

Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz („MAGDA-LENA“)

**STRING-Kommission beim Bundesministerium
für soziale Sicherheit und Generationen**

Teil 2: Hauptteil

Version 2.0 vom 21. 6. 2000

Die aktuelle Version im Internet:
www.bmsg.gv.at
bzw.
www.akh-wien.ac.at/STRING/

I N H A L T

1.	<i>Definition, Grundsätze, allgemeine Ziele, Stellung des Patienten.....</i>	3
2.	<i>Allgemeine Inhalte, Modelle, Standards.....</i>	8
3.	<i>Identifikationsvariablen.....</i>	12
3.1.	MAGDA-LENA Kommunikationsteilnehmer-ID.....	12
3.1.1	Authentifizierung	12
3.1.2	Registrierte Directories	12
3.1.3	Rollen der Teilnehmer	13
3.1.4	ID der Dokumente	13
3.2	 Patienten-ID	14
3.2.1	Patienten-ID bei allgemeinem Datenaustausch.....	14
3.2.2	Patienten-ID bei bilateralem Datenaustausch	14
4.	<i>Datenschutz und Datensicherheit</i>	15
4.1	MAGDA-LENA II Sicherheitspolitik.....	15
4.2	Rahmenbedingungen	15
5.	<i>Netzbetreiber, Netzübergänge.....</i>	18
5.1	 Netzbetreiber.....	18
5.1.1	Richtlinien für den einzelnen Netzbetreiber	20
5.1.2	Richtlinien hinsichtlich der Interoperabilität	21
5.2.	 Netzübergänge	24
5.2.1	Netzübergänge zwischen Netzbetreibern.....	24
5.2.2	Netzübergänge zwischen Client und Netzbetreiber	24
5.2.3	Netzwerkschnittstellen.....	25
6.	<i>Konformität</i>	26
7.	<i>Anhang IV.a: Anforderung an Verfahren und Mechanismen (normativ)</i>	31
8.	<i>Anhang IV.b: Sicherheitsmaßnahmen und Sicherheitsempfehlungen (normativ gemäß Konformitätserklärung).....</i>	34
8.1	Sicherheitsmaßnahmen.....	34
8.2	Empfehlungen	35
9.	<i>Glossar und Abkürzungsverzeichnis</i>	38

1. Definition, Grundsätze, allgemeine Ziele, Stellung des Patienten

In diesem einleitenden Kapitel werden einige grundlegende Begriffe definiert, die allgemeinen Ziele erläutert und auf die Stellung und die Rechte des Patienten¹⁾ eingegangen.

XXXXXXXXXXXXXXXXXXXXXX

Definition:

- 1.1 Unter dem „österreichischen Gesundheitsdatennetz MAGDA-LENA“ (Medizinisch-Administrativer Gesundheitsdatenaustausch – Logisches und Elektronisches Netzwerk Austria) ist die Verbindung von Einrichtungen (Leistungsanbieter, Leistungserbringer, Administration, Kostenträger,...) des Gesundheits- und Sozialwesens zum Zweck des elektronischen Datenaustausches direkt oder indirekt personenbezogener, multimedialer Informationen zu verstehen. Daten ohne Patientenbezug fallen nicht unter die MAGDA-LENA Rahmenbedingungen.
- 1.2 MAGDA-LENA ist kein neues, eigenständiges Netz, sondern entsteht aus der koordinierten Entwicklung von untereinander kompatiblen Ansätzen, wobei auch Schnittstellen zu internationalen Gesundheitsnetzen, so ferne diese dem Standard von MAGDA-LENA entsprechen, gegeben sein soll. Nationale und internationale Standards und Normen sind im Hinblick auf Interoperabilität der Systeme zu berücksichtigen.
- 1.3 MAGDA-LENA ist keine Norm, sondern enthält Richtlinien, um Schnittstellenprobleme zwischen verschiedenen Leistungsanbietern zu vermeiden. Diese Richtlinien stellen eine Mindestanforderung dar.
- 1.4 Die Teilnahme an diesem logischen Gesundheitsdatennetz ist an die Erfüllung der nachstehend formulierten Richtlinien gebunden. Jeder Sender und Empfänger muss eine gesetzliche Befugnis zur Verwaltung von personenbezogenen Gesundheitsdaten haben.

Datenschutz:

- 1.5 Das Datenschutzgesetz, Signaturgesetz und die für den jeweiligen Absender und Empfänger gültigen Gesetze (Krankenanstaltengesetz, Ärztegesetz, Sozialhilfegesetz usw.) sind unbedingt einzuhalten.
- 1.6 Datenschutzrechtliche Bestimmungen für die Verwendung von Gesundheitsdaten:

Daten dürfen nur verarbeitet und übermittelt werden, wenn:

¹ Unter dem Begriff „Patient“ werden hier auch kranke und gesunde BürgerInnen, Pflegefälle, Asylierungsfälle usw. zusammengefasst

- Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind (§ 7 Abs. 1 DSG 2000)

und

- schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (§ 7 Abs. 1 DSG 2000). Da Gesundheitsdaten sensible Daten iSd. § 4 Z 2 DSG 2000 sind, gilt § 9 DSG 2000, wonach die Verwendung von Daten nur in bestimmten Fällen zulässig ist; für den Bereich der Gesundheitsdaten sind die wichtigsten dieser Fälle, dass

sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (§ 9 Abs. 3 DSG 2000),

oder

der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (§ 9 Abs. 6 DSG 2000),

oder

die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann, z.B. Behandlung im Notfall (§ 9 Abs. 7 DSG 2000),

oder

die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich sind und die Verwendung dieser Daten durch ärztliches Personal oder sonstiges Personal erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen (§ 9 Abs. 12 DSG 2000).

Die Weiterverwendung von personenbezogenen Daten für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 DSG 2000 zulässig.

Im übrigen sind bei der Ausgestaltung einer konkreten Datenanwendung die folgenden Grundsätze einzuhalten:

Die Daten dürfen verwendet werden, wenn

- die Verwendung nach Treu und Glauben und auf rechtmäßige Weise geschieht;
- sie für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden;
- soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;

- so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
- solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben (§ 6 Abs. 1 DSGVO 2000)

Teilnehmer/Provider:

1.7 Teilnehmer an MAGDA-LENA (im folgenden Teilnehmer) kann nur ein Auftraggeber im Sinne des DSGVO 2000 sein, der aufgrund seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnisse (§7 Abs. 1 DSGVO 2000) berechtigt ist, patientenbezogene Daten zu verarbeiten und zu übermitteln und der sich zur Einhaltung der in MAGDA-LENA definierten Richtlinien verpflichtet (siehe Konformitäts-Erklärungen, Kapitel 6).

Die Konformitäts-Erklärung enthält (Details siehe Kapitel 6):

1. die Rechtsgrundlagen und den Zweck für Verarbeitung und Übermittlung
2. die Verpflichtung über die Einhaltung des DSGVO 2000 und der Datenschutz- / Datensicherheitsmaßnahmen durch den Teilnehmer (in seinem eigenen Bereich) (Empfehlung dazu im Anhang IV.b und IV.c).
3. Bekanntgabe seiner Identifikationsdaten gemäß Kapitel 3
4. die Verpflichtung der Einhaltung der in Anhang IV.a definierten Kriterien für die sichere Verschlüsselung der Daten bei der Übertragung
5. den Inhalt und die formale Struktur der übermittelten Daten (Kapitel 2)
6. Verpflichtung als MAGDA-LENA-Provider gemäß Kapitel 5

Jeder Teilnehmer muss eine Erklärung nach (1), (2) und (3) abgeben.

Die Erfüllung von (4) und/oder (5) kann an einen MAGDA-LENA-konformen Dienstleister (= Provider) übertragen werden, der die MAGDA-LENA konforme Kommunikation zwischen Teilnehmern garantiert (Kapitel 5). Der MAGDA-LENA-Provider muss eine Konformitätserklärung nach (2), (3), (4), (5) und (6) abgeben.

1.8 Ein MAGDA-LENA-Provider muss den Anschluss MAGDA-LENA-konformer Teilnehmer direkt oder über einen anderen MAGDA-LENA-konformen Provider erlauben. (Allfällige Kosten für die Verbindung zu einem anderen MAGDA-LENA-konformen Provider sind vertraglich festzulegen).

1.9 Dem Stand der Technik muss stets Rechnung getragen werden.

1.10 Mit der Datenübermittlung können auch Netzbetreiber beauftragt werden (siehe Kapitel 5). Diese Netzbetreiber müssen die in Kapitel 5 formulierten Richtlinien erfüllen.

- 1.11 Die Verantwortung für die Speicherung und die inhaltliche Verantwortung für die Daten bleiben immer bei der für die Behandlung und Dokumentation zuständigen Institution.

Datensatz

- 1.12 Jeder personenbezogene Datensatz muss eine eindeutige Identifikation der Person – so ferne anonymisierte Daten enthalten sind, eine eindeutige Identifikation des Falls - des Behandlungsfalles (z.B.: eindeutige Aufnahmezahl), des Absenders und der Empfänger, Datum der Erstellung des Dokuments, für das Dokument verantwortliche Person oder Institution (z.B.: Arzt, Ärztlicher Direktor, ...) enthalten.
- 1.13 Diese Nachrichtenidentifikation muss auch in der Empfangsbestätigung enthalten sein.

Allgemeine Ziele

- 1.14 Ein elektronischer Austausch von Gesundheitsdaten erfolgt zwischen berechtigten Teilnehmern zum Zweck der effizienten Behandlung von Patienten – einschließlich Telekonsultation zwischen Leistungserbringern. Er soll die Verwaltungstätigkeit effizienter gestalten und auch die medizinisch-wissenschaftliche Forschung unterstützen.
- 1.15 Jede Gesundheitseinrichtung hat Zugang zu den für die aktuelle Versorgung eines Menschen notwendigen Informationen unter Wahrung der Rechte auf Geheimhaltung des Betroffenen.
- 1.16 Auf diese Weise soll eine unnötige mehrfache Erfassung identischer Informationen vermindert werden.
- 1.17 Diese Maßnahmen sollen eine Verbesserung der Versorgungsqualität und eine Erhöhung der Effizienz der Patientenbetreuung bei gleichzeitiger Kostenreduktion bewirken.
- 1.18 Die Vertragspartner erklären sich bereit, das System auf die jeweils aktuelle MAGDA-LENA Version nachzuführen. Auf eine Kompatibilität nachfolgender Systeme ist zu achten.

Stellung des Patienten

- 1.19 Jede elektronische Weitergabe von Patientendaten darf nur auf Basis bestehender gesetzlicher Regelungen erfolgen.
- 1.20 Es darf keinen unautorisierten und unprotokollierten Austausch von Gesundheitsdaten zwischen zwei oder mehreren berechtigten Institutionen geben.

- 1.21 Der Patient hat das Recht, die Weitergabe seiner medizinischen Daten an einen Arzt seines Vertrauens oder – gemäß den im Krankenanstaltengesetz formulierten Einschränkungen – und auch an sich selbst zu verlangen.
- 1.22 Nur wenn es unbedingt erforderlich ist, sind Daten patientenbezogen zu übermitteln. Wo immer es möglich ist, muss die Verwendung der Daten und der Datenaustausch in indirekt personenbezogener Form erfolgen.

2. Allgemeine Inhalte, Modelle, Standards

Zusammenfassung:

Der elektronische Austausch patientenbezogener Daten setzt genaue Vereinbarungen über den Inhalt der auszutauschenden Daten voraus. Weiters muss - zumindest im Fall einer automatischen Weiterverarbeitung der übermittelten Dateninhalte - der gesamte Kommunikationsprozess modelliert werden, wobei das externe Verhalten der Kommunikationspartner festzulegen ist.

Auf Grund der großen Anzahl an Kommunikationspartnern im Gesundheitswesen können diese Festlegungen nicht bilateral zwischen den jeweiligen Partnern vereinbart, sondern nur generell festgelegt werden. Deshalb wird international intensiv an der Entwicklung solcher Informationsmodelle des Gesundheitswesens als Grundlage für Standardnachrichten gearbeitet.

In diesem Kapitel wird dazu festgelegt:

- a) Bereits vorhandene internationale oder nationale Standards der Medizinischen Informatik sind im Rahmen von MAGDA-LENA unbedingt zu verwenden.
- b) Existieren für einen Anwendungsbereich solche Standards noch nicht, so hat die Entwicklung der Nachrichten entsprechend dem im folgenden beschriebenen Vorgehensmodell zu erfolgen, um eine möglichst große Einheitlichkeit der Nachrichten zu erreichen. Das beschriebene Vorgehensmodell basiert auf internationalen Vorgaben.

