Gesellschaft für Medizinische Datenverarbeitung mbH
Mai 2006

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das Produkt e-health.solutions

1. Zeitraum der Prüfung

1. September 2005 - 13.2.2006

2. Antragsteller

Gesellschaft für Medizinische Datenverarbeitung mbH
Stromstraße 39
10551 Berlin

3. Sachverständige Prüfstelle

datenschutz nord GmbH
Barkhausenstraße 10-14
27568 Bremerhaven

Gutachter:
Dr. Uwe Schläger
Oliver Stutz

4. Kurzbezeichnung des IT-Produkts

e-health.solutions, Version 4.0

5. Detaillierte Bezeichnung des Produkts

Das Produkt e-health.solutions besteht im Wesentlichen aus folgenden Komponenten:

- Applications-Server:
  - Datenmodell (HL7, DICOM, Formulare, Texte)
  - Berechtigungskonzept (u.a. Ärzte, Pflegestation, auftragserteilende Station, leistungserbringende Station, Pförtner, Notfall-Login)
- Anwendung:
  - Fallübersicht
  - Patientenübersicht
  - Terminverwaltung
  - Auftragserteilung (Labor, Radiologie)
  - Auftragsübersicht
  - Abfragen

--- Dokumentenverwaltung für einfache Dokumente (Texte, Bilder), strukturierte Dokumente (Formulare), generierte Dokumente (z.B. Arztbriefe)

--- Formulargestaltung

--- Erstellung von Arztbriefen, Befundberichten (Schnittstelle zu MS Word)

--- Freigabe von Dokumenten für andere Benutzer

Die Anwendung wird realisiert durch signierte Java-Applikationen (Java 1.5). Hierunter fällt auch ein Java-basierter Dicom-Viewer; dies ist ein Programm zum Anzeigen von medizinischen Bildern im DICOM-Format (Digital Imaging and Communicatins in Medicine). Der DICOM-Viewer ist als Java-Applikation Teil des Produkts und wird – wie alle anderen Anwendungen auch – mittels eines Code-Signing Zertifikats gegen Manipulation gesichert.

Für das Code Signing wird ein kommerzielles Zertifikat von Thawte Consulting verwendet, dessen Zertifikat zusammen mit den gängigen Browsern ausgeliefert wird. Ähnlich wie auch beim Einsatz von SSL wird beim Code Signing RSA mit 1024 Bit als asymmetrisches Verschlüsselungsverfahren und AES mit 256-Bit bzw. aus Kompatibilitätsgründen RC-4 mit 128 Bit als symmetrisches Verschlüsselungs-verfahren eingesetzt.

Die Daten werden zwischen Client und Server per SSL verschlüsselt. Das SSL-Zertifikat wird beim Installieren des Produkts individuell für den jeweiligen Kunden generiert.

Die Zusammenführung von Daten mehrerer Krankenhäuser erfolgt unter Verwendung eines Master Patient Index, der auf einfachen Matchingkriterien basiert, die von den Krankenhäusern beliebig definiert werden können; im Allgemeinen werden hierzu der Name, das Geschlecht und das Geburtsdatum verwendet, aber auch andere Merkmale sind denkbar. Aus den Merkmalen werden entsprechende Hash-Werte gebildet, die eine Zusammenführung von Patienten-daten ermöglichen, sofern der Patient hierin einwilligt.

6. Tools, die zur Erstellung des Produkts verwendet wurden

--- Modellierung: Oxygen XML Editor 6, Poseidon Version 3

--- SUN Java JDK 1.5 (Bibliotheken, Compiler, JavaDoc)

--- Java Entwicklungsumgebung (IDE, Debugger): Eclipse 3.1

--- Java Profiler: J Enerjy

--- Datenbankentwicklung: SQL-Navigator 5.6, NaturalDocs (Datenbank-Code-Dokumentation)

--- Testwerkzeuge: Rational Testsuite inkl. Robot, Last- und Stresstestmodule

--- Changemanagement: Rational ClearQuest (Enhancement-, Bugtracker) sowie Subversion (Versionskontrolle)

