ATG

Management-Papier zur Sicherheitsinfrastruktur

Aktionsforum Telematik im Gesundheitswesen

Köln, 2000

Version:	Meilenstein 1, Version 1.2b
Freigabe:	1.0 IK
Stand:	10.10.2000

Kontakt:
Jürgen Dolle (Koordinierung), GVG
mailto: j.dolle@gvg-koeln.de

Autoren-Team:
Dr. Hamid Farroukh, ABDA
Harald Flex, ITSG
Reinhold Mainz, KBV
Rudolf Meinert, DKG
Irmgard Siebert, KZBV
Wolfgang Strobel, AOK-BV

Inhaltsverzeichnis

Abbildungsverzeichnis

(Anmerkung: Die Abbildungen fehlen noch.)

0 Vorwort und Zielsetzung

Adressat dieses Dokuments sind die Verbände des deutschen Gesundheits- und Sozialsystems und ggfs. der Gesetzgeber.
Von der Basis der Gesundheitsberufe kommen sehr pragmatische Forderungen nach einer Verbesserung der (elektronischen) Kommunikation z. B. zur Unterstützung neuer kooperativer Versorgungsformen, deren Dynamik nicht zu unterschätzen ist. Da diese Kommunikationsvorgänge vertrauenswürdig sind, ist zu deren elektronischer Realisierung eine Sicherheitsinfrastruktur erforderlich.
Kommunikation im Gesundheitswesen findet organisationsübergreifend statt. Deshalb muß eine Sicherheitsinfrastruktur zur Unterstützung einer elektronischen Kommunikation gemeinsam von allen Partnern des Gesundheits- und Sozialsystems, welche die elektronische Kommunikation aktiv gestalten, vereinbart werden.
Eine Sicherheitsinfrastruktur sollte als Infrastrukturkomponente anwendungsneutral definiert und als Basis für beliebige Anwendungen aufgebaut werden. Dabei sind Dienste (z. B. Zertifikate, Zeitstempel) zur Unterstützung einer Kommunikations- und Informationsinfrastruktur und deren Zusammenwirken mit Prozessen zu beschreiben. Diese Beschreibung umfaßt auch eine Sicherheitspolitik (Policy), Organisationsstrukturen für Vertrauenswürdige Stellen (Trust Center) und Elemente zur Benutzung der Infrastruktur (z. B. Hard- und Softwarekomponenten). Ein wesentliches Ziel der Sicherheitsinfrastruktur ist die sichere, rechtssichere und vertrauenswürdige Kommunikation, deren Erfüllung beispielsweise durch die Dienste „Digitale Signatur“ und „Verschlüsselung“ erreicht werden soll. Daneben sind auch Dienste zur Anonymisierung und Pseudonymisierung zu betrachten, die besonders geeignet sind, den Schutz der Privatsphäre zu sichern.

Wesentliches Ziel der Sicherheitsinfrastruktur ist die Unterstützung einer sicheren, rechtssicheren und vertrauenswürdigen elektronischen Kommunikation und der Schutz der Privatsphäre.

Die Akzeptanz der Telematik im Gesundheitswesen wird um so höher sein, je sicherer die technische Ausgestaltung von Anwendungen ist.

Eine organisationsübergreifende elektronische Kommunikation benötigt eine von den Organisationen gemeinsam vereinbarte und verantwortete Sicherheitsinfrastruktur. Diese Sicherheitsinfrastruktur besteht sowohl aus Rahmenbedingungen und Vorgaben als auch- zumindest teilweise - aus Komponenten, welche die Selbstverwaltung bereitstellen muß oder für die ein finanzielles Anreizsystem sinnvoll sein könnte.

Die Sicherheitsinfrastruktur ist eine allgemeine Infrastrukturkomponente, die möglichst anwendungsneutral definiert und als Basis für beliebige Anwendungen aufgebaut werden sollte. Ihr Aufbau stellt sich als Querschnittsaufgabe dar.

Ziel dieses Managementpapiers ist es,

- den Handlungsbedarf für den Aufbau einer einheitlichen, flächendeckenden Sicherheitsinfrastruktur im Gesundheitswesen aufzuzeigen,
- diese Infrastruktur global zu beschreiben und

ausgehend von den vorhandenen Lösungen und Konzepten Wege für eine Umsetzung aufzuzeigen.

