Österreichische Ärztekammer

Richtlinien der Österreichischen Ärztekammer für die Übermittlung medizinischer Daten

Version 6.3
19. Mai 2005

Vorbemerkung

Ziel dieser Richtlinien ist, unterschiedliche Befundcarrier und Client-Systeme anhand vorgegebener Punkte einheitlich zu beurteilen. Durch die hier festgelegten Punkte soll die Kompatibilität unterschiedlicher Befundcarrier und Client-Systeme unter Einhaltung einheitlicher Sicherheitsnormen gewährleistet sein. Damit soll die Übertragung von Befunden auch zwischen Teilnehmern, die sich unterschiedlicher Client-Systeme und Befundcarrier bedienen, ermöglicht werden.

Die Österreichische Ärztekammer sieht dies als wichtigen Schritt zur Umsetzung der von der STRING-Kommission des BMGF vorgelegten und in MAGDA-LENA 2 definierten Rahmenbedingungen an sowie zur Berücksichtigung des Gesundheits-Telematik-Gesetzes.

Definitionen

Zur Erleichterung der Formulierung gelten im Folgenden die hier angeführten Definitionen:

Befundcarrier:

Dienstleister (-Firma) für die Übertragung von medizinischen Daten. Dies können Befunde, Arztbriefe, Bilder oder sonstige Daten aus dem medizinischen Bereich sein.

Befunde, Befundübermittlung, ...:

Mit Befunden sind alle Daten aus dem medizinischen Bereich, also auch Arztbriefe, Überweisungen, Bilder, usw. gemeint.

SMTP-Email-Adresse:

Eindeutige Adresse für jeden Empfänger von medizinischen Daten.

Teilnehmer:

Die organisatorischen Einheiten wie Arzt, Labor oder Krankenhaus welche Befunde versenden oder empfangen.

Signatur:

Mit Signatur ist immer die Signatur des sendenden Teilnehmers - also der organisatorischen Einheit - gemeint. Damit soll der Absender eindeutig festgestellt werden können. Es handelt sich dabei also um keine Signatur im Sinne des SigG, welche sich ja immer auf eine Person bezieht.

1 Das Befundübertragungssystem

In diesem Bereich ist alles angeführt was den Befundcarrier betrifft. Als Schnittstelle zum Bereich 3 (das Client-System) gilt der Übergang an der POP3- bzw. SMTP-Schnittstelle. In diesen Bereich fallen auch alle Übergänge zwischen zwei Befundcarriern.

Die Aufgabe des Befundcarriers ist vor allem, die, vom Client-System des Absenders bereit gestellten Befunde zu übertragen und diese dem Empfänger in dessen Client-System bereitzustellen.

Das Client-System selbst kann vom Befundcarrier zur Verfügung gestellt werden, kann aber auch von diesem unabhängig sein. Die Anpassung des EDV-Systems des Teilnehmers ist nicht Aufgabe des Befundcarriers. Ebenso fällt die Entscheidung über bisherige oder zukünftige Befundformate (EDIFACT, XML, etc.) nicht in die Zuständigkeit des Befundcarriers.

1.1 Der Befundcarrier stellt jedem seiner Kunden mindestens ein Email-Postfach mit einer dazugehörigen SMTP-Email-Adresse (gem. RFC 2822) zur Verfügung.

1.2 Der Abruf des Postfaches durch das Client-System muss zumindest über POP3 möglich sein. Die Übermittlung von medizinischen Daten vom Client-System an den Befundcarrier erfolgt mittels SMTP. Die Übertragung von Befunden zwischen Befundcarriern erfolgt mittels SMTP.

1.3 Die SMTP-Email-Adresse dient als eindeutige Kennung eines Teilnehmers im Befundübermittlungssystem.

1.4 Das Postfach darf ausschließlich für die Übermittlung von Befunden verwendet werden.

1.5 Der Befundcarrier hat sicher zu stellen, dass die SMTP-Email-Adressen aller seiner Kunden gemeinsam mit dem jeweils aktuell gültigen Zertifikat (oder der URL des Zertifikates auf einem Zertifikatsserver) jedes Kunden im eVGA-Verzeichnisdienst eingetragen sind.

1.6 Der Befundcarrier muss bei ausgehenden Befund-Emails sicherstellen, dass:
- diese nur an einen einzigen Empfänger gerichtet sind
- die Email-Adresse des Absenders im („From“-Feld des Emails) bei ihm eingerichtet und gültig ist.
Befund-Emails von nicht gültigen Absendern sind abzulehnen.