7. Zweck und Einsatzbereich

e-health.solutions ist ein Produkt für klinisches Datenmanagement. Es stellt die Komponenten zur Integration medizinischer IT-Systeme im Krankenhaus bereit und unterstützt den Workflow am klinischen Arbeitsplatz. E-health.solutions dient folgenden Aufgaben:

--- Zusammenführung, d.h. Import, Speicherung, visuelle Darstellung von Daten aus verschiedenen medizinischen Systemen (KIS, Labor-Informationssystem, Radiologiesystem),

--- Erfassung medizinischer Leistungen,

--- Erstellung der medizinischen Dokumentation (u.a. Arztbriefe, Formulare),

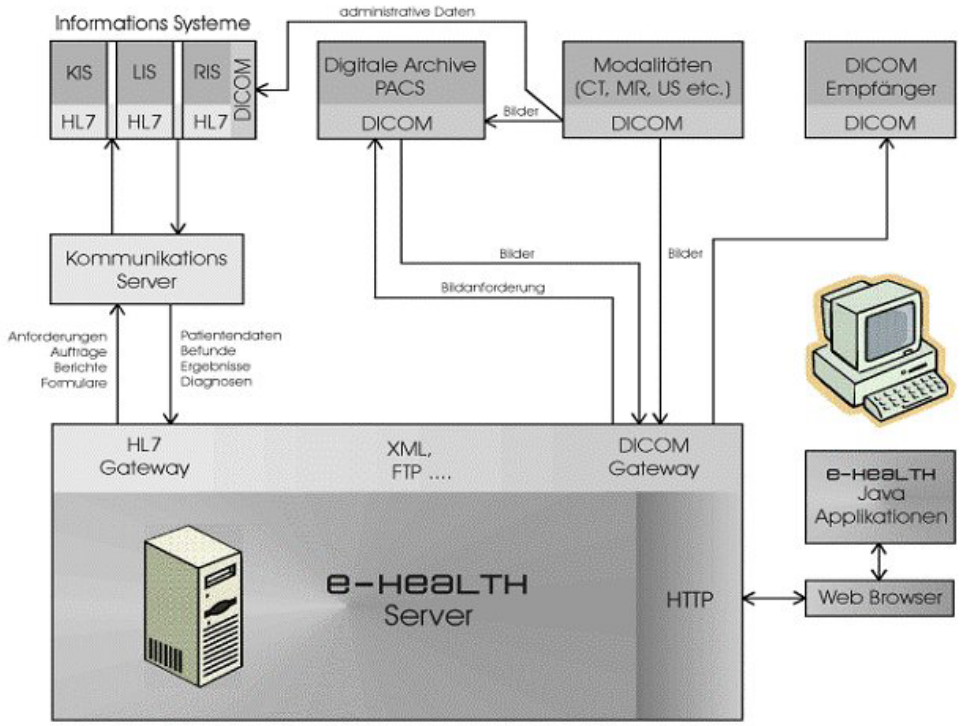
--- Erteilung von Aufträgen an Leistungsstellen (Radiologie, Labor),

--- Terminverwaltung,

--- Erfassung und Kalkulation von Diagnosen, Maßnahmen und DRG,

--- Zusammenführung von Patientendaten aus verschiedenen Krankenhäusern.

8. Modellierung des Datenflusses



9. Version des Anforderungskatalogs, die der Prüfung zugrunde gelegt wurde

Version 1.2

10. Zusammenfassung der Prüfungsergebnisse

Das Produkt e-health.solutions entspricht insgesamt den Anforderungen in besonderer Weise, da die verwendeten technischen Lösungen innovativ die Umsetzung der gesetzlichen Vorgaben ermöglichen. Dies gilt insbesondere für den Notfall-Button sowie die Möglichkeit, die Patientendaten nach Abschluss der Behandlung sperren und ggf. später löschen zu können. Die Produktdokumentation ist verständlich und aussagekräftig.

Der datenschutzkonforme Einsatz von e-health.solutions setzt eine sichere Einsatzumgebung bestehend aus signierter Java-Applikation, gesicherter SSL-Verbindung sowie ordnungsgemäß betriebenen Server- und Client-Betriebssystemen voraus, die nicht Bestandteil des auditierten Produkts sind.