Der Handlungsbedarf und die Handlungsalternativen für den Aufbau einer einheitlichen, flächendeckenden Sicherheitsinfrastruktur in den Phasen Planung, Organisation, Implementierung und Ergebniskontrolle soll aufgezeigt werden.

1 Definition und Abgrenzung des Themas

Eine Telematik-Infrastruktur (Plattform) besteht in ihren technisch-organisatorischen Kernelementen aus den Komponenten Sicherheitsinfrastruktur, Kommunikationsinfrastruktur und Informationsinfrastruktur. Diese Komponenten bilden eine Gesamtarchitektur für informationstechnische Anwendungen.

0. Sicherheitsinfrastruktur

   Von der Sicherheitspolitik (Policy) bis zur Festlegung der Details von kryptografischen Verfahren müssen verbindliche Regeln abgestimmt werden.

1. Kommunikationsinfrastruktur

   Von einer allgemeinen Dienste-Infrastruktur über abgestimmte Basis-Dienste bis hin zu Verzeichnisdiensten sind verbindliche Definitionen für interoperable Verfahren erforderlich.

2. Informationsinfrastruktur

   Von Minimalanforderungen an die medizinische Dokumentation und die Strukturierung sowie Definition von Basiselementen für die technische Kommunikation bis hin zu technischen Elementen einer transparenten Speicherung und vertrauenswürdigen Verarbeitung sind verbindliche Festlegungen notwendig.

Die hier betrachtete Sicherheitsinfrastruktur dient der Sicherheit und Vertrauenswürdigkeit des Informationsaustausches zwischen den Kommunikationspartnern sowie dem Schutz der Privatsphäre. Dabei ist nicht nur der Kommunikationsvorgang selbst, sondern auch die Sicherheit und Vertrauenswürdigkeit der informationstechnischen Umgebung in die Betrachtung einzubeziehen.

Die informationelle - elektronisch unterstützte - Vernetzung des Gesundheitswesens stellt besondere Anforderungen an die Verfügbarkeit, Integrität, Verbindlichkeit und Vertraulichkeit von Informations- und Kommunikationsvorgängen.
Eine Sicherheitsinfrastruktur stellt organisatorische und technische Elemente und Dienste zur Verfügung, die Sicherheit und Vertrauenswürdigkeit beim Einsatz von Informations- und Kommunikationstechnik gewährleisten sollen. Zu den Kernelementen einer Sicherheitsinfrastruktur für das Gesundheitswesenzählen:

Neben rein technisch-organisatorischen Aspekten müssen auch rechtliche – insbesondere datenschutzrechtliche – Rahmenbedingungen betrachtet werden, da es auch um die Zulässigkeit bestimmter elektronischer Transaktionen geht. Dieses Dokument beschäftigt sich jedoch schwerpunktmäßig mit den technisch-organisatorischen Aspekten.

- autorisierte organisatorische Stellen zur Ausgabe von elektronischen Ausweisen/Zertifikaten,
- elektronische Ausweise für die beteiligten Personen (Patienten, "Health Professionals" und andere Beteiligte) sowie Organisationen,

Die Sicherheit der angeschlossenen beteiligten Systeme bedarf einer separaten Betrachtung.

- Verfahren/Regeln zur Authentisierung sowie zur Verschlüsselung und Signierung von Daten,
- Verfahren/Regeln zur Sicherung von Anwendungen und Transportwegen.

Die Sicherheitsinfrastruktur soll für alle zukünftigen Anwendungen geeignet sein. Allerdings kann der Aufbau stufenweise und in erweiterbarer Weise in der Form erfolgen, daß zunächst die Bedürfnisse prioritärer Anwendungen erfüllt werden.

Dieses Dokument behandelt ausschließlich Elemente, Dienste und Funktionen einer Sicherheitsinfrastruktur, die einen vertrauenswürdigen und sicheren Informationstransport zwischen Beteiligten im Gesundheitswesen ermöglichen. Hierzu gehören auch Dienste zum Schutz der Privatsphäre, wie Anonymisierung und Pseudonymisierung.
Beteiligte an Kommunikationsvorgängen sind dabei natürliche Personen, Organisationen/Institutionen und technische Systemkomponenten.
Die Sicherheit der beteiligten Systeme selbst liegt in der Verantwortung der diese betreibenden Organisationen. Hierfür können lediglich Empfehlungen ausgesprochen werden.
Die Infrastruktur soll - auf der Basis von Standards - für alle zukünftigen Anwendungen geeignet sein, muß jedoch vor allem die mit Priorität geplanten Anwendungen "Rezept" und "Arztbrief" abdecken. Anhand von Szenarien kann geprüft werden, ob sich die Sicherheitsinfrastruktur auch für weitere Anwendungen eignet.