1.7 Die Verfügbarkeit seiner "Systeme" muss während der vom Befundcarrier garantierten Betriebszeiten innerhalb eines Jahres mindestens 99,5% betragen. Ausfälle der GIN-Infrastruktur werden nicht in die Verfügbarkeit des Befundcarriers miteingerechnet.

1.8 Der Preis für die Befundübermittlung darf nicht davon abhängig sein, an welchen Empfänger Befunde versendet werden. Zwischen verschiedenen Befundcarriern darf für die Weiterleitung/Entgegennahme von Befunden nichts verrechnet werden.

1.9 Die Entgegennahme von Befunden von anderen zertifizierten Befundcarriern und die Weiterleitung von Befunden an andere zertifizierte Befundcarrier nach den hier definierten Kriterien muss vom Befundcarrier gewährleistet werden.

1.10 Der Befundcarrier muss die Übermittlungen protokollieren (mit Absender, Empfänger, SMTP-Email-Adresse sowie Zeit- und Datumsstempel). Zur Abfrage dieser Protokolle durch den Client muss er eine auf Internet-Technologie basierende (HTTPS) Applikation zur Verfügung stellen. Diese Abfrage darf nur authentifiziert erfolgen.Diese Übertragungs-Kontroll-Funktionen (Rückbestätigung) des Befundcarriers können auch im Client-System implementiert werden.

1.11 Haftung und Gewährleistung sind vertraglich zu regeln.

1.12 Der Befundcarrier muss über eine Security–Policy verfügen, die mindestens folgende Punkte regelt: Administration und Wartung, Zugangsregelungen, Ablaufdokumentationen, Änderungsberechtigungen, Systemdokumentation, Räumlichkeiten.Diese ist auf Anfrage der Österreichischen Ärztekammer dieser zur Verfügung zu stellen.

1.13 Eine Überprüfung eines Befundcarriers muss im Auftrag der Österreichischen Ärztekammer durch geeignete Dritte ermöglicht werden.

1.14 Nur definierte SMTP-Server (IP-Adressen) von zertifizierten Befundcarriern dürfen am Befundübertragungssystem teilnehmen. Es sind dies die Server, bzw. IP-Adressen der Befundcarrier mit einer ÖÄK-Prüfnummer.

1.15 SMTP-Sessions zwischen dem Client-System und dem Befundcarrier müssen authentifiziert werden. Die Art der Authentifizierung (Passwörter, Zertifikate, IP-Adressen etc.) ist dem Befundcarrier überlassen.

1.16 Explizites „Source Routing“ sowie der „%-Hack“ dürfen vom SMTP-Email-System des Befundcarriers nicht unterstützt werden.

1.17 Die SMTP-Server des Befundcarriers müssen über einen gültigen Reverse-DNS-Eintrag verfügen.

1.18 Der Befundcarrier muss zur Absicherung seiner Dienste gegenüber dem Internet ein Firewallsystem betreiben und dieses laufend auf aktuellem sicherheitstechnischem Niveau halten.

1.19 Der mögliche Datenverlust (Postfächer, Posteingang und Mail-Queue (Postausgang)) durch Störungen und Systemausfälle muss vom Befundcarrier durch geeignete Maßnahmen (Backup) auf maximal 24 Stunden begrenzt werden.

1.20 Die Wiederherstellung der gesicherten Email-Postfächer muss innerhalb von 24 Std. erfolgen. Wiederhergestellte Dateien dürfen in der Zwischenzeit eingegangene Dateien nicht löschen oder überschreiben. Eingehende Dateien dürfen in der Zwischenzeit wiederhergestellte Daten nicht löschen oder überschreiben.

1.21 Die Systeme des Befundcarriers sind so auszulegen, dass der Ausfall einer einzelnen Komponente – z.B. einer Festplatte – nicht zum Datenverlust führt.

2 Der Verzeichnisdienst:

Hier werden jene Daten bereitgestellt, die zum Befunddatenaustausch über verschiedene Befundcarrier hinweg benötigt werden (entspricht dem eHealth-Register lt GesTelG).Der Verzeichnisdienst enthält die zur Übertragung medizinischer Daten berechtigten Gesundheitsdienstleister und kann auch für eine ersatzweise postalische Versendung dienen.

