		Elektronischer Datencontainer in der *Telematikinfrastruktur* für die Ablage und Übermittlung von vom *Versicherten* selbst oder für diesen zur Verfügung gestellten Daten, die sich ausschließlich in der Datenhoheit des *Versicherten* befinden. Mehrere *Anwendungen* können hierzu definiert werden (§ 291a Abs. 3, Satz 1, Nr. 5 SGB V/GMG).
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*.

Begriff	Synonym	Definition/Erläuterung
Payload		Nutzlast an Daten, die durch ein Protokoll oder eine Nachricht transportiert wird.
PB	Projektbüro	
PC	Polycarbonat	Material für Karten. Auch genutzt für PC: Personal Computer
PC/SC	Interoperabiltity Specification for ICCs an Personal Computer Systems (References)	
PCS	Procedure Coding System	
PDD	Patientendatendienst	
Performance-Test		Test, bei dem die Leistungsfähigkeit des getesteten *Systems* im Vordergrund steht. Dies können beispielsweise Antwortzeiten bei einzelnen Zugriffen oder einer definierten Anzahl paralleler Zugriffe sein. Fachliche und funktionale Aspekte spielen eine untergeordnete Rolle. Ziel ist ein Nachweis, dass das *System Leistungsanforderungen* des Endbenutzers genügt (*Benutzerfreundlichkeit*) oder dass das *System* in einer bestimmten Zeit eine bestimmte Menge an Aufgaben bewältigen kann. Die Bedeutung von Performance-Tests steigt mit der Komplexität (also z.B. der Anzahl der vernetzten Komponenten) des *Systems*.
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.
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.
Personenbezogene Applikation		Die auf eine Person bezogene Ausprägung einer *Anwendung* nach §291a SGB V/GMG (z. B. die Arzneimittel-Dokumentation von Frau Klara Mustermann)

Begriff	Synonym	Definition/Erläuterung
PET	Polyethylenterephthalat	Material für Karten
PFD	Patientenfachdaten	Daten in der Datenhoheit des Versicherten
PFDD	Patientenfachdatendienst	Dienst zur Ablage und Bereitstellung der in der Datenhoheit des Versicherten liegenden Daten
PFDM	Patientenfachdatenmanagement	Managementsystem zur Verwaltung der Daten im Patientenfach
Pharmazentralnummer	PZN	Bundeseinheitlicher Identifikationsschlüssel zur Kodierung von Arzneimitteln und Apothekenprodukten, die eine *Identifizierung* nach Warenzeichen, Wirkstoffstärken, Darreichungsform, *Packungsgröße* und pharmazeutischem Hersteller ermöglicht.
PHB	Projekthandbuch	
Physikalisch Technische Bundesanstalt	PTB	Die PTB mit Sitz in Braunschweig hat per Deutschem Zeitgesetz von 1978 den Auftrag, die amtliche Deutsche Zeit zur Verfügung zu stellen. Zur Ermittlung der Zeit wird auf das physikalische Verhalten von Cäsium 133 zurückgegriffen, aus dem sich eine Sekunde herleiten lässt: "*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.
Physisches Kartenmanagement		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.
PI	Padding Indicator	
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	Personal Identification Number	Persönliche Identifikationsnummer
PIN Pad		Das PIN Pad ist eine Spezialtastatur zur Eingabe der persönlichen Geheimzahl (PIN) an Geldautomaten, POS-Terminals und Überweisungsterminals.
PIN.CH		PIN.Card Holder, technisches Synonym *für Praxis-PIN*
PIN.home		technisches Synonym *für Privat-PIN*
PIN.QES		technisches Synonym *für Signatur-PIN*
PIP	Post Issuance Processing	Nachladeprozess
PK	Public Key, *Öffentlicher Schlüssel*	

Begriff	Synonym	Definition/Erläuterung
PKCS	Public Key Cryptography Standards	
PKI	Public Key Infrastructure	
PKV	Private Krankenversicherung	
PL	Projektleiter / Projektleitung	
PL-API		Plattform-API (interne Schnittstelle zu den Infrastrukturdiensten)
PLZ		Postleitzahl
Point-to-point Protocol	(PPP)	Das Point-to-point Protocol erlaubt es, TCP/IP-Verbindungen via Telefonleitung und Modem/ISDN herzustellen.
PP	Protection Profile, Schutzprofil	
PPP	Point-to-Point Protocol	
PPS	Protocol Parameter Selection	Die Art eines ausgewählten Protokolls wird in einem Parameter, einem so genannten Protocol Parameter Selection codiert.
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.
Praxis-PIN	PIN.CH	Diese *PIN* wendet der Versicherte an, um bei Inanspruchnahme medizinischer Leistung über die *Telematik-infrastruktur* sich entweder explizit zu *authentisieren* oder jemand anderen für Zugriffe zu *autorisieren.* In technischen Dokumenten (eGK-Spezifikation) wird „PIN.CH“ verwendet.
Praxis-PUK		Eine zur *Praxis-PIN* gehörige *PUK* wird als Praxis-PUK bezeichnet.
Primäres Vertragsverhältnis		Das Vertragsverhältnis eines *Versicherten* mit demjenigen *Kostenträger*, welcher in erster Instanz die Behandlungskosten trägt.
Primärsystem	PS	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.

Begriff	Synonym	Definition/Erläuterung
Privater Schlüssel	Private Key, PrK	Der private Schlüssel ist der Teil eines kryptographischen Schlüsselpaares, auf den nur der Inhaber des Schlüsselpaares zugreifen kann. Er wird in einem Personal Security Environment aufbewahrt und verwendet, um *digitale Signaturen* zu erstellen oder Daten zu entschlüsseln
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		Eine zum *Privat-PIN* gehörige *PUK* wird als Privat-PUK bezeichnet.
PrK	Private Key, *Privater Schlüssel*	
PRND	Padding Random Number	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.
Problem		Zusammenfassende Beschreibung von *Incidents*, deren Ursache unbekannt ist. (*ITIL*-basierter Begriff)
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*.
Projektrisiken	project risk	Risiken die den vorgesehene Ablauf oder die Ziele eines Projektes gefährden.
Protection Profiles	*Schutzprofile*	
Protokollierung		In der *Telematikinfrastruktur* versteht man unter „Protokollierung“ sowohl das fachliche (*Audit*), als auch das technische Protokollieren (*Logging*) von Daten.
Provider		Provider stellen einen *Dienst* im Auftrag eines *Betreibers* bereit. Sie sind gegenüber den *Betreibern* verantwortlich für die Einhaltung der definierten Betriebs- und Servicelevel.
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.

