*Medical Informatics Europe '99*
*P. Kokol et al. (Eds.)*
*IOS Press, 1999*

# Java-based Framework for the Secure Distribution of Electronic Medical Records

Alwyn Goh
USM Computer Sciences
11800 Penang, Malaysia
*Email: alwyn@cs.usm.my*

**Abstract:** In this paper, we present a Java-based framework for the processing, storage and delivery of Electronic Medical Records (EMR). The choice of Java as a developmental and operational environment ensures operability over a wide-range of client-side platforms, with our on-going work emphasising migration towards Extensible Markup Language (XML) capable Web browser clients. Telemedicine in support of womb-to-tomb healthcare as articulated by the Multimedia Supercorridor (MSC) Telemedicine initiative—which motivated this project—will require high-volume data exchange over an insecure public-access Wide Area Network (WAN), thereby requiring a hybrid cryptosystem with both symmetric and asymmetric components. Our prototype framework features a pre-transaction authentication and key negotiation sequence which can be readily modified for client-side environments ranging from Web browsers without local storage capability to workstations with serial connectivity to a tamper-proof device, and also for point-to-multipoint transaction processes.

**Keywords:** Electronic Medical Record, Transaction Processing, Java Client-Server, Authentication, Secure Transactions

## 1 Introduction

MSC-based Telemedicine conceptualises various *information-enriched* products and services [1] for the healthcare community and general population. A wide cross-section of public healthcare facilities—major hospitals down to local clinics—will be eventually provided with WAN connectivity, through which the application-layer services will be delivered. MSC-based Telemedicine has the declared intention of initiating a paradigm shift in healthcare, in which systems and services currently designed to deliver a *curative* response would would henceforth be focussed on generating and implementing a *preventive* Lifetime Health Plan (LHP) based on exhaustive Lifetime Health Record (LHR) documentation. It bears pointing out that healthcare is one of the most basic social services rendered to the general population, hence an effective system would have the potential of contributing directly to an improvement in the quality of life.

The specific healthcare products and services articulated in the Concept Request for Proposal (CRFP) [2] documents have in common the requirement for a *standard* cross-system transaction-enabling framework. In this paper we describe an object-based transaction system designed to enable the automatic exchange of messages constructed and interpreted in compliance with a well-established and internationally recognised standard. When work on this project started in 1997, our choice for the messaging format was the United Nations (UN) sanctioned Electronic Data Interchange for Administration,

Commerce and Transportation (EDIFACT) standard. The usage of EDIFACT for healthcare messaging has been widely explored [3, 4, 5, 6]; but can be considered to be somewhat out-of-place in the context of Personal Computers (PC), thin-clients and the World Wide Web (WWW). The combination of EDI-like documents represented using Extensible Markup Language (XML) [7] looks to be particularly promising as a developmental basis, this will be also discussed in the following section.

## 2 Document Representation and Manipulation

The EDIFACT standard actually specifies both syntax and semantics [8], the former of which is designed to facilitate representation of arbitrarily complex relationships between various data elements organised in terms of the following hierarchy:-

- *Interchanges*: composed of Messages
- *Messages*: composed of Segment Groups and Segments
- *Segment Groups*: composed Segment Groups and Segments
- *Segments*: composed of Composite Data Elements and Data Elements
- *Composite Data Elements*: composed of Data Elements

with individual objects being either conditional or mandatory. Multiple instances of a particular object are also allowed subject to specified repetition factors. An EDIFACT interchange can be visualised as a progressively nested sequence of linked-lists, as shown in Figure 1 below:-

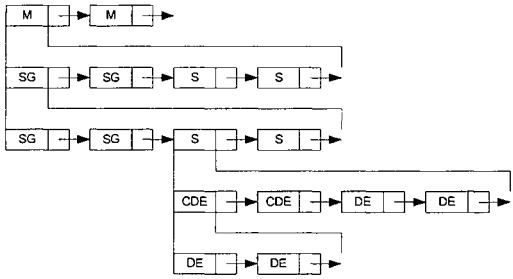


Fig 1: Typical EDIFACT Object

which can be mapped into textual form through usage of simple construction rules. EDIFACT semantics are encapsulated at the message level, with each message type intended for usage within a certain application-layer context. The UN maintains a periodically updated message directory [8], with almost 200 message types representing a broad range of administrative and commercial transactions.

