7 Secure HL7 Transactions Using Internet Mail (Internet Draft)

Gunther SCHADOW¹, Mark TUCKER¹ and Wes RISHEL²
¹The Regenstrief Institute, Indianapolis, U.S.; ²Wes Rishel Consulting, San Francisco, U.S.

edited by Kjeld ENGEL
Otto-von-Guericke University, Medical Informatics Department, Magdeburg, Germany

7.1 Abstract

The document describes the applicability of the Internet standardisation efforts on secure electronic data interchange (EDI) transactions for Health Level-7 (HL7), an EDI standard for Healthcare used world-wide [1].

The document heavily relies on the work in progress by the IETF EDIINT working group. It is in most parts a restatement of the EDIINTs requirements document and application statement 1 (AS#1) tailored to the needs of the HL7 audience. The authors tried to make the document as self consistent as possible. The goal is to give to the reader who is not a security or Internet standards expert enough foundational and detail information to enable him to build communication software that complies to the Internet standards.

Even though the authors rely on and promote the respective Internet standards and drafts, they did not withstand from commenting on and criticising the work where they see upcoming problems in use with HL7 or other EDI protocols that have not been in the initial focus of the EDIINT working group. The authors make suggestions to add parameters to the specification of the MIME type for EDI messages in RFC 1767 in order to enhance functionality. The authors give use cases for a larger subset of disposition types and modifiers of message disposition notifications.

One key issue where the document goes beyond the current EDIINT drafts is the concept of non-repudiation of commitment to an EDI transaction. Secure EDI transactions should be regarded as “distributed contracts,” i.e. not only the sending and receiving of single messages should be non-refutable but also the connection between messages interchanges.

In anticipation of this requirement HL7 usually requires a response message to be sent to acknowledge every transaction. The authors therefore have the requirement to securely couple an EDI response message to its request message. Given the current shape of RFC 1767 this is generally possible only if a response message is coupled with an MDN receipt and the combination of both signed by the responder. The document describes a protocol to bundle MDN and response that uses the MIME multi-part/related content type in RFC 2112.
7.2 Scope

The document contains five categorically different kinds of information:

- A description of the document, its intent, scope, and limitations
- Background information on Internet standards and the relevant technologies
- Specific recommendations for how to apply various Internet standards and draft standards to transmit HL7 messages to meet the stated requirements
- Some general discussion of how systems and organisations may choose to implement these recommendations
- An example that shows the different steps and work products of a complete secure HL7 transaction

7.3 Limitations

The Recommendation is limited to exchanging authentic and private HL7 messages among organisations. Although one technique that it employs is called digital "signature," the reader should not expect to find an approach for authentically determining the individual person who signs orders, reports, or other information that might be contained within an HL7 message.

The mechanisms stated in the document are based on cryptographic technologies that use a pair of cryptographic keys, which allows them not only to encrypt messages but also to securely identify the sender and receiver of a message. These mechanisms are threatened by a number of means including, but not limited to:

- Failure of the communicating partners to exchange their mutual public keys in a trustworthy manner,
- Electronic attacks on systems that store those keys,
- Unscrupulous or careless current or former employees who deal with organisational keys,
- Attacks on the information systems that produce or consume the actual messages or handle them at intermediate points before they are encrypted,
- Unscrupulous current or former employees who get or alter the clear text messages.

Furthermore, the techniques here do nothing to guarantee that a required message is ever initially sent. Organisations that are obligated to send messages using these techniques must employ their own means to ensure that their applications generate and send the initial HL7 message of an exchange and that the appropriate reply is received in the appropriate time frame.

Considerable work is underway to enhance the distribution of authentic keys. This work includes the establishment of trusted authorities who can dispense digital "certificates"-combinations of a name and a key that are signed by the authority. These certificates provide assurance that the public keys are associated with that entity they claim. The document does not require a trusted authority for dispensing certificates. It is assumed that the communicating parties will exchange certificates and other credentials in face-to-face meetings, by fax, or using other means that they deem sufficiently secure.

As the work is based on Internet-drafts and is itself a draft, implementers must assume that there will be changes in the published formats and protocol before the document and the standards upon which it relies are final. This would not preclude implementations
among specific trading partners where they agreed to update their implementations to the final versions.

7.4 Relevant remarks

The recommendation describes a stack of lower layer protocols (LLP) that can be used to transfer HL7 messages reliably and securely. While focusing on Internet e-mail, the recommendation will be applicable for other message exchange protocols with minimal changes. This flexibility is possible because of a modular approach, where modules of higher levels depend on modules of lower levels. If lower-level modules are exchanged in order to cater to other transport protocols, the higher level modules need not be touched.