Begriff	Synonym	Definition/Erläuterung
Prozess		Unter einem Prozess versteht man einen definierten Ablauf von Zuständen eines *Systems*. Der Begriff wird im Kontext der Telematik verwendet, um betriebliche Abläufe zu bezeichnen (Geschäftsprozess, Betriebsprozess) wie auch um technische Abläufe zu benennen (Ausführung von Programmen und Programmschritten).
PRU	Produktionsreferenz-umgebung	
PS	*Primärsystem*	
PSE	Personal Security Environment	
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)
PSO	Perform Security Operation	Berechnung der kryptographischen Prüfsumme bei zu verschlüsselnden Daten
pt	point	Maß für die Größe einer Schrift
PTA	Pharmazeutisch-Technischer Assistent	
PTB	Physikalisch Technische Bundesanstalt	
PTU	Produktionstestumgebung	
PU	Produktionsumgebung	
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 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.

Begriff	Synonym	Definition/Erläuterung
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-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.
Pufferüberlauf	Buffer-Overflow	Häufigste Sicherheitslücke in aktueller Software, die sich dazu eignet über Netzwerke 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.
PUK	Personal Unblocking Key	
PuK	Public Key, *Öffentlicher Schlüssel*	
PVC	Polyvinylchlorid als Kartenmaterial	
PVS	Praxisverwaltungssystem	*Primärsystem* des Arztes
PZN	Pharmazentralnummer	
Q		
QES	Qualified Electronic Signature	*qualifizierte elektronische Signatur*
QS	Quality Assurance	Qualitätssicherung
Qualifizierte elektronische Signatur	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	Definition/Erläuterung
Qualifizierter Zeitstempel	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“.
Qualifiziertes Zertifikat		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.
Quittung der Anforderungsmeldung	receipt	Schriftlich formalisierte Darstellung der Quittung des Eingangs einer Anforderungsmeldung. Sie gibt dem Anforderungssteller die Sicherheit, dass die Anforderungsmeldung in der gematik im Anforderungsmanagement eingegangen ist.
R		
RA	Registration Authority	
Rahmenarchitektur		Ergebnisdokument des Vorprojektes *biT4health*: Die Rahmenarchitektur von *bIT4health* gibt basierend auf den gesetzlichen Vorgaben die Leitlinien für die Implementierung der Funktionen der *eGK* und der unterstützenden technischen Infrastruktur vor.
Rahmenvertrag		Durch den Rahmenvertrag (RV) wird eine Vereinbarung zwischen der gematik und einer juristischen oder natürlichen Personen geschlossen, die einfach oder mehrfach eine Zusammenarbeit, ein Auftraggeber/Auftragnehmer Verhältnis, ein Verkäufer/Käufer-Verhältnis oder ein Dienstleistungsverhältnis betreffen. Der RV regelt grundsätzliche Aspekte der Zusammenarbeit. Zu dem RV werden konkrete Einzelaufgaben in separaten Leistungsscheinen (LS) mit den dazu gehörenden *Service Level Agreements (SLA)* definiert.
RAID	Redundant Array of Inexpensive Disks	
RC	Retry Counter	
RCA	Root CA	Wurzelinstanz
RD	Reference Data, Referenzdaten	
Realisierung		Der Begriff bezeichnet den Vorgang der Verwirklichung von Konzepten, also z.B. die Erstellung eines Programms oder Einrichtung einer Organisation.

Begriff	Synonym	Definition/Erläuterung
Realisierungs-konzept		Zusammenfassendes Konzept, das die Planung von Änderungen von der Initialisierung bis zum Übergang in den Betrieb umfasst. Teil des Realisierungskonzeptes ist u. A. der Projektplan.
Rechteprüfung	Examination of Rights	Prüfung der Zugriffsberechtigung eines Benutzers/Subjekts auf ein Objekt zum Zeitpunkt der Zugriffsanforderung, basierend auf der Identität des Benutzers/Subjekts bzw. Rollen- oder Gruppeneigenschaften und den beim Objekt hinterlegten Rechten oder Zugriffsregeln.
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.
Rechtssicher-heit		Rechtssicherheit wird erreicht, wenn der jederzeitige Nachweis der Einhaltung der relevanten Gesetze möglich ist.
Redundant Array of Inexpensive Disks	RAID	Ein Raid-System erlaubt die Abstraktion von physikalischen Festplatten zu logischen Laufwerken, um so wirtschaftlich eine erhöhte Ausfallsicherheit (durch Redundanz) oder höhere Geschwindigkeit oder beides zu erreichen.
Referenzumge-bung		Eine Referenzumgebung stellt ein Konfigurationsmuster dar, das als Vorlage für die Implementation weiterer Installationen für die Anwendung der *Gesundheitskarte* dient. Die Referenzumgebung enthält je eine der benötigten Komponenten in einer als Standard für die jeweilige Ausbaustufe gültigen Verbindung.
Regelbetrieb		Der Regelbetrieb ist die Phase, in welcher der Einführungsprozess für den definierten Produkt- und Prozessumfang abgeschlossen ist.
Registrierungs-instanz	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.
Registrierungs-stelle	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	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.
RegTP		ehemalige Regulierungsbehörde für Telekommunikation und Post; Nachfolger ist die *Bundesnetzagentur* (*BNetzA*)
Release		Zusammenfassung von Versionen oder Varianten aller für eine Einsatzumgebung benötigten Ergebnistypen zu einem Terminstand.
Release Management	RM	*ITIL*-basierter Prozess, der für die operative Ausführung von *Changes*, die durch das *Change Management* beauftragt wurden, verantwortlich ist. Das Release Management hat eine ganzheitliche Sicht auf die Veränderungen an einem IT-Service.
Release-definition	release definition	Beschreibung des geplanten Inhaltes mit Motivation durch *Auftragsanforderungen* jedoch ohne konzeptionelle Lösungsansätze, der zu einem *Release* führen soll.
Resolver		Programmsoftware, die – getrieben von Client Anfragen – Informationen aus dem Datenbestand von Name Servern extrahiert und an das anfragende Clientsystem zurückgibt.
Restrisiko	residual risk	Nach der Festlegung von Maßnahmen zur Senkung von *Risiken* und/oder der bewussten Entscheidung für die Akzeptanz von *Risiken* verbleibendes *Risiko*.
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.
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.