In Anhang II.a werden die existierenden inhaltlichen CEN-Standards und Ö-Normen aufgezählt.

Hinweis: Technische Standards werden in Kapitel 5 behandelt.

XXXXXXXXXXXXXXXXXXXX

2.1 Jeder Datenaustausch ist durch ein Informationsmodell zu beschreiben. Dieses muss die Kommunikationsprozesse und das Datenmodell exakt beschreiben. So sind beispielsweise die einzelnen Teilschritte bei Prozessen wie „Patientenadministration“ genau zu spezifizieren. Dabei werden Ereignisse (z.B. Patientenaufnahme) auf entsprechende Nachrichten abgebildet. Die Reihenfolge und der Ablauf der einzelnen Nachrichten, ihr Inhalt sowie die Reaktionen auf jede empfangene Nachricht sind für jeden beteiligten Partner genau festzulegen. Nur auf Basis eines solchen „Informationsmodells“ können Routinevorgängen zwischen den verschiedenen Partner des Gesundheitswesens nutzbringend automatisiert werden.

2.2 Die Entwicklung von Nachrichten für das österreichische Gesundheitsdatennetz sollte systematisch auf Basis eines Gesamtmodells des Gesundheitswesens erfolgen. Bei dieser Vorgehensweise geht jeder Entwicklung einer neuen

Nachricht eine entsprechende Modellbildung und eine Harmonisierung mit dem Gesamtmodell voran. Dadurch wird die Kompatibilität der einzelnen Nachrichten sichergestellt und die Entwicklung und Wartung derselben vereinfacht.

An einem Informationsmodell des Gesundheitswesens wird international gearbeitet². Zum gegenwärtigen Zeitpunkt ist ein solches aber noch nicht verfügbar. Daher ist momentan folgendermaßen vorzugehen:

- a) Bereits vorhandene internationale oder nationale Standards der Medizinischen Informatik sind im Rahmen von MAGDA-LENA unbedingt zu verwenden (siehe AnhangII.a).
- b) Existieren für einen Anwendungsbereich solche Standards noch nicht, so hat die Entwicklung der Nachrichten entsprechend dem im folgenden beschriebenen Vorgehensmodell zu erfolgen, um eine möglichst große Einheitlichkeit der Nachrichten zu erreichen.
- c) Ein Teilnehmer / Provider hat zu erklären, dass er eventuell bereits im Einsatz stehende Nachrichten/Codeverzeichnisse, welche noch nicht den Spezifikationen der aktuellen MAGDA-LENA-Version entsprechen, bis 30. Juni 2002 auf solche, die diese Spezifikationen erfüllen, umstellen wird. Ein Überschreiten dieser Frist bedarf der begründeten Mitteilung an das BMSG.

2.3 Das **Vorgehensmodell zur Entwicklung von Nachrichten** basiert auf internationalen Vorgaben. Folgende Schritte sind von den Entwicklern einzuhalten (Details und Beispiele: vgl. AnhangII.b):

1) Spezifikation des Anwendungsbereichs

Das Ziel dieses Schrittes ist eine sprachliche Beschreibung jenes Anwendungsbereichs, in dem die zu entwickelnden Nachrichten eingesetzt werden. Hierbei sind die Parteien, die von der neuen Nachricht vermutlich betroffen sind, sowie die wichtigsten Kommunikationspartner und deren zugeordneten Rollen anzuführen. Weiters sind die speziellen Fachgebiete, die unterstützt werden, sowie die verschiedenen Anwendungsfälle der neuen Nachricht in textueller Form zu beschreiben.

2) Benutzeranforderungen und Anwendungsfälle

Gemeinsam mit Experten des betroffenen Anwendungsbereichs muss eine Anforderungsanalyse durchgeführt werden, welche die Anforderungen an den elektronischen Informationsaustausch klärt. Dafür ist ein gemeinsames Verständnis über die Akteure und die Anwendungsfälle des betrachteten Anwendungsbereichs zu erreichen. Weiters sind in einem Modell die Beziehungen sowohl zwischen Akteuren und Anwendungsfällen als auch zwischen den unterschiedlichen Anwendungsfällen festzulegen.

3) Kommunikationsrollen und unterstützte Dienste

² beispielsweise am Reference Information Model von HL7

Von den Benutzeranforderungen und den einzelnen Anwendungsfällen ausgehend wird durch Verallgemeinerung ein Abstraktionsprozess durchgeführt. Resultate dieser Abstraktion sind die Kommunikationsrollen und die benötigten Allgemeinen Nachrichtenbeschreibungen (vgl. 2.3/Ziffer 5). Auch die Regeln zu deren Austausch sowie der Zusammenhang zwischen den Kommunikationsrollen und den Nachrichten werden als Basis für die weitere Vorgehensweise festgelegt.

Dieser Schritt erfolgt eng verzahnt mit dem vorher beschriebenen Schritt der Erhebung der Benutzeranforderungen und Anwendungsfälle: Während jener primär in das Aufgabengebiet der Experten des betroffenen Anwendungsbereiches fällt, werden die hier beschriebenen Arbeitsschritte von Experten der Analyse und Modellierung durchgeführt.

4) Domäneninformationsmodell

Das Domäneninformationsmodell stellt ein statisches Modell des Anwendungsbereichs dar, das die Klassen, deren Attribute sowie die Beziehungen zwischen den Klassen umfasst. Es dient als übergeordnetes Referenzmodell für die verschiedenen, daraus abgeleiteten, allgemeinen Nachrichtenbeschreibungen. Sämtliche Allgemeinen Nachrichtenbeschreibungen bilden Untermengen des Domäneninformationsmodells.

5) Allgemeine Nachrichtenbeschreibungen

Die Allgemeinen Nachrichtenbeschreibungen sind das wichtigste, syntaxunabhängige Ergebnis des gesamten Entwicklungsprozesses. Sie beschreiben die kommunikationsspezifischen Sichten des Informationsmodells. Jede allgemeine Nachrichtenbeschreibung stellt den Informationsgehalt und die semantische Struktur einer Nachricht, oder einer Menge von Nachrichten gleichen Musters dar. Sie wird durch Bildung eines Teilmodells mittels Reduktion aus dem Domäneninformationsmodell erzeugt.

6) Allgemeine hierarchische Nachrichtenbeschreibung

Die Allgemeinen Nachrichtenbeschreibungen müssen zur Implementierung in hierarchische Strukturen umgewandelt werden. Dabei sind allgemeine Rahmenbedingungen zu beachten, welche unabhängig von spezifischen Transfersyntaxen sind. Die allgemeinen hierarchischen Nachrichtenbeschreibungen sind daher in einer abstrakten Notation abzufassen. Sie dienen als Basis der Konformitätsprüfung von syntaxspezifischen Implementierungen.

7) Implementierbare Nachrichtenspezifikationen

Bei der Entwicklung der implementierbaren Nachrichtenspezifikationen werden, von den Allgemeinen hierarchischen Nachrichtenbeschreibungen ausgehend, die

konkreten Implementierungsvorschriften der Nachrichten für eine bestimmte Transfersyntax festgelegt.

Details und Beispiele zum Vorgehensmodell: vgl. Anhang II.b.

Um eine einheitliche Verwendung der Nachrichten im Österreichischen Gesundheitswesen zu erreichen, ist die Dokumentation obiger 7 Arbeitsschritte in elektronischer Form dem für Gesundheit zuständigen Ministerium zwecks Veröffentlichung zur Verfügung zu stellen. Diese Veröffentlichung sollte über das Internet erfolgen, wobei der Zugriff durch einen Passwortschutz nur auf MAGDA-LENA-Teilnehmer einzuschränken ist.

- 2.4) Die implementierbare Nachrichtenspezifikation hat auf Basis einer international normierten Transfersyntax (vorzugsweise XML, UN/EDIFACT; gegebenenfalls HL7, SGML) zu erfolgen.

Sollen Bilder beim Empfänger weiterverarbeitet werden (z.B. für Therapieplanung, chirurgische Navigation), sind sie gemäß DICOM 3.0 zu übertragen.

- 2.5) Kommen in Nachrichten kodierte Daten zum Einsatz, so sind möglichst bestehende internationale oder nationale Codeverzeichnisse zu verwenden. Sind die verwendeten Codeverzeichnisse noch nicht beim für Gesundheit zuständigen Ministerium registriert, so sind sie dort zur Registrierung einzureichen. Durch diese Registrierung soll die eindeutige Klärung des jeweils verwendeten Codesystems (inklusive allfälliger Versionen) ermöglicht werden. Sie soll in Anlehnung an ISO / IEC 7826 erfolgen, wodurch bei der Registrierung u.a. die für die Code-Wartung zuständige Stelle festgelegt wird³.

Ein Teilnehmer / Provider hat zu erklären, dass er eventuell bereits im Einsatz stehende Codeverzeichnisse, welche noch nicht diesen Spezifikationen entsprechen, bis 30. Juni 2002 auf solche, die diese Spezifikationen erfüllen, umstellen wird. Ein Überschreiten dieser Frist bedarf der begründeten Mitteilung an das BMSG.

FÜR DETAILS SIEHE ANHÄNGE:

II.a - Verzeichnis der Standards

II.b - Vorgehensmodell zur Nachrichtenentwicklung

³ Allfällige Rechte auf die Codesysteme sind dadurch nicht beschnitten.

3. Identifikationsvariable

Im Zuge einer sicheren Datenübertragung im Gesundheitswesen ist sicherzustellen, dass alle an einer diesbezüglichen Kommunikation teilnehmenden Personen und Organisationen bzw. alle zu übermittelnden Daten eindeutig und damit absolut unmißverständlich identifizierbar sind. Damit soll absichtlicher Missbrauch (z.B. unautorisierter Absender) wie auch unabsichtlicher Missbrauch (z.B. Verwechslung von Patienten) unterbunden werden.

Mit dieser Thematik beschäftigt sich das vorliegende Kapitel "Identifikationsvariable (ID)". Im ersten Teil geht es um die ID von Kommunikationsteilnehmern, die in registrierten Directories aufliegen müssen. Weiters geht es um die Authentifizierung von Teilnehmern, deren Kompetenzen und um die ID der zu übermittelnden Dokumente. Im zweiten Teil wird die Patienten-ID behandelt, die bei einem Datenaustausch zur eindeutigen Identifizierung beitragen soll, unter Umständen aber im bilateralen Datenaustausch wegfallen kann.

In beiden Teilen wird auf den derzeitigen Status zurückgegriffen. Aus diesem Grund beschäftigt sich der Anhang mit Kritik und möglichen Alternativen dazu.

XXXXXXXXXXXXXXXXXXXXX

3.1. MAGDA-LENA Kommunikationsteilnehmer-ID

3.1.1 Authentifizierung

Die Authentizität jedes Teilnehmers im Gesundheitsdatennetz muss gesichert sein. Dazu muss sich ein Teilnehmer bei einer noch zu bestimmenden Stelle anmelden, worauf er eine Teilnehmerberechtigung für eine bestimmte Zeitspanne erhält. Nach deren Ablauf hat der Teilnehmer um eine Verlängerung anzusuchen bzw. sich im Falle eines Ausscheidens aktiv abzumelden. Durch diesen Prozeß wird in der für die Verwaltung der Teilnehmerdaten zuständigen Stelle laufend die Teilnehmerliste aktualisiert und die Authentizität der Teilnehmer überprüft. Diese Stelle muss auch mit der entsprechenden Einrichtung, wie z.B. Standesvertretung (Ärztchammer, Apothekerkammer usw.), welche die richtige Identifikation der Teilnehmer gewährleisten kann, in Verbindung stehen. Für zahlreiche potentielle Teilnehmer von MAGDA-LENA bzw. Leistungsanbieter sind entsprechende Organisationen zu nominieren, die diese Teilnehmer identifizieren.

3.1.2 Registrierte Directories

Jeder Teilnehmer muss eindeutig identifizierbar sein, indem er innerhalb einer Organisation, der er zugeteilt ist, in einem registrierten Directory eindeutig identifizierbar ist.

Derzeit existieren mehrere solche Verzeichnisse. Die umfassendsten sind:

Ärzte: Vertragspartnernummer des Hauptverbandes, Ärztenummer der Ärzteliste der Ärztekammer

Apotheken: Apothekenbetriebsnummer

Krankenanstalten (ambulant/stationär): Krankenanstaltsnummer, wenn möglich ergänzt durch den 6- bzw.8-stelligen Funktionscode der jeweiligen Abteilung
Versicherungen (Kostenträger): sozial/privat (unklar).