From lowest to highest level the modules are:

- Internet in general
- Internet e-mail
- MIME (multipurpose Internet mail extensions)
- Security
- Message disposition notifications
- MIME-based secure EDI

7.5 Security: General Issues

The authors describe the following general issues of security:

- Security Services
  - Integrity
  - Authenticity
  - Authorisation
  - Confidentiality
  - Non-repudiation

- Mechanisms
  - Cryptographic Algorithms
    - Message Integrity Check
    - Symmetric and Asymmetric Ciphers
  - Cryptographic Protocols
    - Digital Envelope
    - Digital Signature
    - Certificates
    - Non-repudiation

7.6 Security: Implementation Issues

The authors describe the following implementation issues of security:

- MIME Security in General
Chapter 7

- Integrity, Authenticity and Non-repudiation of Origin: Multi-part/Signed
- Confidentiality: Multi-part/Encrypted
- Non-repudiation of Receipt: Multi-part/Report
- Non-repudiation of Commitment: Multi-part/Related

- MIME-PGP
  - Overview of PGP-Services
  - Digital Signature
  - Digital Envelope
  - Certificates

- S/MIME
  - Overview of PKCS-Services
  - Digital Signature
  - Digital Envelope
  - Certificates

7.7 A Detailed Example – Necessary Steps

This section gives a detailed example of an HL7 transaction over secure e-mail. It shows all relevant steps in building a secure e-mail from an HL7 request message, the reverse process that is applied by the responder to unwrap this HL7 message and the process of building and decomposing the response e-mail message.

1. Generation of the HL7 request message according to rules of the application program:

```
MSH|~~~4|OR|DR.SCHADOW.LAB|TUCKER-GENERAL|... | ORM|RQ-001-01|P|2.2<CR>
PID| |08157411 | |Doe"John"|19690219 |M |<CR>
PV1| |D | |0123"SCHADOW"GUHTHER; | | | | | | | |12 |<CR>
ORC|NW|12345 | |<CR>
OBR|S12345; | | | |19971226175948 |7"ML | |BLBV |<CR>
ORC|CH|12345-1 | |F|12345 |<CR>
OBR|12345-1 | |5383-5"THYROID MICROSOMAL AB"LN |<CR>
ORC|CH|12345-2 | |F|12345 |<CR>
OBR|12345-2 | |5381-9"THYREOGLOBULIN AB"LN |<CR>
ORC|CH|12345-3 | |F|12345 |<CR>
OBR|12345-3 | |5385-0"THYREOTROPIN RECEPTOR AB"LN |<CR>
```

Figure 10: HL7 request message

2. This message is to be wrapped into a MIME-EDI entity:
3. The message shall be signed; **a signature must be calculated over canonical text**:

```
BEGIN PGP MESSAGE
Version: 2.6.3la

iQBVAwUANKPor3g+w2Pf lLsNAQH/iwIAnqYzaL0qB2hqItqniIilD3 jpf 3+9ku
52tL

END PGP MESSAGE
```

Figure 12: Signature and signed message
Chapter 7

4. The next step is to wrap the signed material into a digital envelope:

```
Content-Type: multipart/encrypted; <CR><LF>
  boundary="encbound"; protocol="application/pgp-encrypted"<CR><LF>
<CR><LF>
  --encbound<CR><LF>
Content-Type: application/pgp-encrypted<CR><LF>
<CR><LF>
Version: 1 <CR><LF>
<CR><LF>
  --encbound<CR><LF>
```

Figure 13: Message with digital envelope

5. This MIME entity is now pre-pended by RFC 882 e-mail headers and sent to the receiver:

```
Received: (from oes@schadow.practice.net) by edi.practice.net<CR><LF>
  id SA01629; Fri, 26 Dec 1997 16:26:06 +0100<CR><LF>
From: oes@schadow.practice.net<CR><LF>
To: labStucker-general.edu<CR><LF>
Message-ID: <edi883157166.1607@schadow.practice.net><CR><LF>
Subject: New order<CR><LF>
```

```
Figure 13: Message with digital envelope
```
Figure 14: Message with e-mail header

6. The receiver unwraps the message from the digital envelope to yield the multipart/signed MIME entity:

```
protocol = "application/pgp-signature";
+ sigalg = "pgp-md5";
+ boundary = "sigbound";

BEGIN PGP MESSAGE:---------------------
Version: 2.6.31

-----BEGIN PGP MESSAGE-----
Version: 2.6.31

```

Figure 15: Unwrapped message
7. After the HL7 message has been unwrapped from the MIME-EDI container, it is fed to the HL7 application of the receiver:

```
MSH|"\&|LAB|TUCKER-GENERAL|OE|DR.SCHADOW|...|ORR|RP-001-831|F|2.2<CR>
MSA|AA|RQ-001-001|ORDER_ACCEPTED|<CR>
PID|47110815|08157411|Doe,John|<CR>
PVI|0123"SCHADOW"GUNTHER|<CR>
ORC|12345|54321|SC<CR>
```

Figure 16: Received message fed to HL7

The signature must be validated over the message text. When the authenticity is successfully validated, the data can be stored into a non-repudiation log.