The coding/decoding of EDIFACT documents, their storage within a Relational DBMS (RDMS) and their interactive representation to an enduser is discussed in [5] and [6]. The representation issue is particularly complex, and required the application of GUI design principles strongly reflecting the hierarchical linked-list structure of the transaction object. EDIFACT objects can be intuitively manipulated using nested panels and scroll-panels, with positional layout dictated by type-specific structuring features. For example, the two adjacent scroll-panels in Figure 2.1 represent segment groups GR1 and GR2 within a MEDPID message. GR2— which contains nested segment groups GR3, GR4 and GR5—is the more complex of the two, hence the inclusion of nested panels as shown in Figure 2.2. Transaction objects can be created, viewed or edited; with legitimate operations (ie adding a new segment) controlled using object-specific parameters. Most GUI elements are

intuitive, ie the usage of button-set {*Previous*, *Next*, *New*, *Delete*} to navigate segments within a segment group and pull-down menus for enumerated responses. Java applications for any EDIFACT message-type can be therefore be straightforwardly assembled from a relatively small set of generic GUI object modules.

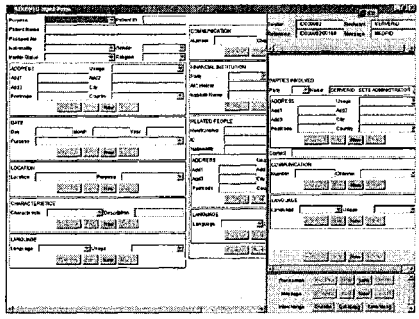

Fig 2.1: Object-based GUI Layout

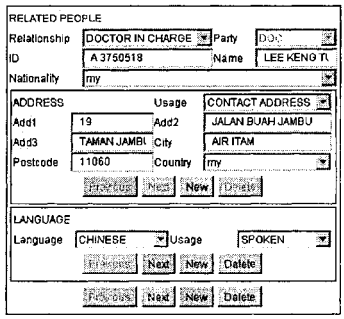


Fig 2.2: GUI Linking and Nesting

The size and complexity of the resulting GUI applications precludes implementation as a Web-downloaded applet functioning within a browser-client. An alternative approach would be to re-use the object construction syntax for presentation, this is in fact the main motivation in our ongoing investigation into XML-based encoding. On the most basic level, XML [7] is a generalisation of HTML in that user-defined tags are allowed. In the XML-model, documents are parsed for *validity* with respect some semantically meaningful document-type template, which is an extension of the syntactical *well-formedness* allowed in HTML. Document parse trees can subsequently be manipulated as objects for database storage, re-transmission or information processing. Human-readability is handled via the Extensible Stylesheet Language (XSL), which is intended to allow the mapping of well-formed documents into some *native* display format ie HTML. HTML-based presentation also allows for the embedding of multimedia and programmed elements (ie Java applets) into *rich* data models, thereby combining the structural capabilities of XML with the transparent object-integrability of HTML. Java-based functionality would be especially important for browser-based *thin* clients, which is a de facto architectural requirement to ensure the widespread accessibility critical for the success of MSC Telemedicine. The overall configuration of such a system would resemble Figure 3 below.

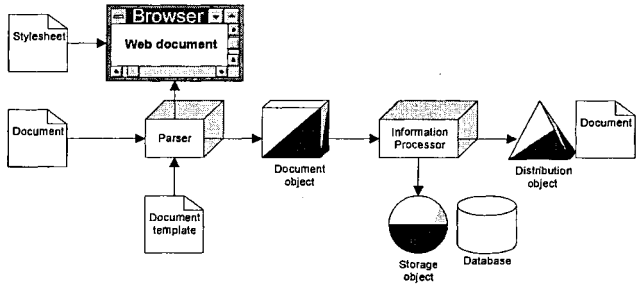


Fig 3: Transactional Architecture Based on Document-Object Modelling

## 3 Node Authentication and Inter-Node Security

Traditional EDI assumes the existence of a secure network environment over which transactions occur, with easy enforceability due to the strictly controlled number of network-connected terminals. Such assumptions would clearly not apply to any system designed to facilitate message distribution over a public-access WAN ie the Internet. The necessity for incorporating security and authentication components adds considerably to the operational overhead, nevertheless this is unavoidable given the legal and ethical sensitivities [10] pertaining to EMR-related information.

