## Sicherheitsprotokolle bei der Anwendung von HL7

Engel K, Blobel B, Pharow P
*eHealth Competence Center, Klinikum der Universität Regensburg, Deutschland*
*kjeld.engel@eh-cc.de*

**Einleitung und Fragestellung** Medizinische und administrative Daten sind auf unterschiedliche Art und Weise sensitive Daten. Deswegen können sie nur unter Anwendung entsprechender Datenschutz- und Datensicherheitsmaßnahmen kommuniziert werden. Detaillierte Sicherheits- und Transportaspekte sind im HL7-Standard allenfalls im Kontext der Infrastrukturdienste behandelt. Die Kommunikationssicherheit wurde bewusst aus dem Standard ausgeklammert, da HL7 ein Layer-7-Protokoll ist. Die Wahl und Umsetzung von Mechanismen insbesondere zur Kommunikationssicherheit gehört in die darunter liegenden Schichten des ISO-OSI-Modells.
Die für HL7 entwickelten Sicherheitslösungen, welche die charakteristische offene Architektur von HL7 gewährleisten sollen, beruhen auf zwei Grundprinzipien: zum einen können gesicherte Mitteilungen in unsicheren Netzen (secure messages), und zum anderen können ungesicherte Mitteilungen durch einen sicheren Kanal (secure channel) übertragen werden [1].
In diesem Beitrag sollen einige der wichtigsten entwickelten Sicherheitsprotokolle bei der Anwendung von HL7 vorgestellt werden.
**Material und Methoden** Eine der ersten Abhandlungen zu HL7-Sicherheitsaspekten war das Health Level Seven Security Services Framework - das so genannte HL7 SIG Secure White Paper, das von mehreren HL7-Mitgliedern verfasst worden ist. Diese Arbeit sollte über den damals aktuellen Stand von Sicherheitslösungen im Gesundheitswesen informieren und Empfehlungen für HL7 geben [2]. Diese Version wurde von den Autoren erheblich erweitert und in 2 Teile sowie ein Glossar untergliedert [3, 4].
Auf der Basis der Ergebnisse europäischer Forschungsprojekte wurde von den Autoren im Anschluss an diese Erweiterung eine allgemeine Bedrohungs- und Risikoanalyse medizinischer Informationssysteme durchgeführt. Mit Hilfe eines allgemeinen Sicherheits-Modells und des daraus abgeleiteten Klassifikations-Schemas wurden die Sicherheitsdienste zur Befriedigung der Sicherheitserfordernisse für EDI-Security - und damit auch für HL7-Sicherheitskonzepte - über Use Cases definiert. Die oben angesprochenen Sicherheitsmechanismen für Kommunikationssicherheit lassen sich in zwei Haupgruppen von Sicherheitsdiensten einordnen, wobei eine Gruppe die zu übertragende Information im Sinne der Ende-zu-Ende-Sicherheit sichert. Diese Dienste laufen auf der Anwendungsschicht des ISO-OSI-Modells der Kommunikation zwischen offenen Systemen. Die andere Gruppe realisiert (insbesondere auf der Transportschicht des ISO-OSI-Modells) die Sicherung des Übertragungsweges. Das spezifizierte offene Framework für HL7-Sicherheitskonzepte berücksichtigt ausschließlich Standards und garantiert auf diese Weise Interoperabilität. Beide Sicherheitsmechnismen wurden für die Kommunikationssicherheit implementiert. Für die Nachrichten-Sicherheit wurden insbesondere sicheres Mailing als auch sicherer File Transfer praktisch eingesetzt. Sichere Übertragungswege werden durch Protokoll-Suiten wie SSL, TLS und IPv6 garantiert [5, 6].
Eine weitere Lösung für sichere Kommunikation wurde mit dem Internet Draft der EDIINT Working Group erarbeitet. Dieses Dokument beschreibt die Eignung der Standardisierungsbemühungen für sichere EDI-Transaktionen für HL7, und wie HL7-Nachrichten unter Nutzung von E-Mail gesendet werden können. Ein entscheidender Punkt ist das Konzept der Verbindlichkeit und der Unbestreitbarkeit für eine EDI-Transaktion [7].
Der RFC 3881 definiert das Format von Daten sowie das minimale Set von Attributen, welche für Sicherheits-Audits in Anwendungssystemen im Gesundheitswesen erforderlich sind. Das Format ist dabei als XML-Schema definiert, das als Empfehlung für Entwickler von Standards für das Gesundheitswesen und Anwendungs-Designer gedacht ist. Die Arbeit verdichtet verschiedene vorhergende Dokumente zum Sicherheits-Audit von Gesundheitsdaten. Zur Gewährleistung des Datenschutzes und der Sicherheit in automatisierten Systemen müssen Daten gesammelt werden. Diese 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. Die Daten beinhalten Records, wer auf die Gesundheitsdaten zugreift, wann, für welche Aktivitäten, von wo, und welche Patienten-Records beteiligt sind [8].
ebXML ist eine Spezifikation für Nachrichten-Kommunikation in XML, die durch das OASIS-Konsortium (www.oasis-open.org) entwickelt worden ist. Das Ziel der HL7 ebXML Transport Specification ist es, den sicheren und flexiblen Transport zum Austausch von HL7-Nachrichten zwischen Nachrichtenübermittlungsschnittstellen oder ebXML Message Service Handlers zu unterstützen. Der Transport bezieht sich auf HL7-Inhalt, -Nachrichten und -Dokumente über eine Anzahl verschiedener Lower Level Transports wie z.B. TCP/IP, HTML und SMTP. Dieses Protokoll unterstützt optional weitere wesentliche Merkmale, z.B. Duplicate Message Handling, Reliable Messaging, Message Routing, Sequencing und Digitale Signaturen. Wird das Protokoll in Verbindung mit einem zertifikat-basierten TLS (Transport Layer Security) oder SSL (Secure Sockets Layer) TCP/IP Lower Level Transport verwendet, stellt es eine stabile, sichere und authentisierte Kommunikations-Infrastruktur zum Austausch von HL7-Nachrichten (sowohl v2 als auch v3) zwischen Organisationen zur Verfügung [9].
Im Rahmen des Übergangs zu einem Architekturstandard gilt es für HL7, auch Anwendungssicherheitsdienste zu spezifizieren. Hier sind insbesondere das Privilege Management, die Autorisierung und die Zugriffskontrolle zu nennen. Im Role-based Access Control Project wurden strukturelle und functionelle Rollen für die Domäne der USA definiert. Die Lösung basiert auf den ISO Standards ISO 21298 “Health informatics – Structural and functional roles” sowie ISO 22600 “Health informatics – Privilege management and access control” [10].
**Ergebnisse** Einige der vorgestellten Protokolle führten zu Implementationen, die sich jahrelang im praktischen Einsatz bewährten. So wurden die in [3-6] beschriebenen Lösungen im ersten wirklich sicheren und durchgängig auf Standards basierenden Gesundheitsnetz: zum ONCONET Sachsen-Anhalt, das den eingebundenen Ärzten in sicherer Weise u.a. die Meldung von patientenbezogenen onkologischen Fakten an das Magdeburger Klinische Krebsregister, die Abfrage von statistischen Daten über ihre Patienten sowie den Austausch patientenbezogener medizinischer Daten (z.B. Arztbriefe, Befunde, CT-Bilder) zwischen ihnen und mitbehandelnden Kollegen und Einrichtungen ermöglichte. Damit wurde eine wichtige Grundlage für die verzahnte, hochqualitative Versorgung krebskranker Patienten geschaffen. In Australien kam eine Anwendung zum Einsatz, die unter Berücksichtigung von [7] entwickelt worden ist.
**Diskussion** Zur Sicherung der Kommunikation zwischen Einrichtungen des Gesundheitswesens auf der Basis des HL7-Standards wurden sichere Übertragungsprotokolle auf der Anwendungsebene spezifiziert und implementiert, die die vertrauenswürdige Kommunikation zwischen sicherheitsbewussten Applikationen realisieren. Außerdem wurden Protokolle zur Kommunikation mittels sicherer Kanäle definiert und demonstriert. Obwohl diese Spezifikationen informativ im HL7-Standard definiert wurden, sind sie domänenunspezifisch und können durch analoge Produkte ersetzt werden (z.B. SMIME, SSL, TLS). 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.