8. MDN receipt:

```
Content-Type: multipart/report;report-type="disposition-notification";boundary="repbound"
--repbound
Content-Type: text/plain
your message has been processed
--repbound
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit

Reporting-UA: lab.tucker-general.edu; EDISend 1.0
Final-Recipient: rfc822;request@lab.tucker-general.edu
Original-Message-Id: <edi883157166.1607@schadow.practice.net>
Disposition: automatic-action/MDN-sent-automatically; processed
Received-content-MIC: 54ee0a559b7a922dbeb76f538c949dbfecedeb3,sha1
--repbound--
```

Figure 17: MDN receipt

The HL7 application also signals to the e-mail agent that the processing was successful. For the generation of a complete message disposition notification it is necessary to calculate a message integrity check over the same text that was subject to signature by the initiator.

9. The MDN receipt is bundled with the HL7 application-level response message in a special `multipart/related` MIME entity:
Again, the HL7 message has been wrapped into a MIME-EDI container with quoted-printable transfer encoding.

10. The signature that is applied over the bundle of MDN receipt and HL7 response performs non-repudiation of receipt of the HL7 request message, non-repudiation of origin of the HL7 reply message, and non-repudiation of commitment to the transaction implied by the given pair of HL7 messages:

---

**Figure 18:** MDN receipt and HL7 response message

---
11. The response and its signature are packed into a multi-part/signed MIME entity:

Figure 19: Non-repudiation of receipt message

Figure 20: Response message and response signature
12. Finally, the signed response is encrypted and sent as an RFC 822 e-mail message back to the authenticated sender of the request message:

```
From: labOtucker - general.edu<CR><LF>
To: oe@eschadow.practice.net<CR><LF>
Date: Fri. 26 Dec 1997 18:26:11 +0100<CR><LF>
Message-Id: <edi883157166.1407@eschadow.practice.net><CR><LF>
In-Reply-To: <edi883157166.1407@eschadow.practice.net><CR><LF>
Subject: Re: New order<CR><LF>
MIME-Version: 1.0<CR><LF>

Content-Type: multipart/encrypted; boundary="encbound";<CR><LF>
   protocol="application/pgp-encrypted"<CR><LF>
<CR><LF>
---encbound<CR><LF>
Content-Type: application/pgp-encrypted<CR><LF>
<CR><LF>
Version: 1<CR><LF>
<CR><LF>
---encbound<CR><LF>
Content-Type: application/octet-stream<CR><LF>
<CR><LF>
-----BEGIN PGP MESSAGE-----<CR><LF>
Version: 2.6.31a<CR><LF>
hWdeUYD79+UowBAf0eLhV0xPGF9EQbe10tcqnQSWXbDEw+/81bnHQ2BGA<CR><LF>
9BSax0BOiyf+g9m71S9Y3rZkZ0McHn4Yne72cpgAAbdnTQqY6XrA1vm<CR><LF>

Figure 21: Message in e-mail format back
```

Back at the sender, this message is decrypted and checked for authenticity.

### 7.8 Architectural and Operational Considerations

The previous sections provide a roadmap of the relevant Internet standards, background information on encryption and the MIME e-mail formats, and detailed specifications of messages and how their content should be created. They are directed towards the implementers of the e-mail handling programs. This section examines a series of operational and architectural issues. It illustrates how the pieces can be fit together with existing TCP/IP based HL7 applications routers and firewalls. It further shows one way to provide the journalising function necessary to disprove attempts to repudiate the sending and processing of a message. It discusses some specific issues in HL7 transaction design that are related to the e-mail medium. Finally, it touches on issues in negotiating interfaces when the sending and receiving systems are not operated by the same organisation.

This section is not normative; its purpose is simply to illuminate issues that must be considered in applying the material of the previous section. As an example the process structure of the e-mail handling machine is described:
Chapter 7

Figure 22: Directing incoming email to a program that processes HL7 messages

In this architectural model, the e-mail handling software will run on a designated machine for an institution. Incoming EDI e-mail messages will be directed to that machine. Processes on that machine will decode the e-mail, recover the original HL7 message, and then transmit via TCP/IP to pre-existing HL7 applications that expect conventional TCP communication.

Figure 23: HL7 using e-mail passing firewall through gatekeeping router

7.9 References and Bibliography (Informative)