Sicherheitsprotokolle bei der Anwendung von HL7

Kjeld Engel
Bernd Blobel
Peter Pharow

eHealth Competence Center Regensburg
Klinikum der Universität Regensburg

eHealth Competence Center
Regensburg

Einleitung

- Medizinische und administrative Daten sind auf unterschiedliche Art und Weise sensitive Daten
- Kommunikation ist nur unter Anwendung entsprechender Datenschutz- und Datensicherheitsmaßnahmen zulässig
- Detaillierte Sicherheits- und Transportaspekte wurden im HL7-Standard lang nur informativ geregelt
- Zwei Grundprinzipien der für HL7 entwickelten Sicherheitslösungen:
  - Übertragung gesicherter Mitteilungen in unsicheren Netzen (secure messages)
  - Übertragung ungesicherter Mitteilungen durch einen sicheren Kanal (secure channel)
- Sicherheitsservices für nicht sicherheitsbewußte Anwendungen (secure channels) in unteren Schichten des ISO-OSI-Modells wurden bewusst aus dem Standard ausgeklammert, da HL7 ein Layer-7-Protokoll ist

HL7-Sicherheitsprotokolle und -projekte

- HL7 SIG Secure White Paper
- Health Level Seven Security Services Framework: Basics, Fundamentals, Glossary
- Standard Guide for EDI (HL7) Communications Security
- Standard Guide for Implementing EDI (HL7) Communications Security
- Secure HL7 Transactions using Internet Mail (Internet Draft, EDIINT Working Group)
- Security Audit and Access Accountability Message: XML Data Definitions for Healthcare Applications (RFC 3881)
- HL7 ebXML Transport Specification
- Role-based Access Control Project

Standard Guide for EDI (HL7) Communications Security &
Standard Guide for Implementing EDI (HL7) Communications Security

- allgemeine Bedrohungs- und Risikoanalyse medizinischer Informationssysteme
- Definition von Sicherheitsdiensten zur Befriedigung der Sicherheitserfordernisse für EDI-Security über Use Cases
- Sicherheitsmechanismen für Kommunikationssicherheit lassen sich in zwei Hauptgruppen von Sicherheitsdiensten einordnen
  - Sicherung der zu übertragenden Information im Sinne der Ende-zu-Ende-Sicherheit
  - Sicherung des Übertragungsweges

Standard Guide for EDI (HL7) Communications Security &
Standard Guide for Implementing EDI (HL7) Communications Security

- Das spezifizierte offene Framework für HL7-Sicherheitskonzepte berücksichtigt ausschließlich Standards und garantiert auf diese Weise Interoperabilität
- Für die Nachrichten-Sicherheit werden sowohl sicheres Mailing als auch sicherer File Transfer praktisch eingesetzt
- Sichere Übertragungswege werden durch Protokoll-Suiten wie SSL, TLS und IPv6 garantiert

Secure HL7 Transactions using Internet Mail

- Weitere Lösung für sichere Kommunikation
- Dokument beschreibt eine Spezifikation für sichere EDI-Transaktionen für HL7, die auch als IETF-Spezifikation verfügbar ist
- Beschreibt, wie HL7-Nachrichten unter Nutzung von E-Mail gesendet werden können
- Entscheidender Punkt ist das Konzept der Verbindlichkeit und der Unbestreitbarkeit für eine EDI-Transaktion

RFC 3881

- RFC 3881 definiert das Format von Daten sowie das minimale Set von Attributen, welche für Sicherheits-Audits in Anwendungssystemen im Gesundheitswesen erforderlich sind
- Format ist dabei als XML-Schema definiert: Empfehlung für Entwickler von Standards für das Gesundheitswesen und Anwendungs-Designer
- Arbeit verdichtet verschiedene vorliegende Dokumente zum Sicherheits-Audit von Gesundheitsdaten
- Zur Gewährleistung des Datenschutzes und der Sicherheit in automatisierten Systemen müssen Daten gesammelt werden
  - Daten müssen durch Verwaltungspersonal geprüft werden, um nachzuweisen, dass diese Gesundheitsdaten in Übereinstimmung mit den Datensicherheitsanforderungen der Gesundheitsversorger genutzt werden, und um die Verantwortlichkeit für die Datennutzung festzustellen
- Daten beinhalten Records: wer greift auf die Gesundheitsdaten zu, wann, für welche Aktivitäten, von wo, welche Patienten-Records sind beteiligt

HL7 ebXML Transport Specification

- ebXML ist eine Spezifikation für Nachrichten-Kommunikation in XML
- Ziel: Unterstützung des sicheren und flexiblen Transports zum Austausch von HL7-Nachrichten zwischen Nachrichtenübermittlungsschnittstellen oder ebXML Message Service Handlers
- Transport bezieht sich auf HL7-Inhalt, -Nachrichten und -Dokumente über eine Anzahl verschiedener Lower Level Transports
- Protokoll unterstützt optional weitere wesentliche Merkmale
- Wird das Protokoll in Verbindung mit einem zertifikat-basierten TLS oder SSL TCP/IP Lower Level Transport verwendet, stellt es eine stabile, sichere und authentisierte Kommunikations-Infrastruktur zum Austausch von HL7-Nachrichten zwischen Organisationen zur Verfügung