### Literatur

[1] Heitmann KU, Blobel B, Dudeck J. HL7 – Kommunikationsstandrad in der Medizin. Köln: Verlag Alexander Mönch; 1999.
[2] Kratz M, Humenn P, Tucker M, Nolte M, Wagner S, Seppala G, Shadrow G, Wilson W, Auton S. Health Level Seven Security Services Framework (HL7 SIG Secure White Paper). Juni, 1999.
[3] Blobel B, Engel K, Pharow P, Spiegel V. HL7 Secure Transactions, Special Interest Group: Health Level Seven Security Services Framework, Part 1: Basics of HL7 Security. Juli, 1999.
[4] Blobel B, Engel K, Pharow P, Spiegel V. HL7 Secure Transactions, Special Interest Group: Health Level Seven Security Services Framework, Part 2: Fundamentals of HL7 Security. Juli, 1999.
[5] Blobel B, Spiegel V, Pharow P, Engel K, Krohn R. Standard Guide for EDI (HL7) Communications Security. In: Allaert FA, Blobel B, Louwerse K and Barber B (Edrs.): Security Standards for Healthcare Information Systems - A Perspective from the EU ISIS MEDSEC Project. Series Studies in Health Technology and Informatics, Vol. 69. Amsterdam: IOS Press; 2002: 153-182.

[6] Blobel B, Spiegel V, Pharow P, Engel K, Krohn R. Standard Guide for Implementing EDI (HL7) Communications Security. In: Allaert FA, Blobel B, Louwerse K and Barber B (Edrs.): Security Standards for Healthcare Information Systems - A Perspective from the EU ISIS MEDSEC Project. Series Studies in Health Technology and Informatics, Vol. 69. Amsterdam: IOS Press; 2002: 183-220.

[7] Schadow G, Tucker M, Rishel W. Secure HL7 Transactions using Internet Mail (draft-ietf-ediint-hl7). Internet Draft (EDIINT Working Group). 4. Februar, 1999.
http://aurora.rg.iupui.edu/~schadow/HL7Mime.html.

[8] Marshall G. Security Audit and Access Accountability Message: XML Data Definitions for Healthcare Applications. RFC 3881. September, 2004.
http://www.ietf.org/rfc/rfc3881.txt?number=3881.

[9] HL7 ebXML Transport Specification.
Info: http://www.hl7.org/Press/20040427b.asp

[10] ISO: http://www.iso.org