2.1 Für den Befunddatenaustausch ist ein Verzeichnisdienst (LDAP) erforderlich.

2.2 Zertifikate, basierend auf dem Standard X.509v3 werden verarbeitet. Das Zertifikat beinhaltet mindestens den Namen und die SMTP-Email-Adresse. Die Gültigkeitsdauer darf maximal 5 Jahre betragen.

2.3 Weitere beschreibende Attribute sind in Anlage A definiert.

2.4 Die für den Verzeichnisdienst nötigen Daten werden auf dem zentralen eVGA Server eingetragen. Dieser gilt als autoritative Quelle für die Daten des Befundübermittlungssystems.

2.5 Der Abgleich der Daten des zentralen eVGA-Servers mit den internen Systemen des Befundcarriers kann täglich und muss mindestens wöchentlich erfolgen.

2.6 Die Eintragungen, Änderungen und Löschungen im zentralen eVGA-Server erfolgen, je nach Inhalt, durch die jeweilige Ärztekammer, die Befundcarrier oder andere berechtigte Teilnehmergruppen mit entsprechend abgestuften Sicherheitsmechanismen.
Diese Abstufung von Inhalt und Sicherheitsmechanismen je Teilnehmergruppe wird in Anlage-A festgelegt.

3 Das Client-System

Das ist jenes System, welches bei einem Sender oder Empfänger von Befunden eingesetzt wird. Als Schnittstelle zum Bereich 1 (das Befundübertragungssystem) gilt der Übergang an der POP3- bzw. SMTP-Schnittstelle. Als Schnittstelle zum Bereich 4 (das EDV-System des Teilnehmers) gilt die Übergabe/Übernahme der Daten in einem definierten Filesystem (Inbox/Outbox).

Die Aufgabe des Client-Systems ist es, Befunde in einer "Outbox" vom EDV-System des Teilnehmers entgegenzunehmen und alle dort befindlichen Daten in folgender Reihenfolge weiterzubearbeiten: als Versender zu signieren, den/die Empfänger zu ermitteln, den public key des Empfängers zu suchen, die Daten zu verschlüsseln und für die Übertragung durch den Carrier bereitzustellen. Auf dem Client-System des Empfängers sind die Daten zu entschlüsseln, die Signatur auf Gültigkeit (z.B. Ablaufdatum, Zertifizierungsdienstanbieter ZDA, Standard lt. Anhang B, passt die eMail-Adresse des Zertifikats mit der gesendeten überein) zu prüfen und die korrekten Befunde in einer "Inbox" dem EDV-System des Teilnehmers zur Verfügung zu stellen. Bei ungültigem Zertifikat sind die Daten in einem speziellen Unterverzeichnis abzulegen. Die Vorgänge in diesem System müssen protokolliert sein.

3.1 Die Validierung der Befunde erfolgt im System des Senders. Für den Befundcarrier sind nur alle jene Befunde, die in der ”Outbox” als klar definierte Schnittstelle stehen, versandfertig. Befunde werden erst von der Übertragungsliste ("Outbox") genommen, wenn diese erfolgreich übertragen wurden.

3.2 Die Übertragungsvorgänge werden auf dem Client-System mit Zeitmarken protokolliert. Die Abweichung der Zeit darf maximal 30 Minuten von der realen Zeit sein.

3.3 Die Protokolle werden für einen Zeitraum von mindestens 6 Monaten archiviert.

3.4 Der Client hat die Möglichkeit, sich über den aktuellen Status des Befundes (der Befundabholung) zu informieren. Siehe dazu auch Punkt 1.10.

3.5 Der Befundcarrier muss den Teilnehmer darüber ausdrücklich informieren, dass bei seinem EDV-System kein ungesicherter Internet-Zugang bestehen darf. Eine entsprechende Verpflichtung des Teilnehmers wird empfohlen.

3.6 Die „private keys“ für die Verschlüsselung von Befunden dürfen ausschließlich unter der physischen Kontrolle des Teilnehmers sein.

3.7 Der Teilnehmer hat dafür zur sorgen, dass der „private key“ gegen Verwendung durch nicht berechtigte Personen gesichert ist.

3.8 Die Verschlüsselungs- u. Signaturstandards sind in Anhang B definiert.

3.9 Die verwendeten Zertifikate für alle verschlüsselten Protokolle müssen von einem durch die ÖÄK gelisteten Zertifikatsanbieter stammen. Zertifikate aller von der ÖÄK gelisteten Zertifikatsanbieter müssen akzeptiert werden. Die Liste der zulässigen Zertifikatsanbieter wird in Abstimmung mit den zertifizierten Befundcarriern von der ÖÄK festgelegt.