The transaction documents discussed in the previous section would be fairly large (even after compression) for practical EDI applications; hence the necessity for bulk encryption using some symmetric cipher, preferably one more secure than Data Encryption Standard (DES) and faster than Triple-DES (T-DES). Our system features the International Data Encryption Algorithm (IDEA) block cipher in Cipher Block Chaining (CBC) mode, thereby ensuring only one plaintext-ciphertext pair per message per session-key. This was deemed a sensible precaution given that a single session would typically be used for the exchange of multiple EDI messages, each of which contribute a large number of 64-bit ciphertext blocks. Such a scheme would, however, require session-key negotiation prior to the commencement of message exchange.

In most transactions, the roles of service provider and consumer are highly context-sensitive and frequently interchangeable within a particular session; hence the basic unacceptability of key-management protocols in which a single transaction participant selects the session-key. Alternatives—ie Needham-Schroeder (Kerberos), Neumann-Stubblebine or Woo-Lam—in which a trusted third party determines the session-key are unattractive due to the transactional overhead placed on a limited number of nodes within the transactional community. In addition, operational support of point-to-multipoint transactional modes would also require that the key-management protocol be extensible to accomodate multi-party computation and reducible for client-side platforms without local storage. All these requirements can be satisfied extending the Secure Remote Password (SRP) protocol [11] to enable bidirectional node-to-node (as opposed unidirectional client-to-server) authentication and mutual key-negotiation. The resultant protocol sequence enhances *standard* Diffie-Hellman (DH) by incorporating:-

- *Permanent and session-specific key-pairs*: the former enabling formulation of an elegantly combining authentication and key-negotiation sequence
- *Challenge-response sequence*: to enable detection of man-in-the-middle attacks, which is a well-known vulnerability associated with standard DH
- *Zero-knowledge proofs*: to verify correct conclusion of the key-negotiation sequence without potentially damaging information exposure

thereby providing security equivalent to the station-to-station [12] and other DH variants supported by the Secure Socket Layer (SSL) framework without the necessity for explicit signature verification during key-negotiation.

All transactions within the trading community can be conceptualised as occurring between a pair of nodes (initiator A and respondant B), with the involvement of a trusted Certificate Authority (CA) to distribute signed discrete logarithm public-keys, with our implementation featuring Digital Signature Algorithm (DSA) in particular. Successful authentication and key-negotiation as described in Table 1 below assumes prior downloading of public-keys associated with all other transaction nodes. Nodes A and B respectively own key-pair ($\alpha$, $A = g^{\alpha} \bmod p$) and ($\beta$, $B = g^{\beta} \bmod p$), with each node possessing the public-key associated with the other. All private-keys are assumed to be

securely stored, ideally on a smartcard capable of performing computations without key exposure. Note the community-wide usage of modular basis p and exponent g, which results in more economical cryptosystem management compared with authentication mechanisms based on Rivest-Shamir-Adleman (RSA) algorithm. The pre-transaction handshaking then proceeds as follows:-

Table 1: Authentication and Key-Negotiation Sequence

| *Step* | *Party* | *Computation* | |
|---|---|---|---|
| 1 | Node A | Generate u, λ<br>$w = g^{u} \bmod p$<br>Transmit (w, λ) | (u, w) = A session key-pair<br>λ = A-to-B challenge parameter |
| 2 | Node B | Generate x, μ<br>$y = g^{x} \bmod p$<br>$\chi = \left(wA^{\mu}\right)^{(x+\lambda\beta)} \bmod p$<br>$k = H(\chi)$<br>$M_1 = H(w, y, k)$<br>Transmit (y, μ, $M_1$) | (x, y) = B session key-pair<br>μ = B-to-A challenge parameter<br>Note $\chi = g^{(u+\alpha\mu)(x+\lambda\beta)} \bmod p$<br>k = symmetric session-key |
| 3 | Node A | $\chi = \left(yB^{\lambda}\right)^{(u+\mu\alpha)} \bmod p$<br>$k = H(\chi)$<br>Verify $M_1$<br>$M_2 = H(w, y, k, M_1)$<br>Transmit $M_2$ | Note $\chi = g^{(x+\beta\lambda)(u+\mu\alpha)} \bmod p$ |
| 4 | Node B | Verify $M_2$ | |

with Secure Hash Algorithm (SHA) used as the one-way hash function. Successful key-negotiation allows resultant message traffic M to be secured as $E_k(M, sign(M))$, with sign(M) being the DSA signature and k the unique session-key. The above-described mechanism allows for fine-tuned access control regulation—with each server maintaining a tabulation of permitted transactions associated with any given client—thereby allowing for protocol termination after step (1) in the event of an insufficiently privileged client (A) or an overloaded server (B).

