datenschutz cert

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das Produkt Galileo

im Auftrag der NoemaLife GmbH

datenschutz cert GmbH

14. Oktober 2008

datenschutz cert

Inhaltsverzeichnis

Kurzgutachten zur Erteilung eines Datenschutz-Gütesiegels für das Produkt Galileo

1. Zeitraum der Prüfung

Die Begutachtung der Applikation Galileo erstreckte sich auf den Zeitraum von 14.09. bis 14.10.2008 und beinhaltete neben der konzeptionellen Analyse der von der NoemaLife GmbH zur Verfügung gestellten Unterlagen (Leistungsbeschreibung, System Configuration, Sicherheitskonzept, Benutzerhandbuch) die Durchführung von Plausibilitätstests.

2. Antragstellerin

Antragstellerin dieses Gutachtens ist die

NoemaLife GmbH
Alt-Moabit 96
10559 Berlin

als Hersteller des Produkts Galileo.

Ansprechpartner ist Herr Jörg Rädisch.

3. Sachverständiger/Prüfstelle

Sachverständige dieses Gutachtens ist die Prüfstelle

datenschutz cert GmbH
Barkhausenstr. 2
27568 Bremerhaven.

Ansprechpartner sind Frau Irene Karper (Recht) und Herr Ralf von Rahden (Technik).

4. Kurzbezeichnung des IT-Produkts

Begutachtet wird das Produkt **Galileo** in der Version **1.0** – ehemals bekannt als e-health®.solutions.

5. Beschreibung des IT-Produkts, Zweck und Einsatzbereich

Galileo kann von Krankenhäusern in öffentlich-rechtlicher Trägerschaft genutzt werden. Es wird als klinisches Datenmanagement eingesetzt, integriert medizinische IT-Systeme im Krankenhaus und unterstützt den Workflow am klinischen Arbeitsplatz.

Das Produkt Galileo besteht im Wesentlichen aus folgenden Komponenten:

- Applikations-Server:
  - Datenmodell (HL7, DICOM, Formulare, Texte)
  - Berechtigungskonzept (u.a. Ärzte, Pflegestation, auftragserteilende Station, leistungserbringende Station, 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 Communications 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.

Die Daten werden zwischen Client und Server per SSL verschlüsselt. Das SSL-Zertifikat wird beim Installieren des Produkts individuell für den jeweiligen Kunden generiert. Das Zertifikats-Template ist im Sicherheitskonzept (Handbuch für den Sicherheitsbeauftragten) zur Kontrolle enthalten. Die standardmäßig verwendeten Algorithmen und Schlüssellängen sind

--- RSA 2048

--- AES-256

In Ländern mit gesetzlich beschränkter Schlüssellänge wird AES-128 bzw. RC4 mit 128-bit Schlüssellänge verwendet. Damit entsprechen die Algorithmen und Schlüssellängen den Empfehlungen der Bundesnetzagentur und des Bundesamtes für Sicherheit in der Informationstechnik.

Die Nutzung von Galileo kann bei Bedarf auf bestimmte IP-Adressen eingeschränkt werden. Diese Funktion ist insbesondere für die Nutzung der Administratorkennung von Bedeutung.

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 Hashwerte gebildet, die eine Zusammenführung von Patientendaten ermöglichen, sofern der Patient hierin einwilligt. Die Verwaltung der Matching-kriterien und Hashwerte erfolgt auf einem sogenannten MPI-Server, der entweder von einem Krankenhaus oder von einem externen Dienstleister im Rahmen von Auftragsdatenverarbeitung betrieben wird. Diejenigen, die berechtigt sind, über die

MPI-Schnittstelle auf Daten anderer Krankenhäuser zugreifen zu dürfen, werden explizit über das Berechtigungskonzept definiert.

Der Funktionsumfang von Galileo 1.0 umfasst den von e-health®.solutions 4.0. Die folgenden Funktionen wurden ergänzt:

--- Eine überarbeitete Navigation und Repräsentation von Daten erlaubt dem Benutzer flexiblere Filter einzusetzen und Ordnerstrukturen anzupassen.