3.10 Beim Empfang entscheidet das Client-System, in welchen Verzeichnissen und unter welchem Namen Nachrichten gespeichert werden. Es muss dabei sicher gestellt sein, dass nur Verzeichnisse verwendet werden, die innerhalb der definierten "Inbox" liegen und dass bestehende Dateien nicht überschrieben werden.

3.11 Da für eine Übergangszeit (siehe auch Punkt 4.3) die Empfängeradressierung auch auf Basis der "ME-Nummer"

(bei Vertragsärzten: ME ergänzt mit der Hauptverbandsnummer) ermöglicht wird, muss das Client-System in der Lage sein, anhand dieser Nummer die SMTP-Email-Adresse des Empfängers zu ermitteln.

3.12 Damit beim Teilnehmer bestehende Systeme unverändert neben neuen Systemen bestehen können, müssen die neuen Formate (laut Punkt 4.6 - XML-Allonge) in einem eigenen Unterverzeichnis innerhalb der "Inbox" bereit gestellt werden.

3.13 Werden Befunde in der "Outbox" versehen mit einer XML-Allonge (siehe Punkt 4.6) bereit gestellt, so müssen die XML-Allonge und alle darin definierten Files gemeinsam verschickt werden.

3.14 Die unverschlüsselte Speicherung von Befunden auf Systemen des Befundcarriers ist nicht zulässig.

3.15 Das Client-System des Versenders muss Befunde als Attachments gem. RFC 2822 an den Befundcarrier übermitteln. Das Client-System des Empfängers muss Attachments gem. RFC 2822 verarbeiten können..

3.16 Das Client-System kann auch die Integration in die EDV- bzw. Softwaresysteme (Patientendatenbank) des Teilnehmers ermöglichen.

4 Das EDV-System des Teilnehmers

Das ist jenes System, welches die zu sendenden Daten in die Outbox zur Übernahme durch das Client-System (Bereich 3) gibt bzw. die vom Client-System (Bereich 3) in der Inbox bereitgestellten Daten aus dieser holt.

Das EDV-System des Teilnehmers liegt im Ermessen und in der Verantwortung des Teilnehmers und kann hier nicht näher spezifiziert werden. Es wird daher im Folgenden nur auf jene Punkte eingegangen, welche für den sicheren und kompatiblen Transport der zu übertragenden Daten erforderlich sind. Eine Normierung von Dateninhalten - wie Arztbriefe, Laborparametern, usw. ist nicht Gegenstand dieser Richtlinien.

4.1 Die Übergabeschnittstellen zum Client-System für den Versand und den Empfang bestehen in den Dateisystem-Directories "Outbox" und "Inbox". Das EDV-System des Teilnehmers darf nur validierte und für den Versand bereite Befunde in die "Outbox" übergeben. Alle Daten müssen vor der Übertragung in die "Outbox" mit einem aktuellen Virenscanner geprüft werden. Wurde ein Befund erfolgreich übertragen, wird dieser durch das Client-System aus der "Outbox" gelöscht. Siehe dazu auch Punkt 3.1.

4.2 Damit das Client-System den Empfänger ermitteln kann, muss dieser in einer der folgenden Arten durch das EDV-System des Teilnehmers bereitgestellt werden:
- In einer XML-Allonge (siehe Punkt 4.6).
- In einer gültigen Edifact-Syntax.
- In einer zwischen dem EDV-System eines Teilnehmers und dem Client-System vereinbarten Form, wenn es sich um einen rein bilateralen Datenaustausch handelt.

4.3 Die Empfänger- und Absenderadressierung erfolgt über die SMTP-Email-Adresse, welche vom EDV-System des Teilnehmers entsprechend Punkt 4.2 bereitgestellt werden muss.
Für eine Übergangszeit bis zum 1.7.2007 ist die Empfänger- und Absenderadressierung auch auf Basis der ME-Nr. laut Punkt 3.11 möglich.

4.4 Das Client-System darf die in der "Outbox" bereitgestellten Daten nicht verändern, muss diese jedoch vor dem Versand verschlüsseln. Es ist daher Aufgabe des EDV-Systems des Teilnehmers, wenn erwünscht, die Daten vor der Übergabe an die "Outbox" zu komprimieren. Ebenso ist es die Aufgabe des EDV-Systems des Teilnehmers in der "Inbox" eingelangte komprimierte Daten zu dekomprimieren. Da das Client-System aus den Daten in der "Outbox" den Empfänger ermitteln muss, ist eine Komprimierung nur bei solchen Daten möglich, welche durch ein zusätzliches File in Form einer nicht komprimierten XML-Allonge beschrieben werden. Derzeit muss für die Komprimierung ZIP verwendet werden.