Weiters bestehen noch für weitere Leistungserbringer des Gesundheitswesens Vertragspartnernummern des Hauptverbandes.

Bis zur Einführung eines neuen Identifikationssystems für die Leistungserbringer sind die derzeitigen ID's zu verwenden. Auf eine mögliche Erweiterbarkeit ist zu achten.

Darüber hinaus muss auch jeder Provider im MKK eindeutig identifizierbar sein. Ein entsprechendes Verzeichnis der MAGDA-LENA- Provider ist einzurichten.

Ein systematischer Aufbau einer eindeutigen ID für alle Anbieter ist empfehlenswert.

Um bei den verschiedenen Nummernsystemen eine Eindeutigkeit zu gewährleisten sind die Nummernsysteme analog zu Codesystemen (vgl. §2.5) beim für Gesundheit zuständigen Ministerium zu registrieren: Die Registriernummer ist der Teilnehmer-ID voranzustellen.

Die registrierten Directories stehen allen Teilnehmern zur Verfügung. Über die Qualität des jeweiligen Nummernformats und die Wartung der Directories findet man mehr im Anhang (9.1. und 9.2.).

3.1.3 Rollen der Teilnehmer

Neben der Authentizität der Teilnehmer muss auch ihre Rolle im Gesundheitsdatennetz definiert sein. Der Absender ist verantwortlich dafür, dass er seine Dokumente nur an berechtigte Teilnehmer adressiert. Daraus ergibt sich auch, dass der Absender den Typ des zu übermittelnden Dokuments festlegen muss.

Die Rolle des Teilnehmers ist vom für Gesundheit zuständigen Bundesministerium festzulegen.

3.1.4 ID der Dokumente

Die verschickten Daten (Befunde etc.) müssen durch eine eindeutige Dokumenten-ID eindeutig identifizierbar sein.

Eine Empfehlung ist, einen mit dem Dokument zu verschlüsselnden Header zu verwenden. Dieser enthält zumindest die ID des Absenders, Zeitstempel, Aufenthaltsnummer und soll durch zusätzliche Merkmale ergänzt werden, so dass eine eindeutige Dokumentidentifikation ermöglicht wird.

3.2 Patienten-ID

3.2.1 Patienten-ID bei allgemeinem Datenaustausch

Bei der Übermittlung von Patientendaten muss immer eine eindeutige Patienten-ID mitgeschickt werden. Daneben werden weiterhin die herkömmlichen Patientendaten (Geburtsname, Familienname, Vorname, Geschlecht, Geburtsdatum, Nationalität) angegeben, können aber gegebenenfalls auch wegfallen (gemäß CEN ENV 12018). Derzeit kommt für die Patienten-ID nur die Österreichische Sozialversicherungsnummer (SV-Nr) in Frage. Über mögliche und vielleicht auch notwendige Alternativen gibt der Anhang Auskunft (siehe 9.3.). Da die Einführung der Chipkarte im Gesundheitswesen die Änderung des jetzigen Status mit sich bringen könnte, sollte auf jeden Fall in allen Computersystemen die Aufwärtskompatibilität der Patienten-ID gewährleistet sein (Vorschlag: 32 Stellen in Anlehnung an den im Anhang angeführten ASTM Standard).

Bis zur Einführung einer neuen Patienten-ID ist die Sozialversicherungsnummer zu verwenden.

3.2.2 Patienten-ID bei bilateralem Datenaustausch

Bei einem rein bilateralen Datenaustausch (z.B.: Arzt – Labor – Arzt) werden die Daten – wenn möglich – in anonymisierter Form übermittelt. In diesem Fall wird statt der Patienten-ID ein intern eindeutiges Identifizierungsverfahren verwendet.

FÜR DETAILS SIEHE ANHANG:

III.a - Identifikationsvariable

4. Datenschutz und Datensicherheit

Für jede Verwendung von Daten und insbesondere für sensible Daten „ . . . ist sicherzustellen, dass die Daten vor zufälligen oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind „ § 14 Abs. 1 DSG 2000.

Zur Erfüllung dieser Forderungen ist eine einheitliche Sicherheitspolitik (Policy) notwendig, die sowohl organisatorische als auch technische Maßnahmen enthält. MAGDA-LENA befasst sich insbesondere mit der Sicherheitspolitik für den Bereich der Datenübertragung zwischen den Teilnehmern und setzt voraus, dass die Teilnehmer in ihrem eigenen Bereich ebenfalls eine Sicherheitspolitik betreiben, die die Erfüllung des Datenschutzes und der Datensicherheit gewährleistet. Empfehlungen und Beispiele für eine Sicherheitspolitik finden sich im Anhang IV.b. In der Konformitätserklärung ist die Einhaltung der Sicherheitsstandards zu garantieren. Eine ausführliche Beschreibung der wesentlichen Fragen und Elemente einer Sicherheitspolitik wird im Anhang IV.c gegeben.

Anhang IV.y in Teil 4 enthält eine Auswahl relevanter rechtlicher Bestimmungen.

XXXXXXXXXXXXXXXXXXXX

4.1 MAGDA-LENA II Sicherheitspolitik

Die im folgenden beschriebenen Elemente der Sicherheitspolitik gelten einerseits für die Teilnehmer des Gesamtsystems, die miteinander Daten austauschen, als auch für die „Binnenstruktur“ der einzelnen Teilnehmer. Das Wort Benutzer bezeichnet bezüglich des Gesamtsystems einen Teilnehmer, bezüglich der teilnehmenden Systeme jeweils einen Endbenutzer, also eine Person, die Daten für die Erfüllung ihrer Aufgaben benötigt.

Wenn sich Teilnehmer des Systems eines MAGDA-LENA-Providers bedienen, dann ist dieser Provider für die Elemente der Sicherheitspolitik und die Sicherheit der Übertragung, die er als Provider zur Verfügung stellt, mitverantwortlich.

Durch die Risikoanalyse der möglichen Bedrohungen durch berechnigte oder nicht berechnigte Nutzer des Systems ergeben sich Mindestanforderungen für Datenschutz und Datensicherheit, welche im Gesundheitswesen verbindlich eingehalten werden müssen. Diese minimalen Rahmenbedingungen können sowohl technisch, organisatorisch oder als gemischte Lösung umgesetzt werden.

4.2 Rahmenbedingungen

Voraussetzung für den Erfolg dieser Sicherheitspolitik ist, dass sie nicht nur von einem, sondern von allen betroffenen Netzwerken erfüllt werden kann. Eine Übermittlung von sensiblen Daten kann so gemäß dem österreichischen Datenschutzgesetz und Richtlinien zur Datensicherheit erfolgen.

Benutzerkontrolle (Authentifizierung)

Die Benutzerkontrolle muss sicherstellen, dass nur authentifizierte Benutzer elektronischen Zugriff auf Daten im System erhalten. Jeder Zugriff, ob berechtigt oder nicht berechtigt, ist zu protokollieren. In Hinblick auf versuchte oder vermutete Verletzungen des Datenschutzes ist das Protokoll in regelmäßigen Zeitintervallen oder auf Anforderung auszuwerten und es sind unberechtigte Zugriffe mit geeigneten Gegenmaßnahmen zu unterbinden. Die Authentifikation muss dem jeweiligen Stand der Technik entsprechen. Bei hohem Schutzbedarf ist eine zusätzliche, mindestens nach Ablauf eines in der Policy vorgegebenen Zeitintervalls durchzuführende Authentifikation gegenüber dem Kommunikationspartner erforderlich.

Zugriffskontrolle (Autorisierung)

Auch authentifizierte Benutzer eines Systems dürfen elektronisch nur auf solche sensiblen Daten zugreifen bzw. Zugriffsrechte erhalten, welche für die berufliche Tätigkeit bzw. für die Behandlung einer Person notwendig sind. Die Begründung, welche sich implizit aus dem Kontext ergeben kann (z.B. Patient in Behandlung), ist nachweislich elektronisch zu dokumentieren. (Beispiel: ein authentifizierter niedergelassener Arzt, fordert von einem Krankenhaus die Krankengeschichte für einen Patienten x an, mit der Begründung, dass x bei ihm in Behandlung sei. Das Krankenhaus kann darauf vertrauen, dass der Arzt nicht unrechtmäßig für einen Dritten Daten anfordert; es muss aber Verbote des Patienten beachten und darf nicht irrelevante Daten, wie z.B. Relig.-Bekenntnis, Abrechnungsdaten, übermitteln.) Sind sensible Daten für die Behandlung eines Patienten unbedingt notwendig, kann auch der nicht im System autorisierte Arzt im Rahmen der technischen und gesetzlichen Möglichkeiten auf diese Daten zugreifen. Das heißt, ein Arzt, der authentifiziert (dem System bekannt) ist, aber normalerweise auf die Daten nicht zugreifen dürfte (nicht autorisiert ist) – z.B. weil er nach der Datenlage im System noch nicht behandelnder Arzt ist (unerwarteter Notfall). Diese Zugriffe sind gesondert zu protokollieren und vom System zu verifizieren (ob z.B. der Patient nach dem Zugriff als Patient an dieser Stelle behandelt wurde) und die sicherheitsrelevanten Informationen einer Kontrollinstanz (z.B. dem Leiter der Organisationseinheit) zu übermitteln. Alle Protokolle sind periodisch oder im Anlassfall zu überprüfen, Zugriffsverletzungen und versuchte Zugriffe auf sensible Daten sind mit geeigneten Mitteln zu unterbinden.

Die hier festgelegten Bestimmungen der Zugriffskontrolle treffen nur auf die mit der Übertragung von MAGDA-LENA relevanten Daten verbundenen Zugriffe auf Daten zu. Die lokale und interne Organisation der Kommunikationspartner wird durch MAGDA-LENA II nicht angesprochen.

Übermittlungskontrolle

Jede elektronische Übermittlung von sensiblen Daten ist vertraulich mittels hinreichend starker Verschlüsselung (gemäß Anhang IV.a) durchzuführen. Die Verschlüsselung hat End to End zu geschehen, ein Offenlegen des Klartextes auf der Übertragung etwa zum Zwecke der Umschlüsselung ist nicht vorzusehen. Weiters ist die Datenintegrität sowie der Datenursprung der übermittelten Informationen bzw. die Identität des Senders durch anerkannte und geeignete Methoden (z.B. elektronische Signatur) sicherzustellen. Jede elektronische Übermittlung von sensiblen Daten ist durch eine Rückmeldung des Kommunikationspartners zu bestätigen. Bei der

Anwendung elektronischer Signaturen sind die gesetzlichen Bestimmungen des Signaturgesetzes und der Verordnung zu beachten.

Die im Planungsstadium befindliche Sozialversicherungskartensystem ist als Schlüsselkarte geplant und diese Technologie kann die Anforderungen an die Übermittlungskontrolle im Bereich der elektronischen Signatur und gegebenenfalls auch der Verschlüsselung erfüllen.

Organisationskontrolle

Die regelmäßige Kontrolle der Organisationsstrukturen ist eine wichtige Voraussetzung, um die gesetzlichen Rahmenbedingungen zum Schutz der betroffenen Personen und Dienstleister einhalten zu können. Schwachstellen im System können damit identifiziert und innerhalb festgelegter Zeiträume beseitigt werden. In der Sicherheitspolitik sind sowohl die Zeitintervalle für eine regelmäßige Überprüfung als auch die Maßnahmen, welche bei einer Verletzung der Sicherheitspolitik zu ergreifen sind, festzulegen. Mangelnde Organisation und Qualität stellen ein Sicherheitsrisiko für jedes System dar.

Vertrauenswürdige Betriebsumgebung

Die vertrauenswürdige Betriebsumgebung muss den Schutz im Betrieb des gesamten Netzes gewährleisten. Dabei sind auch alle Aspekte der übrigen Kommunikation (z.B. Internetanbindung) mit einzubeziehen.

Der Provider von Kommunikationselementen und Kommunikationsdiensten ist dafür verantwortlich, dass unter Einhaltung der von Ihm erteilten und schriftlich aufliegenden Belehrung eine Verletzung des Datenschutzes nicht erfolgen kann.

Tritt eine Organisationseinheit selbst und ohne einen Provider in Anspruch zu nehmen auf, dann trägt sie auch diese Verantwortung des vertrauenswürdigen Betriebes. Auch in diesem Fall muss die Betriebspolicy, die der Belehrung des Providers gleichkommt offengelegt sein.

Ein Netzwerkbetreiber ist zudem für die Verfügbarkeit des Netzes und für die Zustellungsnachweise verantwortlich. Jedenfalls liegt es in der Verantwortung des Providers einer MAGDA-LENA konformen Lösung, dass eine solche mit anderen MAGDA-LENA konformen Lösungen auf der Kommunikationsebene verträglich ist.