2 Anforderungen

Damit zukünftige Kommunikationsbeziehungen für organisationsübergreifende Anwendungen miteinander funktionieren, bedarf es einer einheitlichen Plattform. Auf der Grundlage von einheitlichen rechtlichen, organisatorischen und technischen Regeln soll eine interoperable Sicherheitsinfrastruktur für einen übergreifenden, standardisierten Informationstransport bereitgestellt werden. Diese Infrastruktur soll Regeln umfassen für die Feststellung der Identität/Rolle einer Person oder Organisation (Authentizität) und den sicheren Informationstransport (Integrität, Verbindlichkeit, Vertraulichkeit, Verfügbarkeit, Zugriffsschutz, differenzierte und auftragsbezogene Zugriffsrechte). Eine wesentliche Grundlage einer elektronischen Kommunikation sind dabei Adreßbücher, in denen die Kommunikationspartner sicher identifiziert werden können.

Die Sicherheitsinfrastruktur soll in ihrer Umsetzung in den Bereichen, in denen die digitale Signatur zum Einsatz kommt, auch die Anforderungen des deutschen Signaturgesetzes erfüllen.

Als Basisinvestition für zukünftige Anwendungen muß eine einheitliche Infrastruktur aufgebaut werden. Zur Ausgestaltung einer problemlosen, organisationsübergreifenden elektronischen Kommunikation sind einheitliche rechtliche, organisatorische und technische Regeln erforderlich.

Die bei der traditionellen Informationsübermittlung geltenden Regeln müssen bei einer elektronischen Kommunikation explizit abgebildet werden. Wo die elektronische Kommunikation neue Möglichkeiten schafft, sind auch neue Regeln und Prinzipien zu definieren.

Die Kommunikationsvorgänge sollen in den Bereichen, in denen die digitale Signatur zum Einsatz kommt, nach den Vorgaben des – derzeit novellierten - Signaturgesetzes abgesichert werden, so daß auch eine rechtssichere elektronische Kommunikation möglich wird.

3 Bestandsaufnahme

3.1 Ist-Situation

3.1.1 Beschreibung der Ist-Situation

Die bestehenden Anwendungen im Gesundheits- und Sozialsystem benutzen derzeit keine organisationsübergreifende, flächendeckende, gemeinsame Infrastruktur.
Allerdings gibt es bereits Anwendungen, die sich einer Sicherheitsinfrastruktur bedienen.
Die Gesetzlichen Krankenkassen, die Sozialversicherungen und die Leistungserbringer tauschen heute Daten in dem jeweils zugelassenen Umfang auf maschinell verwertbaren Datenträgern oder mittels Datenfernübertragung aus. Diese Datenlieferungen bilden die Grundlage u.a. für die Genehmigung und Zahlung von Leistungen. Entsprechende Verträge zwischen den Spitzenverbänden regeln den technischen Rahmen und die Verfahren zum Schutz des Transportes der Datenübertragungen. Darüber hinaus gibt es eine Reihe konzeptioneller Überlegungen und Vorarbeiten zum Aufbau einer zukünftigen Sicherheitsinfrastruktur.

Es gibt derzeit keine flächendeckend von allen Organisationen des Gesundheits- und Sozialsystems benutzte Sicherheitsinfrastruktur für die elektronische Kommunikation. Allerdings gibt es am Markt und bei einigen Organisationen des Gesundheits- und Sozialsystems grundsätzlich geeignete Sicherheitsinfrastrukturen, die allerdings zum Teil spezifischen Anwendungen dienen und außerdem noch der Anpassung für eine einheitliche Infrastruktur bedürfen.