4.5 Es ist Aufgabe des EDV-Systems des Teilnehmers, die Datenformate und Normen der in der "Inbox" - entsprechend Punkt 4.2 - bereitgestellten Befunde richtig zu interpretieren und abzulegen. Das EDV-System des Teilnehmers muss in der Lage sein, von einlangenden Befunden das Befund-Format zu bestimmen und diese weiterzuverarbeiten. Die technischen Formate sind durch die Extension definiert.
Das absendende System soll sicherstellen, dass der Empfänger die Möglichkeit hat, zu erkennen, ob ein Dokument (aus technischen Gründen, z.B. Recovery) wiederholt gesendet wurde, oder gezielt ein zweites Mal.

4.6 Die Übertragung von unterschiedlichen Datenformaten und Dateninhalten muss zukünftig ohne Veränderung und ohne Auslesen der für die Übertragung bereitgestellten Daten möglich sein. Dazu muss zur Beschreibung dieser Files vom EDV-System des Teilnehmers ein zusätzliches File - die XML-Allonge erstellt werden. Diese XML-Allonge enthält mindestens den Empfänger und Absender sowie den Verweis auf ein oder mehrere zu übertragende Files. Ein Verweis auf Dateisystem-Verzeichnisse ist optional. Nähere Informationen zur XML-Allonge sind in Anhang C angeführt.

4.7 Wünscht der Absender eines Befundes eine positive Rückbestätigung, so muss das EDV-System dieses Teilnehmers eine XML-Allonge entsprechend Punkt 4.6 bereitstellen, welche zusätzlich den Parameter <Bestaetigung> enthält. Der Inhalt dieses Parameters ist eine interne Kennung des EDV-Systems dieses Teilnehmers für die zu sendende Nachricht.

4.8 Das EDV-System des Empfängers liest diese XML-Allonge und stellt dem Empfänger den angehängten Befund zur Verfügung. Das EDV-System des Empfängers muss ein Verfahren haben, wie der Empfänger den korrekten Empfang bestätigt. Dieses Verfahren muss auch bewirken, dass der XML-Allonge des empfangenen Befundes der Parameter <Empfangsbestaetigung> mit dem Parameter <Datum> hinzugefügt wird. Der Inhalt dieses Parameters ist Datum und Uhrzeit der Empfangsbestätigung. Ansonsten muss die XML-Allonge völlig unverändert bleiben und wieder in die "Outbox" gestellt werden.

4.9 Das Client-System liest diese XML-Allonge und stellt durch den Parameter <Empfangsbestaetigung> fest, dass es sich um eine Empfangsbestätigung handelt. Das Client-Systen muss in diesem Fall nur die XML-Allonge an den Absender (statt an den Empfänger) senden. Somit landet diese XML-Allonge - ergänzt durch den Parameter <Empfangsbestaetigung> - in der "Inbox" des Absenders.

4.10 Das EDV-System des Absenders liest diese XML-Allonge, stellt fest, dass es sich um eine Empfangsbestätigung handelt und kann anhand des Parameters <Bestaetigung> diese Bestätigung automatisch der richtigen Nachricht zuordnen. Notfalls kann diese XML-Allonge auch vom Absender direkt in einem Browser gelesen werden. Da der Inhalt exakt derselbe ist, den der Absender verschickt hat, ist auch eine optische Zuordnung zum verschickten Befund möglich. Damit wird für den Absender sichergestellt, dass der Befund beim Empfänger ordnungsgemäß entgegengenommen wurde.

4.11 Wenn die XML-Allonge zu einer ÖNORM wird (in Vorbereitung ist die ÖNORM K2200) dann behält sich die Österreichische Ärztekammer vor, in einer Übergangsfrist von 1 Jahr diese ÖNORM zu übernehmen.