FÜR DETAILS SIEHE ANHÄNGE

IV.a: Anforderung an Verfahren und Mechanismen (normativ)

IV.b: Sicherheitsmaßnahmen und Sicherheitsempfehlungen (normativ gemäß Konformitätserklärung)

5. Netzbetreiber, Netzübergänge

Kapitel 5 beinhaltet die Themen Netzbetreiber (Kapitel 5.1) und Netzübergänge (Kapitel 5.2). Beide Kapitel definieren Richtlinien, die Netzbetreiber hinsichtlich ihrer Teilnahme am Österreichischen Gesundheitsdatennetzwerk zu erfüllen haben.

Diese Richtlinie definieren Mindeststandards, ihre verbindliche Einhaltung fußt auf der Forderung nach gesicherter Datenübertragung im Gesundheitswesen und stellt die Grundvoraussetzung für eine MAGDA-LENA-konforme Kommunikation dar.

Kapitel 5.1 enthält jene Richtlinien, die jeder einzelne Netzbetreiber in organisatorischer sowie in sicherheitstechnischer Hinsicht zu erfüllen hat. Darüber hinaus definieren diese Richtlinien auch das reibungslose Zusammenwirken zwischen Netzbetreiber und anderen Netzbetreibern bzw. zwischen Netzbetreiber und Clients.

Kapitel 5.2 definiert die Richtlinien, die für Netzübergänge und Schnittstellen⁴ gelten.

In den Anmerkungen im Anhang werden sicherheitsrelevante Aspekte unter Bezugnahme auf die beiden oben genannten Kapitel näher beleuchtet und an Fallbeispielen abgehandelt.

Netzbetreibern bleibt es unbenommen, die geforderten Sicherheitsstandards nach oben hin auszuweiten.

XXXXXXXXXXXXXXXXXXXXXXX

5.1 Netzbetreiber

Netzbetreiber⁵, die MAGDA-LENA-Konformität anstreben, haben im Rahmen eines gesamtösterreichischen Gesundheitsdatennetzes primär folgende Aufgaben wahrzunehmen:

- Annahme medizinischer Daten von Clients in elektronischer bereits verschlüsselter Form
- Zwischenspeicherung elektronischer Daten im Falle der Nichtannahme von Daten
- Automatisierte Datenweiterleitung (in Zusammenarbeit mit anderen Netzbetreibern) bis hin zum Endprovider
- Datenweitergabe an den Endkunden
- Protokollierung der versandten und in Empfang genommenen Daten
- Archivierung von Protokollen für eine bestimmte Zeit
- Um Informationsverlusten bzw. Informationsverfälschungen vorzubeugen, dürfen Netzbetreiber keine Neu- bzw. Umverschlüsselung von Daten auf dem Weg von einem Netzbetreiber zum anderen vornehmen.⁶

⁴ Vgl. hierzu Punkt 5.2 (MAGDA-LENA Version 1.0)

⁵ Zur Unterscheidung zwischen Netzbetreiber und Provider siehe Glossar

⁶ Vgl. hierzu Punkt 5.2 (MAGDA-LENA Version 1.0)

Vor dem Hintergrund gesetzlicher Datenschutzbestimmungen und des Transports äußerst sensibler Daten hat das Handling von elektronischen Daten auf der Basis von vorgeschriebenen Sicherheitsrichtlinien, Zeitvorgaben und strukturellen Abläufen zu erfolgen.

Der elektronische Datenaustausch hat lückenlos über alle daran beteiligten Rechner und Anwendungen stattzufinden. Durch die Verbindung sämtlicher Rechnersysteme (Client – Netzbetreiber, Netzbetreiber – Netzbetreiber, Netzbetreiber – Client) muss gewährleistet sein, dass es zu keinen Medieneinbrüchen und zu keinen Datenverlusten kommt.

Die hier vorgegebenen Richtlinien haben von den Netzbetreibern als Mindestauflagen im Hinblick auf die MAGDA-LENA Konformität erfüllt zu werden.

Die Richtlinien gelten für jeden einzelnen Netzbetreiber (vgl. hierzu Kapitel 5.1.1).

Darüber hinaus wird auch der Umstand berücksichtigt, dass die Realisierung des gesamtösterreichischen Datennetzwerks auf der Teilnahme und der Zusammenarbeit mehrerer Netzbetreiber aufzubauen hat⁷. Über die Vorgabe von Richtlinien ist daher auch sicherzustellen, dass das Datenhandling zwischen Netzwerkbetreibern jeweils auf den gleichen Sicherheitsrichtlinien aufbaut, und eine durchgehende Interoperabilität zwischen Netzbetreibern gegeben ist (vgl. hierzu Kapitel 5.1.2).

Die Klassifizierung der Aufgaben von Netzbetreibern muss auch vor dem Hintergrund der Zusammenarbeit mit Client-Rechnern erfolgen. Client-Rechner müssen zwar nur kurzfristig in das Providernetz für die Dauer der Datenübermittlung und –übernahme einbezogen werden, dennoch wird z.B. vor dem Hintergrund des Themas "Empfangsbestätigung" deutlich, dass Netzbetreiber bis zur Datenübergabe an den Empfänger auch den Absender als Teil der Übertragungskette ansehen müssen (vgl. hierzu Kapitel 5.1.3).

Netzbetreiber haben sicher[zu]stellen, [...] dass der ursprüngliche Dateninhalt (z.B. Umlaute) erhalten bleibt, d.h. [es darf] kein Informationsverlust bzw. keine Informationsverfälschung und kein Informationsverlust ein[treten]. [...] Diese Forderungen gelten sinngemäß auch für Anbindungen an internationale Gesundheitsnetze - unter strikter Beachtung der aktuellen nationalen und internationalen Gesetzeslage (Datenschutz, u.a.).

⁷ Vgl. hierzu Punkt 5.1 (MAGDA-LENA Version 1.0)

5.1.1 Richtlinien für den einzelnen Netzbetreiber

Bauliche Maßnahmen

Um als MAGDA-LENA-konformer Netzbetreiber zu gelten, hat dieser ein Mindestmaß an baulichen Maßnahmen im Hinblick auf den ungestörten Rechnerbetrieb und Erweiterbarkeit des Rechnerparks Genüge zu leisten.

Technische Ausstattung und Betriebssicherheit

Hardware

- Netzbetreiber haben grundsätzlich dafür zu sorgen, dass der Ausfall eines am Datenhandling beteiligten Servers oder einer Hardwarekomponente unter keinen Umständen zu Datenverlust führt.
- Alle am Datenhandling beteiligten Server müssen dem Stand der Technik (derzeit RAID Level 5) entsprechen.

Software

- Netzbetreiber haben softwareseitig für größtmögliche Sicherheit in bezug auf das Datenhandling zu sorgen.
- Der Netzbetreiber verpflichtet sich zu einer vollständigen Abschirmung des Datenhandlings gegenüber den Geschäftsprozessen von anderen Kunden.⁸

Administrative Sicherheit während des laufenden Betriebs

- Jeder Netzbetreiber hat eine Sicherheitspolicy vorzulegen, die vor allem auch die Mitarbeiterschwiegenheit beinhaltet.
- Netzbetreiber müssen dem Kunden die Zugangsverfügbarkeit vertraglich bestätigen.

Architektur des Netzbetreibers

- Jeder Netzbetreiber muss seinem Kunden die Architektur seines Netzes (vgl. z.B. Stern-, Ringtypologien) offen legen.
- Netzbetreiber müssen über aktives Bandbreitenmanagement verfügen (vgl. hierzu die nach oben hin erweiterbaren Bandbreiten von POPs).
- Ausreichende Übertragungskapazitäten müssen hierüber gesichert sein.

Vertragliche Regelungen

Vertrag zwischen Netzbetreiber und Kunden

- Die Übereinkunft hinsichtlich der Nutzung der Dienste eines Netzbetreibers durch den Kunden ist in jedem Fall vertraglich zu regeln, wobei insbesondere auf §11 DSGVO 2000 zu verweisen ist. Wie in MAGDA-LENA 1.0 (Punkt 5.5) bereits angeführt, sind Richtlinien wie

⁸ Vgl. hierzu Punkt 5.4 (MAGDA-LENA Version 1.0)

- Verfügbarkeit
- Security
- HotLine / Help Desk
- Reaktionszeiten
- Wartung
- Accountingfunktionen zu Verrechnungszwecken
- Gebühren, etc.

vertraglich festzulegen.

Besonderes Augenmerk hat den Rechten und Pflichten der jeweiligen Vertragspartner zu gelten. Im Vertrag müssen auch die Kündigungsbedingungen/ -möglichkeiten enthalten sein.

Dem Netzbetreiber muss es möglich sein, die Zusammenarbeit mit Kunden dann aufzukündigen, wenn diese die Sorgfaltspflicht (vgl. hierzu den sorgsamsten Umgang mit Passwörtern) und die Sicherheitsrichtlinien trotz Verwarnung missachten.

Pflichtenheft

Das Pflichtenheft hat die Grundlage für den Vertragsabschluss zwischen Kunden und Netzbetreiber zu sein. Oben genannte Punkte (vgl. hierzu bauliche Maßnahmen oder technische Ausstattung und Betriebssicherheit) müssen darin im Detail beschrieben sein. Netzbetreiberspezifische Besonderheiten sind eigens anzuführen.

Regelung der vorzeitigen Vertragsbeendigung

Verträge zwischen Kunden und Netzbetreibern sind zeitlich zu befristen. Eine Vertragsverlängerung ist daran zu binden, dass ein Netzbetreiber die in MAGDA-LENA vorgegebenen Richtlinien erfüllt.

- Im Falle einer Übernahme des Netzbetreibers durch eine Fremdfirma gilt der Vertrag mit dem Kunden als beendet, sofern der neue Netzbetreiber nicht MAGDA-LENA konform arbeitet und die Pflichten und Rechte des bisherigen Vertragspartners nicht vollständig übernimmt.
- Eine Fortsetzung der Dienstleistung ergibt sich aus dem Umstand, dass die neu entstandene juristische Person die in MAGDA-LENA vorgegebenen Richtlinien erfüllt
- Im Falle der Nichtfortführung des Geschäftes, wie sie z.B. bei Konkurs, Ausgleich oder freiwilliger Niederlegung der Geschäftstätigkeiten vorliegt, ist der Netzbetreiber verpflichtet, den gesamten Datenbestand inklusive Backups in maschinenlesbarer Form umgehend an den Vertragspartner/ die Vertragspartner herauszugeben und anschließend rückstandslos von seinen Rechnern zu löschen.

5.1.2 Richtlinien hinsichtlich der Interoperabilität

Protokollierung

- Übertragungs-Vorgänge müssen vom Netzbetreiber mit Zeitmarken versehen und protokolliert werden.
- Erhält ein Netzbetreiber von einem anderen Netzbetreiber Daten, so muss er ihren Empfang mit einer Zeitmarke bestätigen.
- Der Absender (Client) hat von seinem Netzbetreiber eine positive Übernahmebestätigung seiner Daten zu erhalten, wenn seine Daten zur Weiterleitung an einen Endkunden erfolgreich übernommen worden sind. Für den Fall, dass die Daten vom Netzbetreiber nicht korrekt übernommen worden sind, muss der Absender von seinem Netzbetreiber eine Nachricht erhalten, dass die Datenübernahme nicht geglückt ist. Es darf nicht implizit davon ausgegangen werden, dass bei Nachvorliegen der ursprünglich zu versenden gedachten Daten im Ausgangspostfach des Absenders keine korrekte Datenübergabe an den Netzbetreiber stattgefunden hat.
- Liegen die Daten beim letzten Netzbetreiber auf, so hat dieser, sofern er nicht selber die Daten aktiv in das Postfach des Empfängers zustellt, diesen vom Vorhandensein abholbereiter Daten zu benachrichtigen. Wurden die Daten vom Empfänger erfolgreich in Empfang genommen (dies gilt für die aktive Zustellung durch den Netzbetreiber als auch für die Möglichkeit der Abholung der Daten durch den Clienten), so muss der Adressat vom Empfänger eine positive Nachricht über den Erhalt der Daten bekommen.
- Die Nachrichtenverfolgung bzw. das Befundtracking hat auf der Basis positiver wie negativer Empfangsbestätigungen zu erfolgen.⁹
- In jedem Fall müssen Netzbetreiber eine durchgehende Statusverfolgung ermöglichen.
- Netzbetreiber haben die Pflicht, Protokolle über einen bestimmten Zeitraum zu archivieren. Die Archivierungsdauer der Protokolle hat sich hierbei nach den jeweils für den Absender bzw. für den Empfänger geltenden Gesetzen (vgl. hierzu Aufbewahrungspflicht von Dokumenten für Ärzte, Krankenanstalten, etc.) zu richten.