Komponenten einer zukünftigen Sicherheitsinfrastruktur sind in hieran interessierten Kreisen – zum Teil auch bereits im Konsens – beschrieben worden. Auf diesen Arbeiten kann aufgebaut werden. Allerdings liegt der Schwerpunkt nicht auf der Vervollständigung der technischen Arbeiten, sondern bei der Bewertung der Ergebnisse und bei konkreten Festlegungen. Als Beispiele für bereits weithin akzeptierte technische Festlegungen seien genannt: SSL für die sichere Kommunikation zwischen Anwendungen oder Rechnern, S/MIME als Transportprotokoll, Triple DES für eine symmetrische Verschlüsselung, RSA mit einer Schlüssellänge von 1024 Bit für die asymmetrische Verschlüsselung, SHA-1 oder RIPEMD160 als Hash-Verfahren, Zertifikatstrukturen gem. X.509V3, Chipkartenterminals gem. MKT-Spezifikation.

In einigen regionalen Projekten in Deutschland (z. B. Krebsregister Magdeburg, QuasiNiere) wurden exemplarisch Sicherheitsinfrastrukturen implementiert, die als Muster für eine flächendeckende Infrastruktur in die Betrachtungen einbezogen werden können.

Auf nationaler, europäischer und internationaler Ebene wurden in den letzten Jahren eine Vielzahl von Normen und Normentwürfen erarbeitet, die als Grundlage für den Aufbau einer Telematik-Infrastruktur benutzt werden können. Diese Arbeiten sind nicht abgeschlossen.

Daneben gibt es im Gesundheitswesen Vorarbeiten zum Aufbau einer gemeinsamen Infrastruktur und geeignete regionale Beispiele für eine Realisierung. Auf diesen Arbeiten kann aufgebaut werden. Allerdings liegt der Schwerpunkt nicht auf der Vervollständigung der technischen Arbeiten, sondern bei der Bewertung der Ergebnisse und bei konkreten Festlegungen.

3.1.2 Bewertung der Ist-Situation

Heute wird im Gesundheitssystem bereits umfangreich und teilweise ohne die rechtlich erforderliche und technisch mögliche Sicherheit elektronisch kommuniziert. Diese Situation bedarf dringend einer Änderung.

Zum Aufbau einer gemeinsamen Sicherheitsinfrastruktur sind Vereinbarungen zur interoperablen Verbindung von separaten Sicherheitsinfrastrukturen erforderlich. Diese Vereinbarungen und die Anforderungen aus neuen Anwendungen haben die Anpassung und Erweiterung vorhandener Sicherheitsinfrastrukturen zur Folge.

Die beteiligten Organisationen müssen die Benutzung der Sicherheitsinfrastruktur daneben in einem Rahmenwerk beschreiben.

Für die Benutzung einer einheitlichen Infrastruktur und für interoperable Verfahren bedarf es vor allem vereinbarter Standards für eine offene, übergreifende elektronische Kommunikation. Diese Standards sollten grundsätzlich auf der Basis von (internationalen) Normen, können aber auch auf der Basis von Normentwürfen oder auf der Grundlage allgemein akzeptierter Firmenstandards festgelegt werden. Normen oder Industriestandards stehen jedermann zur Anwendung frei. Es sei denn, Normen sind, z. B. durch einen Vertrag oder durch ein Gesetz, verbindlich gemacht worden. Auch Normen oder Standards definieren häufig nur einen allgemeinen Rahmen, der eine Reihe von Optionen beinhaltet. Dies bedeutet, daß bezüglich dieser Optionen Festlegungen getroffen werden müssen. Bei jeder notwendigen Festlegung ist im Einzelfall zu prüfen, welche relevanten Normen oder Standards in die Überlegungen einbezogen werden sollten. Noch ausstehenden Standardisierungsarbeiten muß ein erheblicher Stellenwert eingeräumt werden.

Zur Herstellung der rechtlich gebotenen vertrauenswürdigen und sicheren elektronischen Kommunikation sind dringend Maßnahmen erforderlich.

Beispiele für möglicherweise geeignete Sicherheitsinfrastrukturen existieren in einigen Projekten. Vorhandene Sicherheitsinfrastrukturen der Selbstverwaltung bedürfen der Anpassung.

Aus (kommerziell) verfügbaren Sicherheitslösungen und auf der Grundlage von Arbeiten interessierter Kreise und von Standardisierungseinrichtungen können interoperable Sicherheitsinfrastrukturen aufgebaut werden, die durch gemeinsame Absprachen eine übergreifende Sicherheitsinfrastruktur bilden.

Die Verwendung der Sicherheitsinfrastruktur ist organisationsspezifisch in einem Rahmenwerk zu beschreiben.