Begriff	Synonym	Definition/Erläuterung
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.
RF	Radio Frequency	
RFC	Request for Comment	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
RfC	Request for Change	*ITIL*-basierter Begriff zur formalisierten vollständigen Beschreibung eines Änderungsbedarfs. Wird im *Change Management* aus einem *NfC* generiert. In der *Telematikinfrastruktur* wird der Begriff *CR* (*Change Request*) verwendet.
RID	Registered Application Provider Identifier	Die RID ist der registrierte Bestandteil eines Application Identifiers (AID) zur Gewährleistung einer weltweit eindeutigen Namensvergabe für Chipkarten-Anwendungen
Risiko	risk	Ein Risiko ist die Kombination der Wahrscheinlichkeit, dass ein Schadensfall eintritt, und die hieraus resultierende Schadenshöhe
RM	Risikomanagement	
RND	Random Number	Zufallszahl
Rolle	role	Eine Rolle beschreibt die Verhaltensweise eines *Akteurs* in einer definierten Aufgabenstellung.
Rollenbasierte Zugriffskontrolle	role based access control	Die *Zugriffskontrolle* eines IT-Systems ist nicht unmittelbar auf ein Objekt (Person, Anwendung) bezogen, sondern wird je *Rolle* festgelegt.
Rollout		Markteinführung. Als Rollout wird der Vorgang bezeichnet, über den neue Produkte und Verfahren in die Fläche gebracht werden, hier also insbesondere der Vorgang der Auslieferung, Verteilung und Installation von Software und Hardware.
Root		Wurzel: Oberste *CA* in einer Hierarchie einer *PKI*
Root-CA		Wurzel-Zertifizierungsinstanz.
Router		Aktive Netzwerkkomponente, die zwischen zwei Netzen gleichen Typs mit unterschiedlichen Adressräumen vermittelt.

Begriff	Synonym	Definition/Erläuterung
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		
SAGA		Standards und Architekturen für eGovernment-Anwendungen des Bundesministerium des Inneren
SAK		Signaturanwendungskomponente
SAVeD		Sicherer Anbindungs- und Vermittlungsdienst
SC	1. Security Condition 2. Smart Card	1. Sicherheitsbedingung 2. anderer Begriff für Prozessorkarte
Schalenmodell		Das Schalenmodell ist ein so genanntes Gültigkeitsmodell für *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-Ableitung	Derive-Key	Dienst des Schlüsselmanagements (siehe [ISO 11770]): Der Dienst Schlüssel-Ableitung 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.
Schlüssel-Archivierung	Archive-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Schlüssel-Archivierung ist der Prozess, Schlüssel nach Ablauf der Nutzung sicher und langfristig zu speichern. Für diesen Dienst ist die Anwendung des Dienstes “Schlüssel-Speicherung” denkbar, es bestehen aber verschiedene Anforderungen, so dass auch verschiedene Implementierungen denkbar sind. So könnte z. B. die Schlüssel-Archivierung offline realisiert werden. Archivierte Schlüssel können noch lange nach dem normalen Gebrauch der Schlüssel benötigt werden, um bestimmte Ansprüche abzuklären

Begriff	Synonym	Definition/Erläuterung
Schlüssel-Deregistrierung	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.
Schlüssel-Erzeugung	Generate-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Schlüssel-Erzeugung 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.
Schlüssel-Installation	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.
Schlüssel-management	Key Management, KM	Verwaltung von Schlüsseln. Bezüglich des *Kartensystems* ist hier das Schlüsselmanagement für die *eGK* gemeint.
Schlüssel-management-system	Key Management System, KMS	System (bzw. eine Komponente im gesamten Kartensystem) für das *Schlüsselmanagement*.
Schlüssel-Registrierung	Register-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Der Dienst Schlüssel-Registrierung 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. Schlüssel-Registrierung 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.

Begriff	Synonym	Definition/Erläuterung
Schlüssel-Speicherung	Store-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Der Dienst Schlüssel-Speicherung bietet sichere Speicherung für Schlüssel im laufenden oder kurz bevorstehenden Gebrauch oder auch für Backup-Schlüssel. Es ist üblicherweise von Vorteil, physikalisch getrennte Schlüssel-Speicher vorzusehen. Zum Beispiel sichert ein Schlüssel-Speicher die Vertraulichkeit und Integrität von Schlüsselmaterial oder die Integrität von öffentlichen Schlüsseln. Speicherung kann in allen Schlüsselzuständen im Lebenszyklus eines Schlüssels vorkommen.
Schlüssel-Suspendierung	Revoke-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Wenn die Kompromittierung eines Schlüssels bekannt ist oder vermutet wird, stellt der Dienst Schlüssel-Suspendierung die sichere Deaktivierung des Schlüssels sicher. Der Dienst ist auch für Schlüssel, deren Gültigkeit abgelaufen ist, notwendig. Schlüssel-Suspendierung 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 Schlüssel-Suspendierung wird kaum bei zertifikatbasierten Schemata angewandt, wo der Lebenszyklus der Schlüssel durch die Gültigkeit der Zertifikate geregelt wird.
Schlüssel-Verteilung	Distribute-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Die Schlüssel-Verteilung ist eine Menge von Prozessen, um Schlüssel-Management-Information-Objekte (in der Regel Schlüssel) sicher zu autorisierten Entitäten zu verteilen.
Schlüssel-Zerstörung	Destroy-Key	Dienst des Schlüsselmanagements (siehe [ISO11770]): Der Dienst Schlüssel-Zerstörung 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*.

Begriff	Synonym	Definition/Erläuterung
Schutzprofile	protection profile	Schutzprofile ermöglichen es, eine Sicherheitslage anhand von Gefährdungen, Annahmen über die Betriebsumgebung der IT, Sicherheitszielen usw. zu beschreiben. Schutzprofile bilden somit die Grundlage für die Standardisierung der Sicherheitsanforderungen an bestimmte Produkte und deren Prüfung.
Schwachstellenanalyse	vulnerability assessment	Gezielte Untersuchung (Auditierung) von Prozessen und Verfahrensabläufen zur Ermittlung von Prozess- und / oder Verfahrensfehlern (Inplausibilitäten, Nonkonformitäten) mit dem Ziel, Prozess- und Verfahrenssicherheit herzustellen.
SE	Security Environment	Sicherheitsumgebung
Secure Hash Algorithm	SHA-1	Der Secure Hash Algorithm (SHA-1) [FIPS180-2] ist ein von der US-amerikanischen Sicherheitsbehörde NSA entwickelter *Hash-Algorithmus*, der 160 Bit *Hash-Werte* produziert.
Secure Signature creation Device	SSCD	Ein Secure Signature Creation Device ist ein Hardware-Module 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 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 Konnektor	SM-K	Pphysikalischer 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.