## 4 Concluding Remarks

It is probably not an exaggeration to claim that MSC Telemedicine constitutes one the boldest policy initiatives with regards the widespread application of advanced technology in healthcare. An operational system implemented along the lines discussed in this paper would enjoy significant advantages over both *traditional* EDI-like and ad hoc Web-based transaction processing. The generic nature of open-standard object documents also makes it conceptually straightforward to incorporate commercial and governmental transactions, the only requirement being the definition of appropriate messaging specifications and the setting-up of additional transaction servers. Progressive evolution towards browser-client architectures would enable service delivery via public-access Internet terminals and home

PCs, thereby opening up MSC Telemedicine—and related commercial services ie sale of pharmaceuticals—to much larger population segments.

The initial implementation of MSC Telemedicine will, due to financial constraints, be scaled-down compared to the original CRFP conceptualisation Nevertheless even a *skeleton* solution—designed with sufficient allowances for future *plug-in* components—would have a dramatic impact on both administrative and clinical practices. The type of system proposed in this paper are in fact extremely amenable to such a roll-out strategy, with browser-clients completely eliminating the need for previously installed components and administratively-expensive version control.

One should also note that none of the systems and services envisaged in this paper are inherently bandwidth-intensive or latency-sensitive. It is therefore not unreasonable to anticipate the development and deployment of *lightweight* client-server systems intended to deliver healthcare and commercial services over generic public-access WANs, as opposed dedicated high-bandwidth environments. Such systems would, in fact, be ideal in that large-scale deployment could commence without significant investments in endpoint hardware and network infrastructure.

**References**


[1] Govt of Malaysia. *CRFP Telemedicine Flagship Applications: Personalised Health Information (PHI), Continuing Medical Education (CME), Teleconsultation and Lifetime Health Plan.* (1997)

[2] SSR Abidi, A Goh & Y Zaharin. *Telemedicine and Medical Informatics in the Multimedia Super Corridor: The Malaysian Vision.* Proc World Congress on Medical Informatics: Seoul, Korea. (1997)

[3] K Pramataris, G Doukidis, G Giaglis & J Raptakis. *The EUROMIDES EDI Prototype System.* Information Exchange for Medical Devices (Eds N Pallikarakis, N Anselmann & A Pernice): IOS Press. (1996)

[4] JL Monteagudo. *Data Exchange in the European Pharmacovigilance.* Information Exchange for Medical Devices (Eds N Pallikarakis, N Anselmann & A Pernice): IOS Press. (1996)

[5] DCL Ngo. *A Generic EDI Application Software.* Proc Conf on Research and Development in Computer Science (REDECS): Penang, Malaysia. (1997)

[6] A Goh, SW Leong & LC Tai. *Secure Transaction Processing Framework for Medical Informatics and Electronic Commerce in the Multimedia Super-Corridor.* Congress of Scientific and Technical Organisations in Malaysia (COSTAM): Penang, Malaysia. (1998)

[7] M Hogan. *XML and the Internet: Driving the Future of EDI.* http://www.poet.com/edi.html (1998)

[8] UN Economic Commision for Europe. *UN Rules and Directories for EDIFACT.* http://www.unece.org/trade/untdid/welcom1.htm (1998)

[9] World Wide Web Consortium (W3C). *XML Version 1.0.* http://www.w3.org/TR/PR-xml.html (1997)

[10] N Gaunt & F Roger-France. *Security of the Electronic Healthcare Record: Professional and Ethical Implications.* Towards Security in Medical Telematics (Eds B Barber, A Treacher & K Louwerse): IOS Press. (1994)

[11] Thomas Wu. *The Secure Remote Password Protocol.* http://srp.stanford.edu/srp/ (1998)

[12] W Diffie, PC van Oorschot and MJ Wiener. *Authentication and Authenticated Key Exchanges.* Design, Codes and Cryptography. (1992)