Auf der Grundlage existierender Normen und Standards oder auf der Basis von Entwürfen müssen jeweils eine konkrete Auswahl und konkrete Festlegungen nach einer solchen Auswahl getroffen werden, um wirklich zu einer gemeinsam nutzbaren Infrastruktur und zu interoperablen Verfahren zu kommen. Diese Festlegungen müssen grundsätzlich in Verträgen der Selbstverwaltung für solche Anwendungen verbindlich gemacht werden, für die die Selbstverwaltung verantwortlich ist.

3.2 Rahmenbedingungen

Die besonders sensiblen Informationen (z. B. personenbezogene Gesundheitsdaten), die im Gesundheits- und Sozialsystem elektronisch kommuniziert werden sollen, bedürfen höchster Anstrengungen zur Gewährleistung der Sicherheit und Vertraulichkeit von auf ihnen beruhenden Kommunikationsvorgängen.

Die Infrastruktur muß grundsätzlich ein Sicherheitsniveau gewährleisten, daß den hohen Ansprüchen an den Schutz von personenbezogenen Gesundheitsdaten gerecht wird, wenn auch nicht alle Anwendungen ein gleich hohes Niveau benötigen.

Wegen der organisationsübergreifenden Kommunikationsvorgänge ist eine einheitliche Infrastruktur erforderlich; sie kann nur gemeinsam von allen Beteiligten definiert und aufgebaut werden. Hierzu besteht ein allgemeiner Konsens. Neben den rechtlichen, organisatorischen und technischen Fragen ist auch ein Finanzierungsmodell für gemeinsame Maßnahmen und Strukturelemente erforderlich.

Die Realisierung einer Sicherheitsinfrastruktur dient der Bereitstellung einer organisatorisch-technischen Plattform. Sie verändert keine bestehenden Strukturen oder Geschäftsprozesse, schafft aber eine Voraussetzung zu ihrer Anpassung und Weiterentwicklung. Sie dient zur Realisierung beliebiger Anwendungen und trägt hierdurch indirekt zur Veränderung von Prozessen der Gesundheitsversorgung bei. Die Implementierung der Sicherheitsinfrastruktur kann nur im zeitlichen Zusammenhang mit einigen Anwendungen durchgeführt werden, die geeignet sind, die Infrastruktur zu finanzieren. Besonders geeignet sind solche Anwendungen, die dem gestiegenen Informationsbedürfnis bei kooperativen Versorgungsformen gerecht werden.

Die Bereitstellung einer einheitlichen Sicherheitsinfrastruktur ist eine gemeinsame Aufgabe aller Organisationen des Gesundheits- und Sozialsystems.

Die Sicherheitsinfrastruktur ist Voraussetzung für viele Anwendungen und muß deshalb für deren Realisierung bereitgestellt werden.

3.2.1 Rechtliche Dimension

Die Neufassung des Signaturgesetzes (SigGÄndG, Kabinettsentwurf) eröffnet die Möglichkeit zur Gleichstellung elektronischer Unterschriften mit eigenhändigen. Darüber hinaus können zur Umsetzung des Signaturgesetzes im öffentlichen Bereich zusätzliche Voraussetzungen an die Sicherheitsinfrastruktur gestellt werden (Akkreditierung der Zertifizierungsstelle). Unklar ist, ob und in wieweit das Gesundheits- und Sozialsystem diesen zusätzlichen Anforderungen unterliegen soll.
Die Regelungen zur Sicherheit und zu den Verfahren in der Telekommunikation im Sinne der regelhaften Berufsausübung sind u. a. Gegenstand der Arbeit der zuständigen Berufsorganisationen (z. B. Kammern) auf der Leistungserbringerseite. Deshalb wird konkret zu prüfen sein, ob und welche neuen/ergänzenden berufsrechtlichen und anderen rechtlichen Regelungen begleitend zum Aufbau einer Sicherheitsinfrastruktur erforderlich sind. Als maßgebliche „Rechtskreise“ sind insbesondere das allgemeine Gebot der Schweigepflicht für Heilberufe und die Datenschutzgesetze zu beachten (Fragen der Zulässigkeit, Anforderungen an technische und organisatorische Maßnahmen der Datensicherheit, z. B: „10 Gebote“ des § 9 BDSG i. V. mit der Anlage hierzu).

Eine verbindliche elektronische Kommunikation wird in absehbarer Zeit durch die Gleichstellung Digitaler Signaturen mit eigenhändigen Unterschriften sowohl im privaten Recht als auch im öffentlichen Recht ermöglicht.