Begriff	Synonym	Definition/Erläuterung
Serveranwendung		Die Serveranwendung ist eine spezielle Form einer *Anwendung*.
Service Consumer Layer		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 Directory Service	SDS	Der Service DirectoryService (SDS) registriert alle Dienste und Dienstinstanzen der Telematik- und der Serviceproder-Schicht und ordnet den Instanzen Adressen (URLs) zu, unter denen die Dienste angesprochen werden können. Technische Grundlage für die Implementierung des SDS ist UDDI v3 [UDDI]: der SDS wird als private UDDI Registry mit einem Knoten (Node) implementiert
Service Katalog		Im Service Katalog werden die verfügbaren IT-Services inklusive der möglichen *Service Level* beschrieben, aus denen ein Nutzer wählen kann.
Service Level Agreement	SLA	Vereinbarung über die Qualität von IT-Dienstleistungen, siehe auch *SLR*
Service Level Management		*ITIL*-basierter Prozess, der die Qualität der IT-Services fokussiert. Aufgabe ist die Vereinbarung von *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 *SL*A erstellt. (ITIL-basierter Begriff)
Service Provider Layer		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		Ein ServiceTicket bezeichnet Berechtigungsinformationen zu einem Service. In einem ServiceTicket sind sowohl die Informationen über die Zugriffsrechte einer Identität auf einen Service als auch mögliche *Hybridschlüssel* für eine zugelassene Identität enthalten.

Begriff	Synonym	Definition/Erläuterung
Service-vereinbarung		Eine Servicevereinbarung (SVB) ist eine Vereinbarung mit einem internen Kunden und enthält Absprachen über die Erbringung von definierten Services. Da es eine firmen- bzw. konzerninterne Vereinbarung ist, entspricht ein SVB in der Regel keinem Vertrag im juristischen Sinne, sondern Dienstleistungsvereinbarungen. Dienstleistungen werden in den *Leistungsscheinen* definiert und die dazu gehörenden *SLAs* spezifizieren die Leistungsparameter.
Servicevertrag		Ein Servicevertrag (SVT) ist eine Vereinbarung mit einem externen Kunden und enthält Absprachen über die Erbringung von definierten Services. Da er eine externe Vereinbarung ist, entspricht ein Servicevertrag einem Vertrag im juristischen Sinne sowie Dienstleistungsvereinbarung. Die juristischen Regelungen sind im Rahmenvertrag enthalten. Dienstleistungen werden in den zum Rahmenvertrag gehörenden *Leistungsscheinen* definiert und die dazu gehörenden *SLAs* spezifizieren die Leistungsparameter.
SFID	Short EF Identifier	
SGB		Sozialgesetzbuch
SGB V		Sozialgesetzbuch Fünftes Buch
SHA-1	Secure Hash Algorithm	
SICCT	Secure Interoperable ChipCard Terminal	
Sichere Signaturerstellungseinheit	SSEE	Eine sichere *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.
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.

Begriff	Synonym	Definition/Erläuterung
Sicherheitsanalyse		Analyse der IT-Sicherheit durch festgeschriebene Methoden
Sicherheitsanforderung	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 Si-cherheitsaspekte erfüllen. Sie klassifizieren sich in Sicherheitsanforderungen mit und ohne Geheimhaltung.
Sicherheitsaudit	security audit	Befragung der Mitarbeiter eines Unternehmens bzgl. Der IT-Sicherheit
Sicherheitsdienst	*Sicherheits-(grund)funktion*	
Sicherheitskomponente	Security Component	Eine Sicherheitskomponente dient unmittelbar zur Abdeckung einer oder mehrerer *Sicherheits(grund)-funktionen*. Sie spezifiziert die bereitgestellte Dienstleistung, ohne aber zu beschreiben, wie die Dienstleistung realisiert ist. Die Komponenten werden durch Sicherheitsmechanismen und Sicherheitsobjekte aufgebaut und durch Produkte realisiert.
Sicherheitskonzept		Konzept, das die Sicherheit der Systemkomponenten sowie deren sicheren Betrieb festlegt
Sicherheitsmodell	security modell	Formulierung bestimmter Regeln für die *Zugriffskontrolle* oder allgemein einer umfassenden *Sicherheitspolitik*.
Sicherheitspolitik		Grundlegende Aussagen bzgl. Der Sicherheit für ein Unternehmen/*System*
sicherheitsrelevant		(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 Nicht-Abstreitbarkeit geschützt werden muss, um die Sicherheit (des Systems) zu gewährleisten.
Sicherheitstechnische Eignung		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.

Begriff	Synonym	Definition/Erläuterung
Sicherheitstest		Nachweis der sicherheitstechnischen Eigenschaften der Komponenten und des Gesamtsystems
SIG	Signature, Signatur	
SigG	Signaturgesetz	
Signatur-algorithmus		Ein Signaturalgorithmus ist ein asymmetrischer Krypto-algorithmus, der zur Erzeugung *digitaler Signaturen* verwendet wird. Zu den populärsten Signaturalgorith-men zählen *RSA*, *DSA* und *ECDSA*.
Signaturan-wendungs-komponente	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* zuzufüh-ren oder *qualifizierte elektronische Signaturen* zu *prüfen* oder *qualifizierte Zertifikate* nachzuprüfen und die Er-gebnisse anzuzeigen.
Signatur-erstellungs-einheit		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 wer-den 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 *qualifi-zierten elektronischen Signaturen* sind *sichere* Signa-turerstellungseinheiten nötig.
Signatur-PIN	PIN.QES	Diese *PIN* wenden *Akteure* im Rahmen der *Telematik-infrastruktur* 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.
SigV	*Signaturverordnung*	Die Signaturverordnung ergänzt das Signaturgesetz um Einzelregelungen zu den Anforderungen an die Zertifi-zierungsdiensteanbieter sowie an die bei der Zertifikats- und Signaturerstellung einzusetzenden Produkte und Verfahren. Sie konkretisiert darüber hinaus die Kosten-regelung in § 22 SigG. In der Anlage 1 macht sie zudem detaillierte Vorgaben für die Prüfung von Produkten für qualifizierte elektronische Signaturen.
Simple Mail Transfer Proto-col	SMTP	Übertragungsprotokoll für E-Mails
Simple Network Management Protocol	SNMP	Leichtgewichtiges Protokoll für die Steuerung und Sta-tus-Abfrage von Netzwerkkomponenten und Servern
Single Point Of Failure (SPOF)		Nicht redundant ausgelegte technische Komponente bei deren Ausfall ein Dienst nicht mehr verfügbar ist.