Empfangsbestätigungen

- Datenübergaben/ -nahmen zwischen einem Clienten und einem Netzbetreiber oder zwischen zwei Netzbetreibern müssen protokolliert werden. Zusätzlich erhält der Absender (= Client oder Netzbetreiber) vom Empfänger (= Client oder Netzbetreiber) eine positive oder negative Empfangsbestätigung.
- Über eine geeignete Empfangsbestätigung muss ermittelt werden, ob das Datenpaket in seiner vollen Länge zum Netzbetreiber bzw. zum Adressaten übermittelt worden ist.
- Da es teilweise übermittelte Daten nicht geben darf, hat ein Netzbetreiber allfällige Dateireste von seinem Server zu eliminieren.
- Wurden die Daten vom empfangenden Client erfolgreich übernommen, muss der letzte Netzbetreiber den Absender auf elektronischem Weg hierüber in Kenntnis setzen.

⁹ Vgl. hierzu Punkt 5.3 (MAGDA-LENA Version 1.0)

Datenverlauf und Protokollierung

- Datenverläufe müssen von den einzelnen Netzbetreibern protokolliert und in Form eines elektronischen Stempels dem Dokument mitgegeben werden. Es muss ersichtlich sein, welche Stationen das Dokument zu welchem Zeitpunkt bis zum Eintreffen auf dem Empfängerrechner genommen hat.
- Diese Verlaufskontrolle (Nachrichtenverfolgung)¹⁰ muss auch dann gegeben sein, wenn Daten nicht den Weg über eine authentifizierten Routerstrecke, sondern über das Internet nehmen.

Anbindung an internationale Gesundheitsnetze

- Netzbetreiber müssen die Anbindung an internationale Gesundheitsnetze ermöglichen, so fern diese Netze MAGDA-LENA-konform sind.

Kommunikationsstandards

- Netzbetreiber müssen gängige technische Kommunikationsstandards unterstützen.
- Von Netzbetreibern wird verlangt, dass sie auch zukünftige Kommunikationsstandards unterstützen.

Datenaustausch über das Internet

- Der Datenaustausch kann über das Internet erfolgen. Der Datenaustausch gilt unter Berücksichtigung der bei Einhaltung der in MAGDA-LENA festgelegten Rahmenbedingungen in Abschnitt 4 beschriebenen Verschlüsselungsverfahren und Sicherheitstechnologien als sichere Methode. Weiters sind die in Kapitel 5 vorher angeführten Aufgaben für Netzbetreiber, insbesondere die Protokollierung der in Empfang genommenen und versandten Nachrichten und die Archivierung der Protokolle, wahrzunehmen. Der MAGDA-LENA Provider hat auch für die Erstellung und Übermittlung der entsprechenden Empfangsbestätigungen zu sorgen.
- Das Datenhandling setzt die Unterstützung von Internet-Standard-Protokollen durch die Netzbetreiber voraus. Bei anderen eingesetzten Protokollen darf es sich nicht um proprietäre Protokolle handeln.

¹⁰ Vgl. hierzu Punkt 5.3 (MAGDA-LENA Version 1.0)

5.1.3 Richtlinien hinsichtlich des Datenaustauschs zwischen Netzbetreiber und Client

Zulassungsberechtigung

- Damit ein Client medizinische Daten verschicken oder empfangen kann, muss er sich zunächst gegenüber seinem Netzanbieter als zulassungsberechtigt ausweisen.

Datenabholung durch Empfänger

- Dem letzten Netzbetreiber obliegt es, den Empfänger elektronisch zu benachrichtigen, dass für ihn Daten abholbereit vorliegen.¹¹
- Daten haben solange auf dem letzten Server gespeichert zu sein, bis der Empfänger sie von dort abholt und bei sich gespeichert hat.
- Hat der Empfänger die Daten erfolgreich abgeholt und bei sich gespeichert, so muss an den Absender vom Empfänger aus eine elektronische Nachricht erfolgen und den positiven Erhalt der Daten bestätigen.

Datenverschlüsselungsaufgaben

- Grundsätzlich gelten hier die im Anhang IV.a im Hinblick auf die Datenübertragung formulierten Richtlinien.

5.2. Netzübergänge

5.2.1 Netzübergänge zwischen Netzbetreibern

- MAGDA-LENA konforme Netzübergänge beschreiben Übergänge vom Netz eines Netzbetreibers auf ein anderes Netz eines anderen Netzbetreibers.
- Derartige Netzübergänge müssen über Router verwaltet werden, die Internet-Standard-Protokolle unterstützen.
- Netzübergänge haben auf hohe Bandbreiten, Nutzungsspitzen und auf extrem hohe Ausfallsicherheit ausgelegt zu sein. Ihre Verfügbarkeit muss auch bei dauerhaftem Hochlastbetrieb gewährleistet sein.
- Die Netzwerk-Architektur aller Netzbetreiber muss dahingehend ausgelegt sein, dass die Zahl der Netzwerkübergänge, welche die Daten bis zum Zielpunkt überwinden müssen, auf ein Minimum reduziert wird. Dadurch muss ein schneller und direkter Datenaustausch zwischen Absender und Empfänger ohne Überlastungs- und Zuverlässigkeitsproblemen möglich sein.

5.2.2 Netzübergänge zwischen Client und Netzbetreiber

- MAGDA-LENA-konforme Netzübergänge haben auch den Übergang des Clienten zum Netzbetreiber zu beschreiben. Für die Dauer der Datenübertragung hat der Client-Rechner in das Netz des Netzbetreibers dynamisch eingebunden zu sein.

¹¹ Dies Modell basiert auf der Holschuld des Arztsystems. In den Anmerkungen (Anhang V.a) wird alternativ auch das Modell vorgestellt, das von der Bringschuld des Netzbetreibers ausgeht.

- Zwischen Client und Server ist der Einwahlknoten des Netzbetreibers als Netzübergang definiert. Hierüber nimmt der Client mit dem Server Kontakt auf.
- Der Netzbetreiber hat sicherzustellen, dass dieser Netzübergang über eine genügend hohe Bandbreite verfügt, um den gleichzeitigen Zugriff von mehreren Clients auf den Server zu ermöglichen. Gegebenenfalls muss der Netzbetreiber für eine nach oben hin erweiterbare Bandbreite sorgen.

5.2.3 Netzwerkschnittstellen

Daten, die Schnittstellen passieren, dürfen inhaltlich in keiner Form verändert werden.

Schnittstelle Software-Ver- und -entschlüsselung

- Eine Schnittstelle bei der Datenübertragung stellt die Software dar.
- Die Verschlüsselung hat auf dem System des Absenders zu erfolgen. Erst nach abgeschlossener Verschlüsselung dürfen Daten an einen Empfänger weitergegeben werden.
- Die Entschlüsselung darf nur auf dem System des Empfängers erfolgen.

Hardware-Schnittstellen

- Über die Spezifikation von Hardware-Schnittstellen hat sichergestellt zu sein, dass Komponenten verschiedener Hersteller miteinander kombiniert werden können (vgl. hierzu Routerkonfigurationen).
- Netzbetreiber haben nur jene Hardwarekomponenten einzusetzen, deren Schnittstellen von den Herstellern offengelegt sind.¹²

FÜR DETAILS SIEHE ANHANG: V.a

¹² Vgl. hierzu Punkt 5.2 (MAGDA-LENA Version 1.0)

6. Konformität

Zusammenfassung:

In diesem Kapitel werden die Maßnahmen beschrieben, welche die Einhaltung der MAGDA-LENA – Richtlinien durch alle Teilnehmer bzw. Provider sicherstellen sollen.

Dazu werden aus den Inhalten der vorigen Kapiteln die wesentlichsten Punkte hier zusammengefaßt. Im Sinne eines funktionsfähigen Gesamtsystems ist die Einhaltung der jeweils zutreffenden MAGDA-LENA-Rahmenbedingungen von den jeweils Betroffenen zu erklären und offenzulegen.

XXXXXXXXXXXXXXXXXXXX

- 6.1. Die Einhaltung der jeweils zutreffenden MAGDA-LENA-Rahmenbedingungen ist von den jeweils Betroffenen zu erklären.

Dies hat in Form unten angeführter Konformitätserklärungen, welche gegenüber dem für Gesundheit zuständigen Ministerium abzugeben sind, zu erfolgen.

- 6.2. Es wird vorgeschlagen, dass diese Erklärungen mit Hilfe eines Web-Formulars im Internet erfolgen. Bis zur allgemeinen Verfügbarkeit elektronischer Signaturen ist das Formular auch ausgedruckt und firmenmäßig unterfertigt an das für Gesundheit zuständige Ministerium, Abteilung für Telematik im Gesundheitswesen, zu übermitteln.

Genauso wie ein Teilnehmer die Erfüllung von Aufgaben – inklusive deren Überprüfung gemäß § 6.3 b) – an einen MAGDA-LENA-konformen Provider (vgl. Kapitel 1) übertragen kann, so kann auch die Durchführung dieser Erklärung an den Provider übertragen werden¹³.

- 6.3 Diese Erklärung hat auch zu enthalten:
- a) Erklärung des Einverständnisses zur Veröffentlichung dieser Angaben
 - b) Erklärung des Einverständnisses zur stichprobenweisen, nicht anlassbezogenen Überprüfung durch eine dritte, unabhängige Instanz und gegebenenfalls die dazu notwendigen Informationen beizustellen.

¹³ So kann beispielsweise die Unterzeichnung der jeweils zutreffenden Konformitätserklärungen im Rahmen des Vertragsabschlusses mit dem MAGDA-LENA Provider erfolgen, die technische Durchführung der Meldung erfolgt dann durch diesen.

- c) Das Einverständnis zur Veröffentlichung allfälliger negativer Resultate dieser Überprüfungen, falls allfällige notwendige Verbesserungen nicht innerhalb einer gesetzten Nachfrist nachweislich durchgeführt wurden.
- d) Eine Verpflichtungserklärung zur selbständigen und sofortigen Meldung bei irgendwelchen Änderungen im Zusammenhang mit der Konformitätserklärung.

6.4 Konformitätserklärungen:

Betroffene	Konformitätserklärung	Verweise
Teilnehmer	K.1) Der Teilnehmer hat die Rechtsgrundlage und den Zweck für die geplante Datenverarbeitung zu erklären. Es gibt weiters die Datenverarbeitungsregister-Nummer (DVR-Nummer) als Auftraggeber nach dem Datenschutzgesetz 2000 und den Inhalt der Meldung an das Datenverarbeitungsregister gemäß §19 Abs. 1 und 2 DSG 2000 bekannt.	Kap. 4
Teilnehmer Provider	K.2) Der Teilnehmer/Provider hat sich zur Einhaltung des Datenschutzes und zur ausschließlichen Verwendung der ihm übermittelten Daten nach Treu und Glauben im Sinne des Zwecks (Behandlung, Abrechnung etc.) zu verpflichten.	Kap. 4
Teilnehmer Provider	K.3) Der Teilnehmer/Provider hat zu erklären, dass er eine interne Sicherheitspolitik entsprechend den in Anhang IV.b definierten Maßnahmen und Empfehlungen implementiert hat. Die wesentlichen Elemente dieser Sicherheitspolitik sind offenzulegen und müssen den Kommunikationspartnern zugänglich sein.	Kap. 4, Anhang IV.b
Teilnehmer Provider	K.4) Der Teilnehmer/Provider hat zu erklären, dass er für die Kommunikation mit anderen Teilnehmern folgende Maßnahmen unter Einhaltung der in Anhang IV.a definierten Anforderungen an Verfahren und Mechanismen implementiert hat (Sofern sich der Teilnehmer für die Kommunikation eines MAGDA-LENA-Providers bedient, muss diese Erklärung nur vom MAGDA-LENA-Provider und nicht von den einzelnen Teilnehmern abgegeben werden.): <ul style="list-style-type: none"> • Authentifikation und Zugriffskontrolle (gemäß Anhang IV.b, 1.1 Sicherheitsmaßnahmen) • Vertraulichkeit (gemäß Anhang IV.b 1.2 Sicherheitsmaßnahmen) • Datenintegrität (gemäß Anhang IV.b 1.3 Sicherheitsmaßnahmen) • Ursprungsnachweis (gemäß Anhang IV.b 1.4 Sicherheitsmaßnahmen) 	Kap. 4

Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz MAGDA-LENA“
Teil 2: Kapitel: Konformität

	<p>In größeren Organisationseinheiten (mehr als 20 Mitarbeiter) und bei MAGDA-LENA-Providern müssen die im Anhang IV.b Sicherheitsmaßnahmen und Sicherheitsempfehlungen genannten Empfehlungen implementiert werden. Darunter sind zu verstehen:</p> <ul style="list-style-type: none"> • Zutrittskontrolle (gemäß Anhang IV.b, 2.1 Sicherheitsempfehlungen) • Audit Trail (gemäß Anhang IV.b, 2.2 Sicherheitsempfehlungen) • Wartung (gemäß Anhang IV.b, 2.3 Sicherheitsempfehlungen) • Verfügbarkeit des Systems (gemäß Anhang IV.b, 2.4 Sicherheitsempfehlungen) • Fernwartung (Anhang IV.d oder äquivalent) <p>Alle Sicherheitsmaßnahmen oder -empfehlungen, welche durch den Einsatz der elektronischen Signatur realisiert werden, unterliegen den Rahmenbedingungen des SigG und der SigVO. Dies gilt auch für die Evaluierung und Bestätigung auf Konformität.</p> <p>Zusätzlich zu den nationalen Gesetzen sind die einschlägigen Vornormen und Normen der Europäischen Union (dzt. verabschiedet durch CEN/ TC 224 und CEN/ TC251) zu beachten. Ein Auszug dieser Normen ist im Anhang IV.e Standardisierung zusammengestellt.</p>	
Teilnehmer	K.5) Jeder Teilnehmer hat zu erklären, dass er die jeweils aktuellen und üblichen Identifier benützt. Weiters hat er die verwendeten Identifikationsvariablen bekannt zu geben.	Kap. 3
Teilnehmer Provider	K.6) Der Provider hat sicherzustellen, dass jeder Teilnehmer die entsprechende Berechtigung aufweist.	Kap.3
Netzbetreiber	K.7) Der Netzbetreiber erklärt sich zur Einhaltung von organisatorischen sowie sicherheitstechnischen Richtlinien bereit. Interne Sicherheitsmaßnahmen werden vom Netzbetreiber gemäß den in Kapitel 5.1.1 definierten Richtlinien und den Kapitel 5.3.1 vorgelegten Empfehlungen (Anhang) aktiv im Betrieb umgesetzt und dem jeweiligen Stand der Technik angepasst. Die wesentlichen Aspekte dieser Sicherheitspolitik sind offen zulegen.	Kap. 5
Netzbetreiber	K.8) Gemäß den in Kapitel 5.1.2 definierten Anforderungen muss die Interoperabilität zwischen Netzbetreibern über alle Ebenen des Datenaustauschs hinweg zu jedem Zeitpunkt gewährleistet sein. Der Datenaustausch betrifft aber auch die Verbindung zwischen Absender und	Kap. 5

Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz MAGDA-LENA“
Teil 2: Kapitel: Konformität

	<p>Netzbetreiber sowie Netzbetreiber und Empfänger. Netzbetreiber erklären sich zur Einhaltung folgender Richtlinien bereit:</p> <ol style="list-style-type: none"> 1) Identifizierung des Absenders und Zugangskontrolle 2) Herstellen einer dynamischen Verbindung zwischen Absender und Netzbetreiber 3) Datenübernahme und Empfangsbestätigung 4) Datenweiterleitung an andere Netzbetreibern 5) Entgegennahme/ Weiterleitung von Empfangsbestätigungen 6) Protokollierung von Übertragungsversuchen (Nachrichtenverfolgung) 7) Archivierung von Protokollen über gesetzlich vorgeschriebene Zeiträume 8) Benachrichtigung des Empfängers über abholbereite Daten bzw. aktive Zustellung von Daten 9) Zwischenlagerung nicht zustellbarer Daten bzw. Löschung von Daten, die vom Netzbetreiber an den Adressaten übermittelt werden konnten 	
Netzbetreiber	K.9) Der Netzbetreiber erklärt sich weiters zur Einhaltung des Datenschutzgesetzes (DSG 2000) bereit. Daten werden ausschließlich zu treuen Händen verwaltet bzw. weitergeleitet.	Kap. 5
Netzbetreiber	K.10) Der Netzbetreiber erklärt, dass er den Datenaustausch zwischen Absender und Empfänger in Zusammenarbeit mit anderen Netzbetreibern derart unterstützt, dass es zu keiner Neuverschlüsselung bzw. Entschlüsselung von Daten kommt.	Kap. 5
Netzbetreiber	K.11) Der Netzbetreiber erklärt, dass er im Hinblick auf die Gewährleistung des MAGDA-LENA-konformen Datenaustauschs jederzeit der Überprüfung durch einen Bevollmächtigten des Vertragspartners zustimmt.	Kap. 5
Teilnehmer	<p>K.12) Der Absender erklärt, dass er Dokumente ausschließlich an berechnigte Personen adressiert.</p> <p>Der Empfänger erklärt, an ihn adressierte Daten (so ferne keine aktive Zustellung vereinbart wurde) umgehend vom Netzbetreiber abzuholen und gemäß den gesetzlichen Vorgaben zu archivieren.</p>	Kap. 5

Rahmenbedingungen für ein logisches österreichisches Gesundheitsdatennetz MAGDA-LENA“
Teil 2: Kapitel: Konformität

Partner des Gesundheitswesens, welche einen Datenaustausch zwecks automatischer Weiterverarbeitung im Empfängersystem durchführen <i>Zu allfälligen Übergangsfristen vgl. unter K.20</i>	K.13) Gemäß Kapitel 2 hat der Teilnehmer zu erklären, dass er vorhandene internationale oder nationale Kommunikationsstandards verwendet. Er hat diese unter präziser Angabe der eingesetzten Version anzugeben. Enthält der Standard noch kein Informationsmodell, so ist dieses wenn möglich zu spezifizieren.	§2.1, §2.2
	K.14) Sind internationale oder nationale Standards nicht verfügbar, so kann eine Nachrichtenentwicklung durchgeführt werden. Es ist zu erklären, dass diese gemäß §2.3 erfolgt ist. Die Dokumentation ist in elektronischer Form dem für Gesundheit zuständigen Ministerium zwecks Veröffentlichung zur Verfügung zu stellen. Diese Veröffentlichung sollte über das Internet erfolgen, wobei der Zugriff durch einen Passwortschutz nur auf die MAGDA-LENA-Teilnehmer einzuschränken ist.	§2.1 – §2.3
	K.15) Der Teilnehmer hat zu erklären, welche Kommunikationsrolle(n) des Informationsmodells (vgl. K.13 bzw. K.14) er einnimmt, und dass er dem dort spezifizierten Verhalten in allen Punkten entspricht.	§2.1. – §2.3
	K.16) Der Teilnehmer hat zu erklären, welche Transfersyntax (inklusive Versionsangaben, verwendete Directories, etc.) zum Einsatz kommt.	§2.4
	K.17) Im Falle der Übermittlung vercodeter Daten hat der Teilnehmer die BMSG-Registriernummern der verwendeten Codesysteme anzugeben.	§2.5
Provider	K.18) Ein Provider hat zu erklären, welche inhaltlichen Kommunikationsstandards er unterstützt.	§2.1 – §2.3
Provider	K.19) Ein Provider hat sich zur Zusammenarbeit mit allen anderen MAGDA-LENA-Providern, auch bei allfällig notwendigen Weiterentwicklungen der Schnittstellen und Kommunikationsstandards, zu verpflichten.	
Teilnehmer / Provider	K.20) Ein Teilnehmer / Provider hat zu erklären, dass er eventuell bereits im Einsatz stehende Nachrichten/Codeverzeichnisse, welche noch nicht den Spezifikationen der aktuellen MAGDA-LENA-Version entsprechen, bis 30. Juni 2002 auf solche, die diese Spezifikationen erfüllen, umstellen wird. Ein Überschreiten dieser Frist bedarf der begründeten Mitteilung an das BMSG.	§2.1 – §2.3; §2.5

7. Anhang IV.a: Anforderung an Verfahren und Mechanismen (normativ)

In diesem Anhang werden jene Teile die sich aufgrund der Technologie wandeln könnten zusammengefasst. Geeignete Technologiebeobachtung ist zum Monitoring der Eignung der Verfahren und Methoden und zur Anpassung an die jeweiligen Veränderungen heranzuziehen.

Es werden insbesondere die folgenden Aspekte geregelt:

1. Inhaltsverschlüsselung – Verfahren und Schlüssellängen

Daten, die den Sicherheitsanforderungen von MAGDA-LENA genügen müssen, sind mit Verfahren zu verschlüsseln, die mindestens den Anforderungen der kommerziellen Datensicherheit genügen. Damit ist die Mindestlänge der symmetrischen Schlüssel mit 80 Bit anzusetzen, wobei folgenden Verfahren zur Anwendung kommen können:

- IDEA,
- 3DES in den Varianten mit zwei Schlüsseln,
- die AES Kandidaten,

Als Protokolle für die verschlüsselte Kommunikation von Inhalten sind vorzugsweise die folgenden vorzusehen:

- S/MIME für die Kommunikation von Daten in der zeitversetzten Variante (z.B. Email)
- SSL für den Direktzugriff und für die Tunnelverschlüsselung
- TLS für den Direktzugriff und für die Tunnelverschlüsselung
- IPSEC für die Verschlüsselung des gesamten IP-Verkehrs

In Übergangssituationen kann auch PEM eingesetzt werden.

Das Keymanagement bzw. Keyagreement für Zwecke der Inhaltsverschlüsselung hat die folgenden Aspekte umzusetzen:

- Die Schlüssel zwischen den Kommunikationspartner sind auch für die Inhaltsverschlüsselung so auszuhandeln, dass die Authentizität gesichert ist. Dazu haben sich Server und Client bzw. die Kommunikationspartner zu authentifizieren. Diese Authentifikation hat auf Zertifikaten zu basieren.
- Für die Erzeugung der Schlüssel bzw. soweit es sich um Pseudozufallszahlen handelt für die Erzeugung der Seed-Daten ist ein geeigneter qualitätsvollen Zufall zu verwenden. Der qualitätsvolle Zufall ist analog den Anforderungen der Signaturverordnung (SigV0) zu gestalten.
- Werden Pseudozufallszahlen mit einem Seed verwendet, so darf weder eine Vorwärts- noch eine Rückwärtsprognose der Werte aus bekannt gewordenen Werten möglich sein.

2. Elektronische Signatur:

- Die elektronische Signatur ist in den Bereichen, wo eine Schriftform erforderlich ist als sichere Signatur gemäß Signaturgesetz (SigG) auszubilden.
- Die Mechanismen, Schlüssellängen und Stärken der Verfahren sind auch dann einzuhalten, wenn es sich nicht um sichere Signaturen handelt und solche nicht erforderlich wären.

3. Sicherheitstoken

- Für den Einsatz der elektronischen Signatur sind entsprechende technische Mittel (Token) notwendig. Die Anforderungen an Sicherheitskriterien bzw. Evaluierung ist im SigG und der SigVO geregelt. Zusätzlich existieren im Bereich Medizinische Informatik Anforderungen, die in der europäischen Vornorm ENV 13727 Health Informatics - Secure User Identification for Healthcare, Strong Authentication using Microprocessor Cards
- Als Sicherheitstoken dürfen im Gesundheitsbereich nur Prozessorkarten, bei stationärer Verwendung besondere Sicherheitsmodule verwendet werden. Das Freischalten des Tokens kann entweder über Passphrasen oder biometrischer Merkmale (dzt. noch in Entwicklung) erfolgen.
- Der Sicherheitstoken wird zur Authentifizierung des Benutzers und zur impliziten Sicherstellung der Datenintegrität (digitale Signatur) benötigt. Hierzu muss der Sicherheitstoken in der Lage sein, den benötigten asymmetrischen Schlüssel generieren zu können. Die geforderten Rahmenbedingungen (verwendeter Algorithmus, Schlüssellänge,...) sind der SigVO zu entnehmen.
- Die Evaluierung der Sicherheitstoken hat gemäß den Vorgaben der SigVO (Prüfstellen, Bestätigungsstelle, Rahmenbedingungen) zu erfolgen.

4. Passwortsysteme

Die Anforderungen an Passwortsysteme sind in der europäischen Vornorm ENV 12251 (1999) Health Informatics - Secure User Identification for Healthcare - Identification and Authentication by Passwords - Management and Security beschrieben. Folgende Rahmenbedingungen müssen bei der Verwendung von Passwörtern eingehalten werden.