5 Änderungsprozess für dieses Dokument

5.1 Die ÖÄK überarbeitet diese Richtlinien grundsätzlich im Jahreszyklus und gibt bei jeder Änderung die Notwendigkeit einer Rezertifizierung bekannt. Das Arbeitsdokument wird an die zertifizierten Befundcarrier ausgesendet. Nach dem schriftlichen Rücklauf und den Stellungnahmen beginnt der ÖÄK-Überarbeitungszyklus. Danach wird die Endversion veröffentlicht und Betroffene setzen die neuen Richtlinien um. Sollte eine Rezertifizierung notwendig sein, wird diese durchgeführt

5.2 Die Ärztekammer wird bis 1. Juli jeden Jahres dieses Dokument überarbeiten und an alle zertifizierten Befundcarrier aussenden.

5.3 Die Befundcarrier haben nach der Aussendung 3 Wochen Zeit, um schriftliche Stellungnahmen und Korrekturwünsche an die ÖÄK zu übermittlen.

5.4 Danach wird die ÖÄK innerhalb von 4 Wochen eine endgültige neue Version dieses Dokumentes fertig stellen und aussenden.

5.5 Alle zertifizierten Befundcarrier sind verpflichtet, bis 12 Monate nach Veröffentlichung der Endversion ihre Produkte entsprechend den geänderten Richtlinien bei all ihren Kunden zu implementieren und – wenn eine Rezertifizierung notwendig ist - rezertifizieren zu lassen.

5.6 Die ÖÄK kann kurzfristige Änderungen an diesem Dokument jederzeit aus folgenden Gründen vornehmen:

- Anpassung an gesetzliche Änderungen
- Behebung von kritischen Sicherheitsmängeln
- Präzisierung von vorhandenen Regelungen in diesem Dokument

Im Falle solcher Änderungen gelten ebenfalls die in 5.1 bis 5.5 definierten Fristen mit Ausnahme gesetzlich vorgegebener Fristen. Kritische Sicherheitsmängel sind unverzüglich zu beheben.

6 Anhang A) Das zentrale LDAP-Verzeichnis (eVGA)

6.1 Allgemeines

6.1.1 Das zentrale Verzeichnis wird unter dem Namen eVGA (elektronisches Verzeichnis der Gesundheitsdienste-Anbieter) und den entsprechenden Hostnamen „ldap.evga.at“ und „ldap2.evga.at“ zur Verfügung gestellt.

6.1.2 Der eVGA-Verzeichnisdienst unterstützt das Protokoll LDAPv3.

6.2 Zugriff

6.2.1 Der Basiszugriff auf den eVGA-Verzeichnisdienst kann anonym und unverschlüsselt erfolgen. Dabei ist die Suche nach einzelnen Einträgen möglich; als Resultat werden nur öffentlich verfügbare Attribute zurückgeliefert. Für eine erweiterte Anzahl von Attributen im Resultat ist der authentifizierte Zugriff Bedingung.

6.2.2 Der authentifizierte Zugriff auf den eVGA Verzeichnisdienst erfolgt verschlüsselt über TLS auf Port 389 (RFC 2830).

6.2.3 Die Authentifizierung von Clients erfolgt mittels Benutzername und Passwort über simple Authentication oder SASL (RFC 2222, RFC 2829) mit der Methode DIGEST-MD5. Benutzername und Passwort werden vom Betreiber des eVGA-Verzeichnisdienstes zur Verfügung gestellt.

6.2.4 Die Authentifizierung kann auch über Client-Zertifikate erfolgen, die der Server beim TLS-Verbindungsaufbau vom Client anfordert. Für diesen Zweck dürfen nur Zertifikate verwendet werden, die jeweils von einem der von der ÖÄK genannten Zertifizierungsdiensteanbieter ausgestellt wurden, welche die Identität des Inhabers nachweislich repräsentieren, und bei welchen der Zertifikatsinhalt eine eindeutige, automatisierte Zuordnung zum jeweiligen Eintrag des Nutzers im Verzeichnis ermöglicht.

6.2.5 Der Befundcarrier kann eigene LDAP-Server betreiben. Die Möglichkeit zur LDAP-Replikation des eVGA-Servers wird auf Wunsch durch den Betreiber des eVGA-Verzeichnisdienstes für zertifizierte Befundcarrier konfiguriert. Unterstützt wird OpenLDAP V2.2 und neuere Versionen, sowie kompatible Server.

6.3 Datenlieferung/Datenwartung

6.3.1 Der Befundcarrier hat alle technischen Datensätze der von ihm betreuten Kunden jede Woche bis spätestens Montag 6.00 zu aktualisieren bzw. für deren Aktualisierung zu sorgen.Die Datenlieferung erfolgt durch das Web-Interface des eVGA-Integrationsservers (www.evga.at). Es ist auch eine automatische Datenanlieferung möglich. Detaillierte Informationen sind der eVGA-Dokumentation zu entnehmen.
Die Datenlieferung hat im XML-Format zu erfolgen. Das Schema ist der jeweils aktuellen eVGA-Dokumentation zu entnehmen.