Begriff	Synonym	Definition/Erläuterung
SK	Secret Key, *geheimer Schlüssel*	
SL	Stationäre Leistungen	
SLA	Service Level Agreement	
SM	Secure Messaging	Secure Messaging bezeichnet ein serverbasiertes sicheres E-Mail-System.
SM-AK	Security Module Anwendungskonnektor	
SMC	Security Module Card, Sicherheitsmodulkarte	
SMC-B	Security Module Card Typ B, Institutionenkarte	Die SMC-B ist kennzeichnend für eine Einheit oder Organisation des Gesundheitswesens (z.B. Praxis, Apotheke).
SMK	SM key, SM-Schlüssel	
SM-K	Security Module Konnektor	
SM-KT	Security Module Kartenterminal	
SM-NK	Security Module Netzkonnektor	
Smoketest	smoke testing	In der Programmierung bezeichnet smoke testing den ersten grundlegenden Probelauf einer Software, der simple Probleme offen legen soll, die ernst genug sind, um das Programm nochmals zu überarbeiten und ein mögliches *Release* zu vereiteln
SN	Serial Number, Serien-Nummer	
SNMP	Simple Network Management Protocol	
SNMP-Traps		Dezentral initiierte Statusmeldungen, Teil des SNMP
SOAP		Standard für die Kommunikation innerhalb der WEB-Services
SP	Service Provider	
Spec.	Specification	*Spezifikation*
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.

Begriff	Synonym	Definition/Erläuterung
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.
SPOF	Single Point Of Failure	
Spoofing		Vortäuschen falscher Identitäten
SRQ	Specification related question	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.
SSC	Send Sequence Counter	Ein Mechanismus der zum sicheren Versenden von Nachrichten benutzt wird, wo es keinen eigenen Sicherheitsmechanismus gibt.
SSCD	Secure Signature Creation Device	
SSEE	Sichere Signaturerstellungseinheit	
SSL	Secure Socket Layer	
Stammdaten	master data	Daten einer Person oder eines Gegenstandes, welche über längere Zeit unverändert bleiben. Bezogen z.B. auf die *Versicherten* handelt es sich um die Personenstammdaten wie Name, Geburtsdatum und Wohnort. Die Stammdaten sind Teil der *Vertragsdaten (VSD)* nach §291 a.
Stammzertifikat	Root-Certificate	Das selbstsignierte *Zertifikat*, welches in einer *PKI*-Hierarchie an höchster Stelle steht und den Vertrauensanker (Wurzel) bildet.

Begriff	Synonym	Definition/Erläuterung
Status im Anforderungsmanagement		Ein Prozessschritt im Anforderungsmanagement erhält einen Ergebnistypen in definiertem Status und gibt ihn in einem anderen definierten Status wieder aus. Die Ergebnistypen *Anforderung* und Anforderung-Dokument-Beziehung werden durch den Prozess anhand der Statusvergabe geführt. Die *Anforderung* unterliegt den Status „quittiert“, „ZurVorentscheidungVorgelegt“, „offen“, „redundant“, „ZurBewertungAbgegeben“, „Zur EntscheidungVorgelegt“, „akzeptiert/Umsetzung offen“, „komplett umgesetzt“, „abgelehnt“, „zurückgestellt“ und „storniert“. An der Beziehung zwischen *Anforderung* und Dokument sind folgende Status möglich: „zugeordnet“, „umzusetzen“ und „umgesetzt“. Zwischen den Status der Anforderung und der Anforderung-Dokument-Beziehung bestehen Regelwerke, die die Abhängigkeiten festlegen.
Strategische Risiken	strategic risk	Strategische Risiken sind Gefährdungen der Zielerreichung, die aus den Veränderungen des Umfeldes eines *Systems* resultieren.
Stratum		Die Nähe einer Server-Zeit zu einer geeichten Normal-Zeit (z.B. Atomuhr o.ä.) wird durch das sog. Stratum ausgedrückt. Der Wert des Stratums ist Null für einen *NTP-Server*, der seine Zeit direkt mit einer geeichten Quelle synchronisiert. Server, die ihre Zeitinformation direkt von einer Cäsium Atomuhr beziehen, können selbst als Stratum-0-Server fungieren. Der hierarchisch eine Stufe tiefer angeordnete Server, der seine Zeitinformationen vom Stratum 0 Server bezieht bzw. etwa per DCF-77 Funksignal erhält, bezeichnet sich als Stratum 1 Server.
Subscriptio		Herstellungsanweisung für Rezepturen, Beispiel: Salbebeschreibung, die sich aus mehreren Bestandteilen zusammensetzt.
SVA	Sozialversicherungsabkommen (der EU)	
SVR	Server	
SW	1. Software 2. Status Word	
Switch		Verbindet mehrere Geräte in einem LAN
Symmetrischer Schlüssel		Zeichen- oder bit-Folge, die zum Entschlüsseln und Verschlüsseln von Daten verwendet wird. Bei einem symmetrischen (No Suggestions) Schlüssel dient der gleiche Schlüssel sowohl zum Ver- als auch zum Entschlüsseln
System		Die Gesamtheit miteinander verknüpfter und sich gegenseitig beeinflussender Elemente, die entsprechend einem bestimmten Zweck organisiert ist. Das *System* hat eine gänzlich andere Qualität als die Summe seiner Elemente.