RBAC-Projekt

- Role Engineering Projekt
- Spezifikation von Zugriffserlaubnissen für verschiedene Szenarios, aufgeschlüsselt auf rollenspezifische Transaktionen
- Wegen der Policy-Abhängigkeit der Spezifikationen können diese nicht in andere Policy-Domänen exportiert werden
- Spezifikation basiert auf ISO TS 22600 und ISO TS 21298

Healthcare Scenario Roadmap Maps

Work Tasks

Pharmacist

- Pharmacist, Apothecary
- Pharmacist, Clinical

Physician

- Chiropractor
- Homeopath
- MD/Allopath
- Naturopath
- Osteopath
- Pathologist
- Psychiatrist
- Radiologist

ASTM E1986 Roles	Order Entry	New/Change/Discontinue Laboratory Order	New/Change/Discontinue Radiology Order	New/Renew/Change/Discontinue/Refill Outps	New/Change/Discontinue Inpatient Medicatio	New/Change/Discontinue Diet Order	New/Change/Discontinue Consult Order	New/Change/Discontinue Nursing Order	New/Change/Discontinue Standing Order(s)	New/Change/Discontinue Verbal and Telepho	Sign Order(s)	Requires Order Co-Sign	Co-Sign Order(s)	Review Documentation	Review Patient Testing Reports	Review Chief Complaint	Review Medical History	Review Existing Order(s)	Review Patient Medications	Review Prescription Costing Information	Review Vital Signs/Patient Measurements	Patient Identification and Lookup	Review Patient or Disease-Specific Clinical Guidelines	Review Alerts	Review Current Directory of Provider Information	Review Mental Health Record	Perform Documentation	New/Edit/Addend/Sign Progress Notes	Requires Progress Notes Co-Sign	Co-Sign Progress Notes	New/Edit/Addend Progress Note Comment (non-clin data e.g. "No Show	New/Edit/Addend/Sign Patient Education	Requires Patient Education Co-Sign	Co-Sign Patient Education	New/Edit/Addend/Sign History and Physical	Requires History and Physical Co-Sign	Co-Sign History and Physical	New/Edit/Addend/Sign Consultation Findings	Requires Consultation Findings Co-Sign	Co-Sign Consultation Findings	New/Edit/Addend/Sign Surgical Report	Requires Surgical Report Co-Sign	Co-Sign Surgical Report
Licensed Health Care Providers																																										
Nurse	x	x	x	o	o	x	x	o	x	o	o	o	o	o	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	x	o	x	x	o	x	x
Nurse Practitioner (NP)		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Nurse Midwife (NM)		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Clinical Nurse Specialist (CNS)		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Clinical Registered Nurse Anesthetist (CRNA)		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Registered Nurse (RN)		x	x	x	x	x	x	x	x	x	x	x	o	o		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	x	x	o	x	o	o	o	o	o	o	o
Licensed Vocational Nurse (LVN)/Licensed Practical Nurse		x	x	o	o	x	x	o	x	o	o	o	o	o		x	x	x	x	x	x	x	x	x	x	x	o		x	o	o	x	x	o	o	o	o	o	o	o	o	o
Pharmacist	x	x	o	x	x	o	o	o	x	x	x	o	o	o	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	o	o	o	o	o	o	o
Pharmacist, Apothecary		x	o	x	x	o	o	o	x	x	x	o	o	o		x	x	x	x	x	x	x	x	x	x	x	o		x	o	o	o	x	o	x	o	o	o	o	o	o	o
Pharmacist, Clinical		x	o	x	x	o	x	o	x	x	x	o	o	o		x	x	x	x	x	x	x	x	x	x	x	o		x	o	o	o	x	o	x	o	o	o	o	o	o	o
Physician	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	x	o	x	x	o	x	x
Chiropractor		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Homeopath		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
MD/Allopath		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	x		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Naturopath		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Osteopath		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Pathologist		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Psychiatrist		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	x		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Radiologist		x	x	x	x	x	x	x	x	x	x	x	o	x		x	x	x	x	x	x	x	x	x	x	x	o		x	o	x	o	x	o	x	x	o	x	x	o	o	x
Physician Assistant (PA)	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	x	o	x	x	o	x	x
Psychologist	x	x	x	o	x	x	o	o	o	o	o	o	o	x	x	x	x	x	x	x	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	o	o	o	o	o	o	o
Speech Pathologist	x	o	o	o	o	x	o	o	o	o	o	o	o	x	x	x	x	x	x	o	x	x	x	x	x	x	o	x	x	o	o	o	x	o	x	o	o	o	o	o	o	o
Technician	x	o	o	o	o	o	o	o	o	o	o	o	o	x	x	x	x	x	o	x	x	x	x	x	x	x	o	x	x	o	o	o	o	o	o	o	o	o	o	o	o	o
Laboratory Technician		x	o	o	o	o	o	o	o	o	o	o	o		x	x	x	x	o	x	x	x	x	x	x	o		x	o	o	x	x	o	o	o	o	o	o	o	o	o	o
Radiology Technician		o	x	o	o	o	o	o	o	o	o	o	o		x	x	x	x	o	x	x	x	x	x	x	o		x	o	o	x	x	o	o	o	o	o	o	o	o	o	o