6.3.2 Datenlieferanten, die vor dem 30.4.2005 im LDIF-Format geliefert haben, können ihre Daten in einer Übergangszeit bis 31.12.2005 weiterhin im LDIF-Format bereitstellen. Dabei hat die Lieferung im Encoding ISO 8859-1 (Latin 1) zu erfolgen.

6.3.3 Die Feldinhalte der LDIF-Datensätze haben den Vorgaben der eVGA-Dokumentation (http://www.evga.at) in der jeweils aktuellen Form zu entsprechen.

6.3.4 Der Befundcarrier hat zu jedem technischen Datensatz entweder das Zertifikat des Kunden selbst oder aber die URL des auf einem öffentlich verfügbaren Verzeichnisserver gespeicherten Zertifikates zu übermitteln.

6.3.5 Der Befundcarrier hat bei der Datenlieferung sicher zu stellen, dass jede von ihm gelieferte ME-Nummer über alle seine Teilnehmeradressen hinweg eindeutig ist.

7 Anhang B) Die Verschlüsselungs- und Signaturstandards

7.1 Zu verwendende Algorithmen

S/MIME
S/MIMEv2 (RFC 2311)
Unter Verwendung einer der folgenden Ciphersuites:
DES-EDE3-CBC bzw. RC2-CBC: 128
Mit
SHA bzw. MD5

7.2 Zertifikate

X.509v3

Housley, R., Ford, W., Polk, W., Solo, D.: Internet X.509 Public Key Infrastructure, Certificate and CRL Profile. RFC 2459, Jänner 1999.
bzw.:
ITU-T Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, Juni 1997.

7.3 Kompatibilität

Die Kompatibilität zu folgenden Produkten ist wesentlich
S/Mimev2

- Outlook 2000
- Outlook 2003
- Outlook Express
- Outlook 98
- Netscape Messenger
- IAIK S/MIME-Mapper

8 Anhang C) Die XML-Allonge - Beispiele

Das exakte Format von XML-Allongen wird durch XML-Schemata definiert, die auf www.evga.at zu finden sind. An dieser Stelle sind beispielhaft zwei Muster von Allongen / Empfangsbestätigungen angeführt.

Beispiel 1: Version Vorarlberg

8.1 Mindestinhalt:

```
<?xml version="1.0" encoding="windows-1252"?>
<Allonge>
        <Empfaenger>
                <EMail>empf.teilnehmer@befundcarrier.at</EMail>
        </Empfaenger>
        <Absender>
                <EMail> abs.teilnehmer@befundcarrier.at</EMail>
        </Absender>
        <Nachricht>
                <Betreff>Bilder wie eben besprochen</Betreff>
        </Nachricht>
        <Inhalte>
                <Datei>bild1.jpg</Datei>
                <Datei>bildx.jpg</Datei>
        </Inhalte>
</Allonge>
```

8.2 Inhalt, wenn Empfangsbestätigung erwünscht:

```
<?xml version="1.0" encoding="windows-1252"?>
<Allonge>
        <Empfaenger>
                <EMail>empf.teilnehmer@befundcarrier.at</EMail>
        </Empfaenger>
        <Absender>
                <EMail>abs.teilnehmer@befundcarrier.at</EMail>
                <Bestaetigung>Internes Kennzeichen des Senders</Bestaetigung >
        </Absender>
        <Nachricht>
                <Betreff>Bilder wie eben besprochen</Betreff>
        </Nachricht>
        <Inhalte>
                <Datei>bild1.jpg</Datei>
                <Datei>bildx.jpg</Datei>
        </Inhalte>
</Allonge>
```

8.3 Empfangsbestätigung:

```
<?xml version="1.0" encoding="windows-1252"?>
<Empfangsbestaetigung>
        <Datum>TT.MM.YYYY HH:MM</Datum>
        <Allonge>
                        <Empfaenger>
                        <EMail>empf.teilnehmer@befundcarrier.at</EMail>
                        </Empfaenger>
                        <Absender>
                        <EMail>abs.teilnehmer@befundcarrier.at</EMail>
                        <Bestaetigung>Internes Kennzeichen des Senders</Bestaetigung >
                        </Absender>
                <Nachricht>
                        <Betreff>Bilder wie eben besprochen</Betreff>
                </Nachricht>
                <Inhalte>
                        <Datei>bild1.jpg</Datei>
                        <Datei>bildx.jpg</Datei>
                </Inhalte>
        </Allonge>
</Empfangsbestaetigung>
```