Begriff	Synonym	Definition/Erläuterung
System Management		Zusammenfassung aller Aufgaben, die den operativen Betrieb der IT-Infrastruktur technisch und organisatorisch unterstützen.
System-Funktionstest		Ziel des Tests ist es, nachzuweisen, dass der Aufbau / die Konfiguration der Komponente in der Wirkumgebung keine Auswirkungen auf funktionale Eigenschaften hat, die bereits in den *Komponenten- bzw. Schnittstellentests* überprüft wurden. In diesem Sinne ein Regressionstest, es sei denn die Funktion wird erstmalig bereitgestellt
System-Interoperabilitätstest		Im Rahmen des *Interoperabilitätstests* werden für ausgewählte Kombinationen der in der Wirkumgebung aufgebauten Komponenten die Fähigkeit zum verlässlichen Datenaustausch und die Zusammenarbeit der aufgebauten Teilsysteme gegen die Prüfanforderungen der entsprechenden *Prüfvorschriften* überprüft.
System-Leistungstest		Die Leistungstests gliedern sich in die Überprüfung nicht-funktionaler Qualitätsmerkmale wie Lastverhalten (Lasttest), Antwortzeit- und Durchsatzverhalten (Performanztest), Verhalten in Abhängigkeit von Datenmengen (Massentest) sowie Verhalten bei Überlast (Stresstest).
System-Sicherheitstest		Im Rahmen der Sicherheitstests erfolgt eine Überprüfung der geforderten Sicherheitsmaßnahmen in der Wirkumgebung. Dies umfasst den Test des Systemverhaltens bei gezielten Systemabbrüchen und provozierten Ausfällen von Netzknoten. Darüber hinaus wird die Abwehr unerlaubter Eingriffe ins Netz getestet
T		
Target of Evaluation	(TOE)	*Evaluationsgegenstand* (EVG)
TBD	To be determined	
TC	1. Trusted Channel 2. Trust Center	1. sicherer Kanal 2. Trust Center
TCL	Trusted Component List	
TCP/IP	Transmission Control Protocol/Internet Protocol	herstellerunabhängiges Protokoll zur Übertragung von Daten im Internet oder Intranet.
TCS	Test Case Specification	
TDS	Time Distribution System	

Begriff	Synonym	Definition/Erläuterung
Technology View		Der Technology View nach RMODP (Reference Model for Open Distriubuted 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 könnten, also nur Teile eingelöst werden, so spricht man von einer Teileinlösung.
Telematik		Telematik ist zusammengesetzt aus den Begriffen Telekommunikation und Informatik. Er beschreibt die Zusammenführung, Verarbeitung und Weitergabe verteilter, u.U. heterogener Datenbestände.
Telematik Layer		Der Telematik Layer verbindet den *Service Comsumer Layer* mit dem *Service Provider Layer*. Er stellt dazu vermittelnde Netzwerk- und Transportdienste sowie *Sicherheitsdienste* bereit und steuert die *Fachdienste* an.
Telematikinfrastruktur	(TI)	Gesamtmenge der technischen Komponenten, die zur Realisierung einer integrierten Versorgung der Gesellschaft mit medizinischen Dienstleistungen benötigt werden.
Telematik-zulassungs-infrastruktur	TZI	dient der Zuteilung von Zertifikaten für von der gematik freigegebene Komponenten
Terminal API		Schnittstelle für *Primärsysteme* zum *Kartenterminal*
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 Vorstufe im Lebenszyklus von Diensten und Services der Gesundheitstelematik vor dem Wirkbetrieb und dient der Erprobung der Implementation. Ein Testbetrieb kann Testdaten oder Echtdaten verarbeiten
Testdesign		Aktivität im Testprozess zur Erstellung von *Testfällen*, *Testspezifikationen* und –szenarien
Test-durchführung		Aktivität im Testprozess, die die Tätigkeiten zum manuellen bzw. automatisierten Ausführen der freigegebenen Testfälle bzw. Testsuiten umfasst.

Begriff	Synonym	Definition/Erläuterung
Testentwurf		Der Testentwurf (oder auch Testdetailkonzept genannt) wird aus den Anforderungen von *Fachkonzept* (FK), *Facharchitektur* (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.
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.
Test-implementierung		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).
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.
Testphase		In der *gematik* wird der Test in die folgenden Testphasen (in der Literatur oft auch *Teststufen* genannt) unterteilt: • *Komponententest* • *Komponentenleistungstest* • *Schnittstellentest* • *System-Funktionstest* • *System-Interoperabilitätstest* • *System-Leistungstest* • *System-Sicherheitstest* • *Gesamtsystemtest*

Begriff	Synonym	Definition/Erläuterung
Testplan		Der Testplan (oft auch Testkonzept genannt) beschreibt, welche Testobjekte aufgrund welcher Grundlage und mit welchen Verfahren getestet werden. Der Testplan definiert darüber hinaus den Testumfang, die Vorgehensweise, die Anforderungen an die Prüfumgebung, die Ressourcen und die Zeitplanung der intendierten Tests.
Testplanung		Aktivität im Testprozess zur Erstellung und Fortschreibung des *Testplans*, 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.
Testspezifikation		Die Testspezifikation umfasst die Auflistung der *Testfälle* für eine logische Gruppierung (z. B. zu testende Komponenten oder Problem).

Begriff	Synonym	Definition/Erläuterung
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)
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.
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*).
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 o *Testplan* o Testentwurf o *Prüfvorschrift* • Testdesign

Begriff	Synonym	Definition/Erläuterung
		○ *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 Test-Bereich produzieren diese: Testkonzepte, *Testfälle*, Test-Berichte, Fehlermeldungen, Eingabe-Dateien/Skripte für Testwerkzeuge,… Diese sollten alle wieder benutzbar sein und deshalb auch per Konfigurationsmanagement verwaltet werden.
TI	*Telematikinfrastruktur*	
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*
Tiefen-verteidigung	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.
TLS	Transport Layer Security	Nachfolger von *SSL*
TLV	Tag Length Value	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.
TMS	Token Management Service	Dient zur Steuerung der Authentifizierungsvorgängen
To be determined	TBD	Noch zu entscheiden
TOE	Target of Evaluation	

Begriff	Synonym	Definition/Erläuterung
TOP	Testorganisations-Plattform	
TPM	Trusted Platform Module	
Transmission Control Protocol	TCP	Das in RFC793 spezifizierte TCP ist ein zuverlässiges, verbindungsorientiertes Transportprotokoll in Rechnernetzen, das auch im Internet zum Einsatz kommt.
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.
Trojaner, Trojanisches Pferd		Scheinbar nützliche Software, die durch Anwender installiert wird, aber geheimen Schadcode enthält
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		Siehe *virtueller Kanal*
Trusted Platform Module	TPM	Ein Trusted Platform Module ist ein Chip zur Ausführung von kryptographischen Funktionen sowie zur Speicherung von Schlüsseln. Ein TPM kann mit einer fest eingebauten Smartcard verglichen werden, wobei ein TPM im Gegensatz zur Smartcard fest an ein Gerät gebunden ist.
Trusted Service	TS	Service der *Telematikinfrastruktur*, der für die Umsetzung eines Teils der Sicherheitspolicy zuständig ist
Trusted Viewer		Vertrauenswürdige Anzeige dessen, was signiert werden soll