Das Signaturgesetz in seiner beabsichtigten Fassung ermöglicht dem öffentlichen Bereich, zusätzliche Anforderungen an die Sicherheitsinfrastruktur zur Erzeugung Digitaler Signaturen zu stellen. Es ist – im europäischen Kontext – zu prüfen, ob derartige zusätzliche Anforderungen sinnvoll sind. Im europäischen Rahmen ist die „Reichweite“ von Rahmenbedingungen und Lösungen zu beachten.

Die Sicherheitsinfrastruktur bedarf unter Umständen rechtlicher Regelungen, z. B. auf der Ebene der Berufsordnungen der Leistungserbringer.

3.2.2 Organisatorisch-technologische Dimension

Aufgaben einer Sicherheitsinfrastruktur müssen zum Teil selbst wahrgenommen werden, für andere können Dienstleister in Anspruch genommen werden.

Für den Aufbau einer Sicherheitsinfrastruktur gibt es heute bereits eine Reihe von Definitionen, Standards, etablierten Verfahren und Mechanismen, deren Nutzung im Hinblick auf nationale und internationale Interoperabilität unumgänglich ist. Die Sicherheitsinfrastruktur soll deshalb zur Herstellung einer umfassenden Interoperabilität auf der Grundlage von internationalen Normen realisiert werden. Die optionalen Parameter müssen dabei zwischen allen Vertragspartnern durch konkrete und einheitliche Absprachen festgelegt werden.

Die konkrete Ausgestaltung einer einheitlichen Infrastruktur bedarf der Absprachen zwischen allen Vertragspartnern, auch zu organisatorischen und technischen Details. Dabei geht es weniger um die technischen Definitionen als vielmehr um verbindliche Entscheidungen für deren Einsatz und um Festlegungen, wo es einen Entscheidungsspielraum gibt.

Bei der Realisierung der technischen Elemente einer Sicherheitsinfrastruktur können neben kommerziellen - zum Signaturgesetz konformen - Einrichtungen auch bestehende organisatorische und technische Einrichtungen des Gesundheits- und Sozialsystems genutzt werden, sofern sie die Anforderungen an die Sicherheitsinfrastruktur erfüllen.

Noch ausstehenden Standardisierungsarbeiten muß ein hoher Stellenwert eingeräumt werden.

Organisatorische Aufgaben einer Sicherheitsinfrastruktur müssen teilweise auch von Organisationen des Gesundheits- und Sozialsystems selbst wahrgenommen werden (z. B. Ausgabe von elektronischen Ausweisen).

Die Benutzung einer einheitlichen Sicherheitsinfrastruktur bedarf vertraglicher Vereinbarungen aller Beteiligter, damit die erforderlichen Festlegungen verbindlich werden.

Von der Einführung einer Sicherheitsinfrastruktur sind nicht nur die Organisationen des Gesundheits- und Sozialsystems, sondern vor allem die Nutzer von Anwendungen (z. B. Ärzte, Zahnärzte, Apotheker, Angestellte in Versicherungen) einschließlich der Patienten/Versicherten betroffen. Dabei bedürfen die elektronischen Hilfsmittel zur Ausgestaltung/Sicherung des informationellen Selbstbestimmungsrechts einer besonderen Betrachtung.
Die derzeit dort vorhandene EDV-Infrastruktur muß in bezug auf die Fähigkeit zur Integration in eine Sicherheitsinfrastruktur überprüft und angepaßt werden. Der Aufbau einer flächendeckenden Sicherheitsinfrastruktur wird daher nicht kurzfristig zu bewerkstelligen sein.

Von einer Sicherheitsinfrastruktur im Gesundheits- und Sozialwesen sind möglicherweise alle Bürger betroffen. Die Ausgestaltung ihrer Beteiligung in elektronischen Verfahren bringt neue Anforderungen mit sich.

Die vorhandene informationstechnische Infrastruktur – insbesondere bei den einzelnen Leistungserbringern – wird nur mit Schwierigkeiten in eine neue Sicherheitsinfrastruktur eingebunden werden können. Deshalb ist von Übergangszeiten auszugehen.

(Achtung:
Die fehlenden Kapitel 4 – 7 werden zu den folgenden Meilensteinen 2 und 3 vorgelegt.)

Indexverzeichnis

(Anmerkung: Der Index fehlt noch.)