Beispiel 2: GNW-Gesundheitsnetz Wien - Version

8.4 Beispiel XML-Allonge:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Allonge xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="AllongeALA.xsd">
  <Header>
    <Empfaenger>
      <eMail>empfangemail@befundcarrier.at</eMail>
    </Empfaenger>
    <Absender>
      <eMail>absendemail@befundcarrier.at</eMail>
    </Absender>
    <Message>
      <MessageKennung>MessageKennung</MessageKennung>
      <BetriebsStelleKey>BetriebsStelleKey</BetriebsStelleKey>
      <DatenArt>AbrechnungsDaten</DatenArt>
      <DatenType>DatenSenden</DatenType>
      <TransportFormat>TransportECommerce</TransportFormat>
      <AnzahlDerElementeDieserNachricht>1</AnzahlDerElementeDieserNachricht>
      <ElementNummerDieserNachricht>1</ElementNummerDieserNachricht>
    </Message>
  </Header>
  <SentItems>
    <Bloecke>
      <Block>
        <Datei>
          <NameInAttachment>attachmentName</NameInAttachment>
          <DateiNameLang>fileName</DateiNameLang>
          <Zuordnung>assignment</Zuordnung>
        </Datei>
      </Block>
    </Bloecke>
    <NameAttachment>Attachment.ZIP</NameAttachment>
    <NameAllonge>XYZ_Allonge.ALE</NameAllonge>
  </SentItems>
  <StatusBlock>
    <Status>
      <HauptStatus>4</HauptStatus>
      <HauptStatusText>Transport</HauptStatusText>
      <BearbeitungsStatus>ErfolgreichBeendet</BearbeitungsStatus>
      <DatumZeit>2005-09-01T02:09:11</DatumZeit>
    </Status>
  </StatusBlock>
  <PhysicalSenderParameter>
    <eMail>eMail@physicalSender</eMail>
  </PhysicalSenderParameter>
  <PhysicalEmpfaengerParameter>
    <eMail>eMail@physicalReceiver</eMail>
  </PhysicalEmpfaengerParameter>
</Allonge>
```

8.5 Beispiel Empfangsbestätigung:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<Allonge xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="AllongeALE.xsd">
  <Header>
    <Empfaenger>
      <eMail>empfangemail@befundcarrier.at</eMail>
    </Empfaenger>
    <Absender>
      <eMail>absendemail@befundcarrier.at</eMail>
    </Absender>
    <Message>
      <MessageKennung>MessageKennung</MessageKennung>
      <BetriebsStelleKey>BetriebsStelleKey</BetriebsStelleKey>
      <DatenArt>AbrechnungsDaten</DatenArt>
      <DatenType>DatenSenden</DatenType>
      <TransportFormat>PatientenDaten</TransportFormat>
      <AnzahlDerElementeDieserNachricht>1</AnzahlDerElementeDieserNachricht>
      <ElementNummerDieserNachricht>1</ElementNummerDieserNachricht>
    </Message>
  </Header>
  <SentItems>
    <Bloecke>
      <Block>
        <Datei>
          <NameInAttachment>attachmentName</NameInAttachment>
          <DateiNameLang>fileName</DateiNameLang>
          <Zuordnung>assignment</Zuordnung>
        </Datei>
      </Block>
    </Bloecke>
    <NameAttachment>Attachment.ZIP</NameAttachment>
    <NameAllonge>XYZ_Allonge.ALE</NameAllonge>
  </SentItems>

  <StatusBlock>
    <Status>
      <HauptStatus>4</HauptStatus>
      <HauptStatusText>Transport</HauptStatusText>
      <BearbeitungsStatus>ErfolgreichBeendet</BearbeitungsStatus>
      <DatumZeit>2005-09-01T02:09:11</DatumZeit>
    </Status>
  </StatusBlock>
  <PhysicalSenderParameter>
    <eMail>eMail@physicalSender</eMail>
  </PhysicalSenderParameter>
  <PhysicalEmpfaengerParameter>
    <eMail>eMail@physicalReceiver</eMail>
  </PhysicalEmpfaengerParameter>
</Allonge>
```