Begriff	Synonym	Definition/Erläuterung
Trust-service Status List	TSL	Eine Trust-service Status List bietet alle relevanten Informationen zur vertrauenswürdigen Verteilung und Prüfung der Wurzelzertifikate verschiedener „Certification Authorities“ in Form einer signierten *XML*-Datei (ETSI-Standard). Hierdurch können auch bereits existierende heterogene *PKI*´s nach einem einheitlichen Schema eingebunden werden.
TS	TrustedService	
TSL	Trust-service Status List	
TSP	Trust Service Provider	
TVS	Ticket Validation Service	Wird für die Überprüfung von Tickets genutzt.
TZI	*Telematikzulassungsinfrastruktur*	
TZP	Telematik-Zugangsprovider	
U		
Übergabedokument		Dokumente, die von einem *Leistungserbringer* zwecks Fortführung der Behandlung einem anderen *Leistungserbringer* übergeben werden.
UC	Use Case, *Anwendungsfall*	
UDDI	Universal Description, Discovery and Integration	
UDDI Registry		Implementierung des UDDI Standards, siehe auch (*UDDI, Universal Description, Discovery and Integration*)
UDP	User Datagram Protocol	
UML	Unified Modelling Language	
Umsetzungsanforderung	implementation requirement	Klassifizierung von *Anforderung* *Anforderungen* aus dem Umsetzungsprozess in der gematik (nicht entscheidungsrelevant).
Underpinning Contract	UC	Ein Underpinning Contract (UC) ist eine Vereinbarung mit einem externen 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.

Begriff	Synonym	Definition/Erläuterung
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 Ressource Identifier	URI	Zeichenfolge, die zur Identifizierung einer abstrakten oder physikalischen Ressource dient. Die Struktur der URI ist hierbei im Standard festgelegt
Unit-of-Work		Arbeitseinheit bzw. geschlossenes Arbeitspaket, welches stets vollständig ausgeführt werden muss.
Universal Description, Discovery and Integration	UDDI	Standard für einen Verzeichnisdienst, der basierend auf dem *SOAP*-Protokoll die dynamische Verwaltung von Webservices ermöglicht.
Update		Umfassendere Aktualisierung von Software
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.
UQ	Usage Qualifier	Karteninhaber-Authentifikation
URI	Uniform Ressource Identifier	
URL	Uniform Ressource Locator	
Usability		Die Usability eines Produktes ist das Ausmaß, in dem es von einem bestimmten Benutzer verwendet werden kann, um bestimmte Ziele in einem bestimmten Kontext effektiv, effizient und zufrieden stellend zu erreichen (ISO-Norm 9241). Ins Deutsche ließe sich das Ganze am ehesten mit „Benutzbarkeit“, „Bedienungsfreundlichkeit“ oder „Ergonomie“ übersetzen.
USB	Universal Serial Bus	Standardschnittstellenformat am PC
Use Case		*Anwendungsfall*
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 als zentrale Kontaktstelle bereitstellt.
UTC	Coordinated Universal Time	Koordinierte Weltzeit

Begriff	Synonym	Definition/Erläuterung
UTF8	8-bit Unicode Transformation Format	Unicode Transfomation Format ist eine Methode, Unicode-Zeichen auf Folgen von Bytes abzubilden (Zeichencodierung).
UUID	Universal Unique ID	
V		
VdAK/AEV	Verband der Angestellten-Krankenkassen e.V./Arbeiter-Ersatzkassen-Verband e.V.	
VDAP	Verband deutscher Arztpraxis-Softwarehersteller eV	
VDDS	Verband Deutscher Dental-Software Unternehmen	
Verbindlichkeit	Liability	Verbindlichkeit bezeichnet den Zustand, in dem die Eigenschaften der *Integrität, Authentizität, Nichtabstreitbarkeit (Non-Repudiation)* und *Zurechenbarkeit* gemeinsam erfüllt sind.
Verfügbarkeit	Availability	Verfügbarkeit ist die Fähigkeit, bestimmte Informationen/Dienste in zugesicherter Form und Qualität innerhalb eines definierten Zeitraums am benötigten Ort zu liefern.
Verordner ~~**Verordnungsgeber**~~		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.*
Verordnungsdaten		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.
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.

Begriff	Synonym	Definition/Erläuterung
Versicherten-ID		Unveränderbarer und eindeutiger Teil der *Krankenversichertennummer* zur *Identifikation* des *Versicherten*.
Versicherten-stammdaten (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 *Kostenträger*s. Dieser ist verantwortlich für die Bereitstellung, kontinuierliche Pflege, bedarfsgerechte Aktualisierung und schließlich Löschung der Daten.
Versicherter		Person, die in einer Vertragsbeziehung zum Krankenversicherer steht. Im Fall einer nicht geschäftsfähigen Person bzw. bei Verhinderung können die Rechte des Versicherten durch einen *Bevollmächtigten* wahrgenommen werden. Der Begriff wird im Rahmen des Projekts *eGK* als *Akteur* verwendet.
Vertragsarzt-nummer		Eindeutige alphanummerische Nummer für einen *Arzt*, der an der *GKV*-Versorgung teilnimmt. Die Nummer wird auf Antrag durch den Zulassungsausschuß der Kassenärztlichen Vereinigung zugeteilt.
Vertragsdaten		Die Daten, die in § 291 SGB V aufgeführt sind. Sie setzen sich zusammen aus Stammdaten und Daten bezogen auf den Krankenversicherer.
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*.
Vertrauens-würdig	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.

Begriff	Synonym	Definition/Erläuterung
Verzeichnis-dienst	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.
VhitG	Verband der Hersteller von IT-Lösungen für das Gesundheitswesen	
VHK	Verein patientenorientierter Informations- und Kommunikationssysteme	
Virtuelles Privates Netz	VPN	Bei einem VPN wird unter Verwendung kryptographischer Mechanismen und öffentlicher Transportnetze (z.B. Internet) ein virtuelles privates Netz geschaffen, in dem die Teilnehmer so sicher wie in einem lokalen Netz kommunizieren können.
Virus		Virus eine sich selbst verteilende Software mit meist schädlichen Eigenschaften
VOD	*Verordnungsdaten*	
VODD	Verordnungsdatendienst	
VODM	Verordnungsdatenmanagement	
VPN	Virtual Private Network	Virtuelles Privates Netz
VPN-Gateway	*VPN Konzentrator*	
VPN-K	VPN-Konzentrator	
VPN-Konzentrator	VPN	Sammelpunkt für mehrere VPN-Verbindungen.
VSD	Versichertenstammdaten	
VSDD	Versichertenstammdatendienst	
VSDM	Versichertenstammdatenmanagement	
W		
WAN	Wide Area Network	