--- Überarbeitete GUI und Übersichtsdarstellung von Informationen

--- Vorschlagsliste und Löschfunktion von Altdaten

--- API/Plugin Schnittstelle zur Entwicklung von kundenspezifischen Modulen und Applikationsdesigner zur komfortableren Nutzung der bereits vorhandenen Funktionalität zur Erstellung neuer Formulare.. Beides steht nicht dem Endanwender zur Verfügung. Sicherheits- und Zugriffschutzfunktionen sind bei allen neuen Services implementiert

6. Tools, die zur Herstellung des Produkts verwendet wurden

--- Modellierung: Oxygen XML Editor 6, Visual Paradigm 6.2

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

--- Java Entwicklungsumgebung (IDE, Debugger): Eclipse 3.3

--- Java Profiler: J Profiler

--- Datenbankentwicklung: SQL-Navigator 6.0, NaturalDocs (Datenbank-Code-Dokumentation)

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

--- Changemanagement: JIRA 3.12 (Enhancement-, Bugtracker) sowie Subversion (Versionskontrolle)

7. Zweck und Einsatzbereich von Galileo

Galileo 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. Es 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),

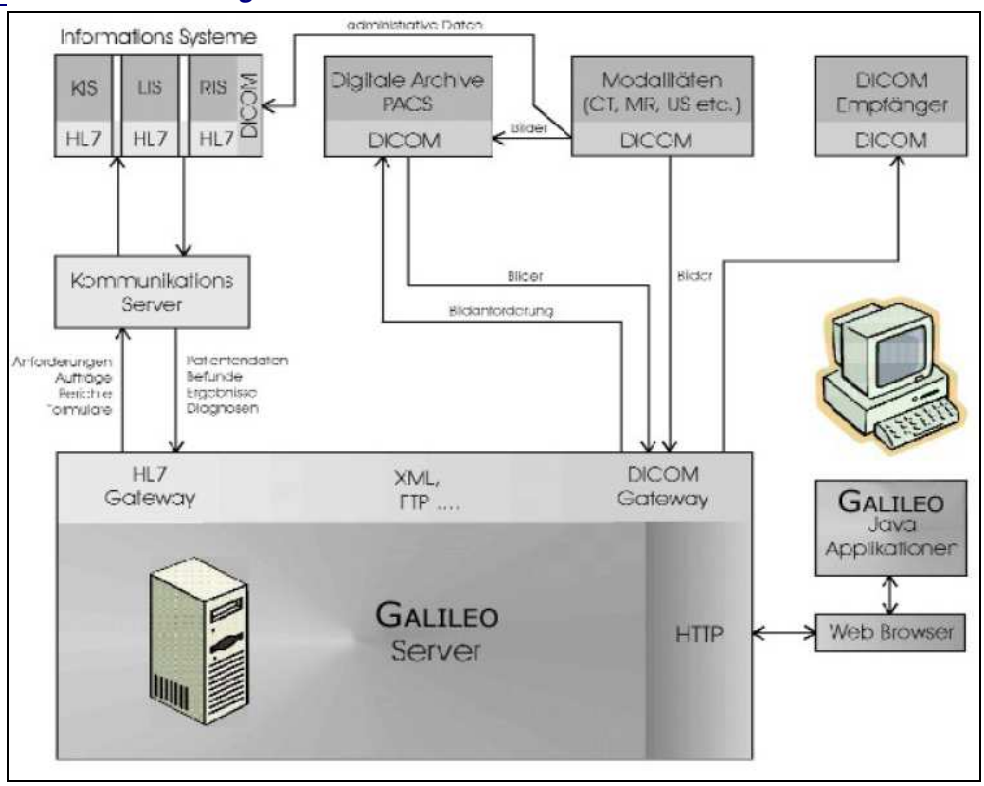
--- Erteilung von Aufträgen an Leistungsstellen (Radiologie, Labor),

--- 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 Prüfergebnisse

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 IT-Produkt den Datenschutz fördert

Das Produkt Galileo enthält folgende Datenschutz fördernde Funktionen:

--- Sperrung von Daten nach Abschluss der Behandlung:

Galileo ermöglicht das Sperren eines Falles nach Abschluss der Behandlung. Sofern der jeweilige Fall ggf. wieder benötigt wird, kann der Fall wieder entsperrt werden. Hierfür ist eine Begründung anzugeben, die zusammen mit Benutzer und Zeitpunkt protokolliert wird.

--- 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.

--- Vorschlagliste und Löschfunktion von Altdaten:

Der Sicherheitsbeauftragte kann sich unter Verwendung eines Filters Daten von einem bestimmten Mindestalter anzeigen lassen (10 Jahre, 20 Jahre,...). Hier hat er die Möglichkeit, gezielt einzelne Daten oder auch alle angezeigten Daten nach erneuter Bestätigung zu löschen.

Des Weiteren wird die Pförtnersperre nach Aussage des Herstellers in Form eines VIP-Merkmals wieder in die Software integriert werden, so dass dem Benutzer die Auskunftseinschränkung für einen Patienten sofort deutlich angezeigt wird.