- Ein Passwort muss mindestens 8 Charakter lang sein
- Als verwendbare Zeichen sind alle Groß- und Kleinbuchstaben, alle Ziffern sowie die Sonderzeichen zulässig
- Ein Passwort muss mindestens eine Zahl bzw. ein Sonderzeichen auf weisen
- Passwörter dürfen nur an sicheren Orten aufbewahrt werden, die sichtbare und lesbare Verwahrung eines Passwortes am Bildschirm (z.B. Postit,...) ist nicht zulässig.
- Die Verwendungsdauer eines Passwortes darf maximal 3 Monate betragen. Wurde ein Passwort kompromittiert, ist das Passwort unverzüglich geändert werden.
- Passwörter dürfen nicht in Shellscripts oder auf Funktionstasten gespeichert werden.

Nach mehrfacher fehlerhafter Eingabe eines Passwortes (im Normalfall 3x) ist das Passwort zu sperren. Das weitere Vorgehen ist in der Sicherheitspolitik festzulegen.

8. Anhang IV.b: Sicherheitsmaßnahmen und Sicherheitsempfehlungen **(normativ gemäß Konformitätserklärung)**

8.1 Sicherheitsmaßnahmen

Um die in Kapitel 4 beschriebene Sicherheitspolitik auch technisch realisieren zu können, sind folgende Sicherheitsmaßnahmen notwendig. Diese Maßnahmen können je nach Größe der Organisationseinheit durchaus unterschiedlich sein. Als Minimalforderungen müssen jedoch entsprechende Methoden für Authentifikation, Zugriffskontrolle, Vertraulichkeit, Datenintegrität und Ursprungsnachweis implementiert sein. Die dazu notwendigen Mechanismen und Implementierungen des Keymanagements, der Sicherheitstoken, der Passwortsysteme, der Verschlüsselung und der elektronischen Signatur müssen geeignet und soweit im Anhang zu MAGDA-LENA II genauer spezifiziert, diesem entsprechend umgesetzt werden.

Authentifikation und Zugriffskontrolle

Bevorzugt zur Authentifikation von Personen oder Systemen sind Verfahren einzusetzen, welche eine Zertifizierungsstruktur mit eingebundenen Sicherheitstoken, die auch in geeigneter Weise vor fahrlässiger Benutzung schützen können (z.B. Smartcards) unterstützen. Integrierte und ortsbezogene Systeme (z.B. personalisierter Sicherheitstoken zum Raumzutritt und zur EDV-Authentifikation) können die Anforderungen der Benutzerfreundlichkeit und der Sicherheit gleichzeitig erfüllen. Für die EDV-Authentifikation werden asymmetrische Methoden, die gleiche Techniken wie die elektronische Signatur nutzen bzw. zero-knowledge Methoden als angemessen empfohlen. Herkömmliche Passworte sind nur mehr in jenen Fällen, wo dies aus technischen oder organisatorischen Gründen derzeit nicht möglich ist und konventionelle Passwortsysteme eingesetzt werden, müssen diese einer vorgegebenen Policy (Länge und Zeichenwahl) entsprechen. Die Übergangsphase darf längstens 2 Jahre betragen. Alle eingesetzten Mechanismen sind mit einem automatischen Ablaufdatum zu versehen. Die Authentifikation muss im System effizient umgesetzt sein und es müssen Umgehungsmechanismen auch für Insider ausgeschlossen sein.

Vertraulichkeit

Geeignete Verschlüsselung von sensiblen Daten mit hinreichender Schlüssellänge und vertrauenswürdigem Keymanagement garantiert, dass diese Informationen vertraulich zwischen den Kommunikationspartnern übermittelt werden können. Die Methoden sind für gleichzeitige und zeitversetzte Kommunikation zwar unterschiedlich, doch in den entsprechenden Standards, die im Anhang zu MAGDA-LENA II aufgelistet sind, verfügbar. Die Verschlüsselung zur Vertraulichkeit ist für die Übertragung und für die allfällige Speicherung jedenfalls unterschiedlich zu wählen. Die Verschlüsselung der gespeicherten Daten ist nicht Gegenstand von MAGDA-LENA II. Der Sessionkey für eine vertrauliche Kommunikation ist nur während des betreffenden Kommunikationsprozesses relevant. Keys für unterschiedliche Sessions sind hinreichend unterschiedlich zu wählen, damit dadurch keine Sicherheitslücke entsteht. Eine Hinterlegung bzw. Langzeitspeicherung der Schlüssel der Übertragung ist nicht

vorzusehen. Die Verarbeitung der Schlüssel muss so gestaltet sein, dass diese weder aus Backups, noch aus Swap-space-Analysen oder sonstigen temporären Datenrelikten des Systems ermittelt werden können. Weiters werden die entsprechenden Rahmenbedingungen (siehe Anforderungen an Keymanagement) eingehalten werden, welche für den sicheren Schlüsselaustausch als auch für die sichere Generierung dieser Schlüssel notwendig sind. In die Erzeugung des Sessionkeys sind Verfahren der Authentifizierung einzubinden, die hinreichend kryptographische Stärke besitzen. Die konkreten Anforderungen werden im Anhang zu MAGDA-LENA näher festgelegt.

Datenintegrität

Um die Unverfälschtheit der in elektronischen Netzen übermittelten Daten zu garantieren sind Methoden notwendig, welche die Datenintegrität der übermittelten Informationen anzeigen. Als einfachste Methoden sind Prüfsummen bzw. Hash - Algorithmen zu nennen. Implizit wird die Datenintegrität von übermittelten Informationen auch gewährleistet, wenn der Ursprungsnachweis mittels elektronischer Signatur erfolgt. Die Rahmenbedingungen hierfür sind im Signaturgesetz und der Signaturverordnung festgelegt. Bei sensiblen Anwendungsteilen, die eine zusätzliche Kontrolle der Integrität der Informationen durch Personen nicht ermöglichen oder bei welchen aus dem Prozedere heraus eine solche in der Regel entfällt, sind als Methoden der Datenintegrität jene Verfahren einzusetzen, die den sicheren elektronischen Signaturen nach SigG bzw. SigVO entsprechen. Dies muss jedenfalls bei allen vollautomatisierten Vorgängen, die im Bereich der ärztlichen Tätigkeit eingesetzt werden, der Fall sein.

Ursprungsnachweis

Der Ursprungsnachweis von Daten kann durch den Einsatz asymmetrischer kryptographischer Verfahren gewährleistet werden. Hierfür werden die Elemente, Methoden und Verfahren der elektronischen Signatur (inklusive der notwendigen Rahmenbedingungen) empfohlen. Dies gilt auch dann, wenn diese Methoden automatisiert ausgelöst werden und daher keine Signaturen im Sinne des SigG sind. Die entsprechenden technischen und organisatorischen Grundlagen für die elektronische Signatur sind im Signaturgesetz und der Signaturverordnung festgelegt. Ein Ursprungsnachweis nach den Technologien der sicheren elektronischen Signaturen muss jedenfalls bei allen vollautomatisierten Vorgängen, die im Bereich der ärztlichen Tätigkeit eingesetzt werden, erfolgen.

8.2 Empfehlungen

Sind die Methoden für Authentifikation, Vertraulichkeit, Datenintegrität und Ursprungsnachweis verbindlich zu implementieren, sind die nachstehenden Sicherheitsmaßnahmen nur von größeren Organisationseinheiten zu implementieren. Die nachstehenden Maßnahmen sollen sicherstellen, dass sicherheitsrelevante Komponenten schwer manipuliert bzw. umgangen werden können. Neben den sicherheitstechnischen Überlegungen sind die Realisierungen der nachstehenden Sicherheitsdienste auch von wirtschaftlichen Überlegungen abhängig. Für Betreiber

von Netzwerken bzw. Provider ist zusätzlich zu den Punkten a. - c. Punkt d. Verfügbarkeit des Systems anzuwenden.

Zutrittskontrolle

Der Zugang zu den eigenen Netzwerken von außen (einkommender Datenverkehr insbesondere auch von offenen Netzen) soll über entsprechende Sicherheitskomponenten (z.B. Firewalls, abgesicherte RAS Server) erfolgen. Diese Komponenten sind vertrauenswürdig aufzubauen und zu betreiben. Der Zutritt zu diesen Komponenten darf nur einem eingeschränkten und in der Sicherheitspolicy festgelegten Personenkreis möglich sein. Jeder Zutritt in diesem Bereich ist zu protokollieren und in geeigneter Weise periodisch oder bei Bedarf auszuwerten. Ausreichende Mechanismen sind zu installieren, um den Missbrauch möglichst verhindern zu können.

Audit Trail

Große Organisationseinheiten bzw. Dienstleister sind verpflichtet, die gesamte anfallende Protokollierung regelmäßig oder bei Bedarf auszuwerten. Ebenso sind auch nicht erfolgreiche Attacken von außen auf das System zu protokollieren und mit Gegenmaßnahmen zu beantworten. Mittels Audit Trails sollen alle Maßnahmen auf ihre Effizienz überprüft werden. Protokolle sind elektronisch und in gesicherter Form (zeitgestempelt und elektronisch signiert) aufzubewahren.

Wartung

Alle Maßnahmen, welche zur Instandhaltung eines Systems eingesetzt werden können, bedürfen zusätzlicher Regelungen. Hierzu zählen die Wartung vor Ort, die Fernwartung sowie das Software Update. Eine Wartung vor Ort soll nur in Gegenwart eines Vertreters des Auftraggebers erfolgen, Fernwartung soll auf nicht sicherheitsrelevante Komponenten des Systems beschränkt werden. Das Update von Software Modulen bzw. das Upgrade von Hardware Komponenten soll ebenfalls nach bestimmten Richtlinien erfolgen. Wird Fernwartung ermöglicht, so ist eine klare Policy festzulegen. Anhang „Fernwartung“ zu MAGDA-LENA II gibt dazu ein Beispiel an.

Verfügbarkeit des Systems

Der Betreiber eines Netzwerkes bzw. Provider hat für die gesicherte Zustellung innerhalb eines definierten Zeitraums zu sorgen. Das Kommunikationssystem hat entsprechende Informationen (z.B. Identifikation, Zeitpunkt der Kommunikation) am System zu protokollieren. Diese Daten sind entsprechend dem Telekommunikationsgesetz aufzubewahren bzw. bei Bedarf zu überprüfen.

Die genannten organisatorischen und technischen Maßnahmen können durch weitere Sicherheitsmaßnahmen ergänzt werden. Alle unter 4.2 Organisatorischen Rahmenbedingungen und im Anhang aufgezählten Maßnahmen sind Minimalanforderungen für ein sicheres Kommunikationssystem. In bestimmten Bereichen können die genannten Anforderungen nach Durchführung einer Risikoanalyse während eines beschränkten Übergangszeitraumes (längstens jedoch für

2 Jahre) aufgeschoben werden. Die Sicherheit des Systems muss jedoch durch geeignete technische und organisatorische Maßnahmen gewährleistet sein. Alle genannten Maßnahmen können durch andere Methoden ersetzt werden, soweit diese zumindest gleichwertige Sicherheit gewährleisten. Die einzusetzenden Methoden sind in Anhang D beschrieben.

9. Glossar und Abkürzungsverzeichnis

(ohne englische Ausdrücke in Anhang 3.3.)

Abstract Syntax Notation One

Ist eine Standardgrammatik, die unter anderem für die Beschreibung von abstrakten Datentypen, Syntaxen und Nachrichten verwendet und üblicherweise in einer Backus-Naur Form eingesetzt wird

Akteur

Wird im Sinne von UML verwendet (engl. Actor)

Allgemeine hierarchische Nachrichtenbeschreibung

Zwischenschritt bei der Nachrichtenentwicklung, um nicht-hierarchische theoretische Modelle in hierarchische Strukturen umwandeln zu können. Dieser Schritt kann entfallen, wenn bereits im Modell hierarchische Strukturen vorliegen oder bei der weiteren Umsetzung keine hierarchischen Strukturen benötigt werden.

Allgemeine Nachrichtenbeschreibung

Untermenge eines Domäneninformationsmodells, welches sowohl den semantischen Kontext, die Struktur einer Nachricht, als auch die Beziehungen der einzelnen Objekte zueinander beschreibt

ANSI

American National Standards Institute

Anwendungsfall

Wird im Sinne von UML verwendet (engl. Use Case)

Anwendungsfalldiagramm

Wird im Sinne von UML verwendet (engl. Use Case Diagram)

Anwendungsfallmodell

Wird im Sinne von UML verwendet (engl. Use Case Model)

ASN.1 - Siehe Abstract Syntax Notation One

ASTM

American Society for Testing and Materials.