Begriff	Synonym	Definition/Erläuterung
Wert	asset	Allgemein eine Sache mit einem wirtschaftlichen Wert welche von einer Privatperson oder Organisation im Besitz in Cash umgetauscht werden kann. Im Rahmen der IT-Sicherheit sind auch nicht in Geld wandelbare Werte (z.B. Reputation, Persönlichkeitsrechte) davon umfasst.
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		Wirkbetrieb beschreibt den Betriebszustand von Diensten und Services der Gesundheitstelematik, der Echtdaten von Versicherten und Leistungserbringern verarbeitet.
Wohnortprinzip	WOP	Das in 2002 eingeführte Wohnortprinzip sieht vor, dass Vertrags- und Abrechnungsbeziehungen unmittelbar zwischen einer Krankenkasse und allen Kven bestehen, in deren Bezirk Mitglieder der Krankenkasse wohnen.
WOP	*Wohnortprinzip*	
Workaround		Übergangslösung eines *Known Error* mit dem Ziel der schnellen Wiederherstellung eines Services. (*ITL* basierter Begriff)
Wurm		siehe Computerwurm
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

Begriff	Synonym	Definition/Erläuterung
X.509		Rahmenwerk der ITU-T für standardisierte Zertifikatsformate und die Zertifikatsprüfung in Authentisierungsdiensten
X.509 Directory Service		Ein X.509 Directory Service (Verzeichnisdienst) ist Bestandteil der X.509-PKI und wird zur Veröffentlichung der Zertifikate und Zertifikatsinformationen der X.509-Zertifikate (x.509-ENC und X.509-AUT) verwendet, welche auf der *eGK* abgelegt sind.
XML	Extensible Markup Language	universelle Datenbeschreibungssprache
XML Digital Signature	XML-Dsig	Für die *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
XML-Appliance		Hardware-Modul für die performante Verarbeitung von *XML*-Daten.
XSD	Extensible Schema Definition	
Z		
Zahlungsbeteiligung		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.
ZDA		*Zertifizierungsdiensteanbieter*
Zeitdienst		Er beschreibt ein Verfahren, das basierend auf existenten und weltweit jahrelang erprobten Technologien *(NTP)* für alle zentralen und dezentralen Komponenten und Systeme der *Telematikinfrastruktur* im Deutschen Gesundheitswesen, bis hinunter zu den *Primärsystemen* der *Leistungserbringer* eine bundesweit einheitliche Systemzeit gewährleistet.
Zeitstempel	time stamp	Digitale Daten, mit denen die Existenz bestimmter Daten vor einem bestimmten Zeitpunkt bewiesen werden kann. Häufig, wie z.B. beim Time Stamp Protocol, werden Zeitstempel unter Einsatz *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.
Zeitstempeldienst		Ein Zeitstempeldienst stellt *Zeitstempel* aus. Oft wird hierbei das in der *IETF* spezifizierte *Time Stamp Protocol* verwendet.

Begriff	Synonym	Definition/Erläuterung
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*.
Zertifikats-Erzeugung	Create-Key-Certificate	Dienst des Schlüsselmanagements (siehe [ISO11770]): Erzeugung eines Schlüssel-Zertifikats: Der Dienst zur Registrierung der Erzeugung eines Schlüssel-Zertifikats verbindet einen öffentlichen Schlüssel mit einer Entität und wird von einer Zertifizierungsinstanz betrieben. Wenn eine Anforderung zur Schlüssel-Zertifizierung akzeptiert wird, erzeugt die Zertifizierungsinstanz ein Schlüssel-Zertifikat.
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.
Zertifizierungsdiensteanbieter (ZDA)	Certification Authority, CA	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, CA	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, CA	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.
ZI	Zentralinstitut für die Kassenärztliche Versorgung	

Begriff	Synonym	Definition/Erläuterung
ZIS	Zugangs- und Integrationsschicht	
ZPVS	Zahnarztpraxisverwaltungssystem	
ZS	Zuzahlungsstatus	
Zugangskontrolle	Admission Control	Die Zugangskontrolle soll den unbefugten Zugang zu einem IT-System verhindern und führt hierzu eine *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.
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.
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.
Zulassung		Für den Einsatz in der Testphase müssen die Komponenten (*eGK, HBA, SMC, Kartenterminal, Konnektor*), Dienste und Einrichtungen zugelassen sein. Die Zulassung wird erteilt, wenn die Komponenten (*eGK, HBA, SMC, Kartenterminal, Konnektor*), Dienste und Einrichtungen für die Testung gemäß der zugrunde liegenden Spezifikationen funktionsfähig, interoperabel und sicher sind. Die gematik prüft die Funktionsfähigkeit und *Interoperabilität* auf der Grundlage der Prüfkriterien. Die Prüfung der Sicherheit erfolgt nach den Vorgaben des *BSI*. Werden die ((nicht-)funktionalen, sicherheitstechnischen und ggf. materialtechnischen) Voraussetzungen einer Zulassung erfüllt, so wird diese durch einen Zulassungsbescheid und eine Zulassungsurkunde erteilt. Eine Zulassung wird bescheinigt für Komponenten, Dienste und Einrichtungen, für die eine Zulassungshoheit vorliegt.

Begriff	Synonym	Definition/Erläuterung
Zulassungs-verfahren		Das Zulassungsverfahren ist Teil der Testmaßnahmen zur Einführung der *elektronischen Gesundheitskarte*. Für die Testmaßnahmen vorgesehene Komponenten werden durch die gematik funktional geprüft. Zusätzlich werden Sicherheitstests durch externe Prüflabore durchgeführt. Auf der Basis dieser Tests spricht die gematik die *Zulassung* bzw. die teilweise *Zulassung* für den Einsatz in den *Testregionen* aus.
Zurechen-barkeit	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.
Zuzahlungs-stand		Die Information, in welcher Höhe der *Patient* bereits *Zuzahlungen* geleistet hat.
Zuzahlungs-status		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.

Anhang

A1 – Abkürzungen

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

Generell werden Abkürzungen in den jeweiligen Ergebnisdokumenten des Projektes erläutert.

A2 – Glossar

Das vorliegende Dokument ist das zentrale Projektglossar.

A3 – Abbildungsverzeichnis

entfällt

A4 – Tabellenverzeichnis

entfällt

A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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) # Kapitel 4.4
[gemFK_VODM]	gematik: Einführung der Gesundheitskarte - Fachkonzept Verordnungsdatenmanagement
[gemPolicy]	gematik: Einführung der Gesundheitskarte - Betrieb der Gesundheitstelematik - Policy

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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
[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 (zuletzt geprüft am 14.12.2006)
[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)