ISO/TS 22600 “Health informatics – Privilege management and access control”

- ISO 22600: "Privilege management and access control“; Sicherheits-Standard
- Ursprünglich in CEN vorbereitet und – den Schwerpunkt auf Privilege Management legend – vollständig überarbeitet in ISO
- Definiert Dienste für Privilege Management und Access Control, die für die Kommunikation und Nutzung von verteilten Gesundheitsinformationen über Domain- und Sicherheitsgrenze hinweg erforderlich sind
- Führt Principles ein und spezifiziert Dienste, die für das Management von Rechten und Access Control benötigt werden
- Spezifiziert notwendige komponentenbasierte Konzepte und soll deren technische Implementation unterstützen
- Spezifiziert nicht die Nutzung dieser Konzepte in spezifischen klinischen Prozessketten

ISO/TS 22600-1:2006

- Health informatics - Privilege management and access control - Part 1: Overview and policy management

- Current stage: 60.60 (Publication stage: International Standard published)
- Stage date: 2006-07-24

- Intended to support the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems
- Supports collaboration between several authorization managers that may operate over organizational and policy borders

ISO/TS 22600-2:2006

- Health informatics - Privilege management and access control - Part 2: Formal models

- Current stage: 60.60 (Publication stage: International Standard published)
- Stage date: 2006-07-24

- Introduces the underlying paradigm of formal high level models for architectural components based on ISO/IEC 10746
- In that context, the Domain Model, the Document Model, the Policy Model, the Role Model, the Authorization Model, the Delegation Model, the Control Model and the Access Control Model are introduced

ISO/TS 22600 Teil 3

- Health informatics - Privilege management and access control - Part 3: Implementations

- Not yet published

- Provides examples for the formal models of part 2
- Adaptation ASN.1 to XML should be considered
- Two emphases of the contents: the bridge to formal models and the implementation on basis of meta-languages and tools
- Existing specifications should be used
- The data are usable for administration by structural and organisational roles (MAC model as pate)
- The data also based on special applications (DAC model)
- Both parts are role-related, both are role-based access control models (RBAC)

ISO/TS 21298 “Health informatics – Structural and functional roles”

- Normvorlage aus PMAC-Standard 22600 herausgelöst, um die Rollenbeschreibungen auch für andere Anwendungen verwenden zu können
- Grundsätzlich hohe Akzeptanz für die PMAC-Normen
- In dieser Spezifikation werden die unterschiedlichen Rollen beschrieben:
  - allgemein
  - klassisch (mit Attributen, die gemanagt werden)
  - detaillierte Rollenbschreibungen
    - strukturelle Rollen
    - funktionelle Rollen

Ergebnisse

- Einige der vorgestellten Protokolle führten zu Implementationen, die sich jahrelang im praktischen Einsatz bewährten
- So führten einige der beschriebenen Lösungen zum ersten wirklich sicheren und durchgängig auf Standards basierenden Gesundheitsnetz: zum ONCONET Sachsen-Anhalt
- In Australien kam eine Anwendung zum Einsatz, die unter Berücksichtigung vom EDIINT-Draft entwickelt worden ist
- Implementierungen von ISO 22600

Diskussion

- Zur Sicherung der Kommunikation zwischen Einrichtungen des Gesundheitswesens auf der Basis von HL7 wurden sichere Übertragungsprotokolle auf der Anwendungsebene spezifiziert und implementiert
- Außerdem wurden Protokolle zur Kommunikation mittels sicherer Kanäle definiert und demonstriert
- Diese Spezifikationen sind domänenunspezifisch und können durch analoge Produkte ersetzt werden
- Mit dem Übergang zum Architekturparadigma und damit dem Übergang zur Berücksichtigung der Funktion der Applikationen und der Verwendung der Daten als Charakteristikum semantischer Interoperabilität werden künftig auch Anwendungssicherheitsdienste im HL7-Standard Einzug halten

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Kontakt:

Kjeld Engel
eHealth Competence Center Regensburg
Franz-Josef-Strauss-Allee 11
93053 Regensburg
E-Mail: kjeld.engel@klinik.uni-regensburg.de
Tel.: 0941/944-6768
Fax: 0941/944-6766