Auftraggeber (DSG 2000):

Natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu

einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;

Authentifizierung

Die eindeutige individuelle Identifizierung eines Benutzers durch das System oder gegenüber dem System (z.B. durch Eingabe einer Identifikation und eines Passwortes oder durch eine ID-Card oder durch biometrische Methoden).

Autorisierung

Die Vergabe von Zugriffsrechten (Berechtigungsprofil) durch das System an einen authentifizierten Benutzer (diese Zugriffsrechte müssen nicht direkt mit dem individuellen Benutzer verbunden sein, sondern können mit einer Benutzergruppe verbunden sein, der der Benutzer aufgrund seiner Authentifizierung zugeordnet ist).

Backus-Naur Form

Ist eine Notationsform für Ersetzungsregeln kontextfreier Grammatiken, die vor allem zur Definition der Syntaxen von formalen Sprachen eingesetzt wird.

Betroffener (DSG 2000)

Jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;

BNF - Siehe Backus-Naur Form

CEN

Europäische Normungsbehörde (European Committee for Standardization, vgl.: <http://www.cenorm.be/>)

Check digit - siehe Prüfziffer.

Datei (DSG 2000)

Strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;

Daten (DSG 2000)

(„personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist; „nur indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;

Datenanwendung (DSG 2000)

(früher: „Datenverarbeitung“): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);

Datenintegrität

Die Tatsache, dass Daten nicht unbefugt oder unbeabsichtigt verändert oder gelöscht wurden.

DHCP (Dynamic Host Configuration Protocol)

Ermöglicht die dynamische Konfiguration von IP-Adressen und dazugehörigen Parametern.

DICOM

Der DICOM-Standard ("Digital Imaging and Communications in Medicine") wurde im Jahr 1993 publiziert und kontinuierlich weiterentwickelt. 1995 wurde er als MEDICOM (ENV 12052) auch in Europa als Standard (siehe CEN) akzeptiert.

Dienste

Wird in der internationalen Literatur oft auch als „Service“ bezeichnet

Dienstleister (DSG 2000)

Natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z 8);

Domäne

Jenes Problem oder jener Fachbereich der bearbeitet wird

Domänenexperte

Eine Person, die mit den Charakteristika eines bestimmten Fachbereichs vertraut ist und dieses Wissen entsprechend anwenden oder weitergeben kann

Domäneninformationsmodell

Modell, das dazu dient die Informationserfordernisse eines Fachbereichs darzustellen

EGP (Exterior Gateway Protocol)

Exterior Gateway Protocol ist das erste Protokoll aus der Gruppe der ExteriorGateway Protokolle. Inzwischen wird es zunehmend durch BGP (Border Gateway Protocol) und IDRP (Inter Domain Routing Protocol) ersetzt.

Ermitteln von Daten (DSG 2000)

Das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;

Header

Kopfstück eines Dokuments.

HL7

HL7 ist eine Non-profit Organisation, welche Standards entwickelt und beim American National Standards Institute (ANSI) akkreditiert ist (vgl. www.hl7.org)

ICMP (Internet Control Message Protocol)

Das Internet Control Message Protocol ist ein wesentlicher Bestandteil von IP und muss in jeder Implementation vorhanden sein. ICMP hat ausschließlich die Aufgabe, Fehler- und Diagnoseinformationen für IP zu transportieren. Es dient damit der Kommunikation zwischen den an der Datagrammvermittlung beteiligten Übertragungseinrichtung und Endgeräten.

ID

Identifizier: Ein Code aus Zahlen und/oder Buchstaben, der einen Patienten identifiziert.

IDEF1X

Ist eine Methode zur Datenmodellierung, die ihren Schwerpunkt auf den Entwurf von relationale Datenbanken legt und im Dezember 1993 vom amerikanischen "National Institute of Standards and Technology (NIST)" als Standard verabschiedet wurde.

Identifikationsvariable: siehe ID.

IDRP (Inter Domain Routing Protocol)

IDRP hat eine Ende-zu-Ende-Sicherung implementiert. IDRP ist durch kryptographische Signaturen in den Routinginformationen besser als BGP vor Fehlern und Sabotage geschützt.

Implementierbare Nachrichtenspezifikationen

Umsetzung der im allgemeinen Modell beschriebenen Bedingungen in eine spezielle Transfersyntax. Hierzu kann unter Berücksichtigung der betreffenden Transfersyntax eine weitere Entwicklung der beschriebenen Strukturen notwendig sein.

Klasse - Wird im Sinne von UML verwendet (engl. Class)

Informationsverbundsystem (DSG 2000)

Die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;

Instanz - Wird im Sinne von UML verwendet (engl. Instance)

ISDN (Integrated Services Digital Network)

Digitales Datenkommunikationsnetzwerk zur integrierten Übertragung von Sprache und Daten, welches in absehbarer Zeit das herkömmliche analoge Telefonnetz zunehmend ersetzen wird.

Kommunikationspartner

Sind jene Parteien, die an einer Kommunikation mit Hilfe von Nachrichten beteiligt sind

Kommunikationsrolle

Beschreibt die Funktion eines Kommunikationspartners in Beziehung zum Informationsaustausch

Konformität - Übereinstimmung mit einer Spezifikation

Konformitäts-Erklärung.

Eine Erklärung eines Teilnehmers oder Providers über die Einhaltung der MAGDA-LENA Richtlinien und die Offenlegung von Methoden und Maßnahmen gemäß Kapitel 6 dieses Papiers.

LAN - (Local Area Network)

LDAP (Lightweight Directory Access Protocol)

Despite all the progress in messaging, corporate directories are still a bit of a mess. On LANs, each e-mail system has its own directory, which is not interoperable with those of other vendors. On larger systems using TCP/IP, there's no single directory standard -- certainly not one that's routinely used on the scale of intranets. X.500, the CCITT standard for directories, offers promise for large-scale directories but is large and unwieldy to implement, plus its specifications call for use of the OSI protocol stack. Add to that the ungainly nature of X.500 addresses and user acceptance has been slow, at best.

Although no single directory specification is likely to become the global standard, LDAP, or the Lightweight Directory Access Protocol, ties together various directories in a useful manner.

(<http://www.sunworld.com/swol-10-1996/swol-10-ldap.html>)

MAGDA-LENA Provider

Ein Dienstleister, der für eine Gruppe von MAGDA-LENA Teilnehmern eine MAGDA-LENA-konforme Kommunikation anbietet. Dies umfasst jedenfalls auch die Verschlüsselung der Daten gemäß Anhang IV.a und die Betreuung der Teilnehmer in Bezug auf Datenschutz und Datensicherheit gemäß Kapitel 4. Der Provider kann auch die Dienste eines Netzbetreibers (vgl. dort) anbieten.

Metasyntax

Ist eine Syntax, die zur Beschreibung einer anderen Syntax verwendet wird.

MIB (Management Information Base)

MKK - MAGDA-LENA-konformes Kommunikationskonzept.

Modulus-X

Mathematischer Algorithmus zur Berechnung einer Prüfwert.

Nachricht

Identifizierbare und strukturierte Menge von funktionell zusammengehöriger Information für den Datenaustausch, welche einen bestimmten Verwendungszweck erfüllt.

Netzbetreiber

Ein MAGDA-LENA-Netzbetreiber bietet Dienste gemäß Kapitel 5 an (vgl. auch MAGDA-LENA-Provider).

Partei

Wird als Oberbegriff für Person oder Organisation verstanden.

POP (Point of Presence)

Internetzugangspunkt von Providern.

PPTP - (Point to Point Tunneling Protocol)

Profil

Beschreibt die für einen bestimmten, genau definierten Anwendungsbereich benötigten Komponenten einer bestimmten Nachricht

Provider - siehe MAGDA-LENA Provider.

Prüfziffer

Ein Teil einer Nummer, der mit Hilfe eines mathematischen Algorithmus die Korrektheit der ganzen Nummer mit einer bestimmten Wahrscheinlichkeit bestätigt.

RAID 5

Sicherheitsstandard zur Datenrekonstruktion auf in Servern eingesetzten Festplatten

Die Daten werden über mehrere Laufwerke verteilt.

Zusätzlich wird eine Art Prüfsumme (=Parity) berechnet .

Die Parity-Information wird über alle Laufwerke verteilt, d. h. es gibt kein dediziertes Parity-Laufwerk. Bei Ausfall eines Laufwerkes werden dessen Daten mit Hilfe der verbleibenden Laufwerke wieder rekonstruiert. Weitere Infos: <http://www.innosoft.com/ldapworld/>

Registrierte Directories

Listen, in denen alle potentiellen Kommunikationsteilnehmer angeführt sind und die in Pfaden organisiert sind, so dass jeder Teilnehmer im Zusammenhang mit der Organisation, der er angehört, auffindbar ist.

RSA

Die Mathematiker Rivest, Shamir und Adleman entwickelten 1978 das nach ihnen benannte und heute noch eingesetzte asymmetrische RSA-Verfahren (= Public Key Verfahren).

Sensible Daten (DSG 2000)

(„besonders schutzwürdige Daten“): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;

Sicherheitspolitik

Die Gesamtheit der organisatorischen und technischen Maßnahmen zum Schutz der Datenintegrität und zum Schutz vor unbefugtem Zugriff auf die Daten oder missbräuchliche Verwendung der Daten .

SMTP (Simple Mail Transfer Protocol)

Ermöglicht den Versand von ASCII-Textnachrichten zu Mailboxen auf TCP/IP-Hosts in einem Netzwerk

SNMP (Simple Network Management Protocol)

Das Simple Network Management Protocol verwirklicht den Austausch von Managementinformationen zwischen Netzelementen und Managementsystemen. Grundsätzlich sollten alle TCP/IP-Implementationen über das Netz managebar sein.

SSN

Social Security Number.

Standards Internationale oder Nationale

Alle von internationalen Standardisierungsgremien (ISO, IEC, ITU, W3C, UN, CEN, CENELEC, ETS) - oder von deren nationalen Vertretungen - verabschiedeten Standards

Stereotyp

Wird im Sinne von UML verwendet (engl. Stereotype)

SV-Nr- . (Österreichische) Sozialversicherungsnummer.

Syntax

Ist die Beschreibung der Struktur einer formalen Sprache

Szenario

Wird im Sinne von UML verwendet (engl. Scenario)

TCP/IP (Transmission Control Protocol/ Internet Protocol)

Wird für das Management von TCP/IP-Netzwerken verwendet. Dieses Protokoll kann Managementabfragen zu anderen Knoten in einem Netzwerk senden.

Transfersyntax

Regeln und Beschreibungen, welche eine strukturierte Übertragung von Informationen ermöglichen.

UDP (User Datagram Protocol)

Das User Datagram Protocol realisiert den verbindungslosen, datagrammorientierten Dienst der Transportschicht. UDP liefert über die Leistungen von IP hinaus leiglich eine Prüfsumme über die Daten und eine Portnummer. UDP läßt sich gut für Hochgeschwindigkeitsanwendungen einsetzen.

Überlassen von Daten (DSG 2000)

Die Weitergabe von Daten vom Auftraggeber an einen Dienstleister

Übermitteln von Daten (DSG 2000)

Die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;

UML - Siehe Unified Modeling Language

UN/CEFACT

United Nations/Centre for the Facilitation of Procedures and Practices for Administration, Commerce and Transport (vgl. <http://www.unece.org/cefact>)

UN/EDIFACT

United Nations / Electronic Data Interchange for Administration, Commerce and Transport (vgl. <http://www.unece.org/trade/untdid/>)

Unified Modeling Language

Ist eine objektorientierte Modellierungssprache und Notation zur Spezifikation, Konstruktion, Visualisierung und Dokumentation von Modellen. Sie wurde durch die Object Management Group (<http://www.omg.com/uml>) standardisiert und besitzt eine weltweite industrielle Unterstützung.

USV

Unterbrechungsfreie Stromversorgungseinheit) Stichworte mit der Bezeichnung (DSG 2000) sind dem DSG 2000 § 4 entnommen.

Verarbeiten von Daten (DSG 2000)

Das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z 12) von Daten;

Verwenden von Daten (DSG 2000)

Jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten;

Vorgehensmodell

Gesamtheit der Aktivitäten aller beteiligten Personen eines Entwicklungsprozesses, ihre Beziehungen, Voraussetzungen und Ergebnisse.

Zeitstempel

Eindeutige Kennung eines Dokumentes durch die genaue Angabe des Zeitpunkts seiner Fertigstellung.

Wird im Sinne von UML verwendet (engl. Class)

Zustimmung (DSG 2000)

Die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;