Mit dem Produkt e-health.solutions werden dem Anwender zahlreiche Funktionen zur Verfügung gestellt, die ebenso wie die Einsatzumgebung im Rahmen des Customizing an die jeweiligen Anforderungen des Anwenders anzugleichen sind. So stellt e-health.solutions ein differenziertes Berechtigungskonzept mit vorkonfigurierten Rollen zur Verfügung; diese müssen jedoch vor Inbetriebnahme individuell an die Geschäftsprozesse eines jeden Krankenhauses angepasst werden. Die Ausgestaltung der vorkonfigurierten Rollen war nicht Bestandteil der Begutachtung.

Aus den Bewertungen der beiden Datenart-Anforderungsprofile ergibt sich folgende Gesamtbewertung:

Nr.	Anforderungsprofil	Bewertung / Kommentar
Datenart A: Medizinische Daten (Primärdaten)		
A1	Produktbeschreibung	verständlich und aussagekräftig, in vollem Umfang sichergestellt
A2	Datensparsamkeit, Pseudonyme	in adäquater Weise sichergestellt
A3	Zulässigkeit der Datenverarbeitung	zulässig
A4	Authentizität der Nutzer	in vollem Umfang sichergestellt
A5	Authentizität des Servers	in vollem Umfang sichergestellt
A6	Vertraulichkeit der übertragenen Daten	in vollem Umfang sichergestellt
A7	Vertraulichkeit der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A8	Integrität der übertragenen Daten	in vollem Umfang sichergestellt
A9	Integrität der auf dem Server gespeicherten Daten	in vollem Umfang sichergestellt
A10	Verfügbarkeit der Daten	in vollem Umfang sichergestellt
A11	Revisionsfähigkeit	in vollem Umfang sichergestellt
A12	Betroffenenrechte	in vollem Umfang sichergestellt

Datenart B: Protokolldaten (Sekundärdaten)		
B1	Produktbeschreibung	verständlich und aussagefähig, in vollem Umfang sichergestellt
B2	Zulässigkeit der Verarbeitung	zulässig
B3	Vertraulichkeit der Protokolldaten	im vollem Umfang sichergestellt
B4	Integrität der Protokolldaten	in vollem Umfang sichergestellt
B5	Verfügbarkeit der Protokolldaten	im vollem Umfang sichergestellt

11. Beschreibung, wie das Produkt den Datenschutz fördert

Das Produkt e-health.solutions enthält folgende datenschutzfördernde Funktionen:

--- Pförtnersperre:

e-health.solutions ermöglicht eine patientenbezogene Aktivierung der Pförtnersperre, d.h. der Aufenthalt eines Patienten im Krankenhaus wird nicht auf den Monitoren von Auskunftspersonen (Pförtner, Telefonzentrale) angezeigt, sofern ein Patient seinen Krankenhausaufenthalt nicht Dritten offenbaren möchte.

--- Sperrung von Daten nach Abschluss der Behandlung:

e-health.solutions ermöglicht das Sperren eines Falles nach Abschluss der Behandlung. Sofern der jeweilige Fall ggf. wieder benötigt wird, kann der Fall wieder entsperrt werden.

--- Notfall-Login:

Es existiert ein Notfall-Button, mit dessen Hilfe ein umfassender Zugriff auf sämtliche Daten möglich ist. Die Aktivierung des Notfall-Logins wird ebenfalls entsprechend dokumentiert.

--- Dezidiertes Berechtigungskonzept:

Die Vertraulichkeit der Daten wird durch ein Berechtigungskonzept sichergestellt, das die Vergabe sehr differenzierter Zugriffsrechte ermöglicht.

--- Finalisierung von Dokumenten:

Durch die Finalisierung von Dokumenten, die nur von explizit hierzu berechtigten Personen durchgeführt werden kann, wird die Integrität der Daten in besonderer Weise sichergestellt.

--- Auskunftsfunktion:

Durch die umfassende Auskunftsfunktion wird den betroffenen Patienten die Möglichkeit gegeben, detailliert Auskunft über die zu ihrer Person gespeicherten Daten zu erhalten.