NPL Report CISE 7/96

June 1996

Secure-EDI Workshop Report

Stephen Hehir
Information Systems Engineering Branch
Centre for Mechanical and Optical Technology
National Physical Laboratory
Teddington
Middlesex
United Kingdom
TW11 0LW

ABSTRACT

A description of the proceedings of a one day workshop to discuss the security aspects of EDI is given. There are summaries of the main points made by the guest speakers and questions put by the audience. A list of attendees is included.

NPL CISE 7/96

ISSN 1361-407X

National Physical Laboratory
Teddington Middlesex UK TW11 0LW

Approved on behalf of the Managing Director of NPL
by Dr. David Rayner, Branch Head, Information Systems Engineering (CMOT)

Secure-EDI Workshop Report

Prepared by Stephen Hehir, NPL.

Date: March 25th 1996
Location: DTI Conference Centre, Victoria Street

INTRODUCTION

The Techniques for High Integrity Section (THIS) at NPL recently conducted a research programme in the area of application of the Strict Conformance Testing Methodology to Secure Electronic Data Interchange (EDI) standards. Contact with EDI translator manufacturers in the UK during that programme highlighted a reluctance to take up the secure EDIFACT and X.435 standards. It became clear that the UK industry needed some encouragement since foreign competitors appear to be preparing for the secure EDI market ahead of the standards.

The aim of this workshop was therefore to present the current state of the relevant standards, to hear from users and developers on their preferred solutions, and to attempt to uncover perceived barriers to the take up of standards.

The workshop was organised on behalf of the DTI and MoD by NPL and consisted of four sessions chaired by Bronia Szczygiel of NPL. There were approximately 50 attendees representing users, developers, standards makers and test houses.

This report contains a summary of the presentations and discussions of the day. Unfortunately many of those asking questions and making comments from the floor did not identify themselves and therefore no identification is made in this report.

1 WELCOME

Nigel Hickson, Communications and Information Industries Division, DTI

Nigel Hickson welcomed all attendees to the workshop and said that applications of EDI (and its applied security) were of strong interest to the DTI. The issues surrounding Secure EDI were regarded seriously by the DTI at the highest level. The key was not the technology itself but what it can do to further the business interests of the UK. It was of paramount importance to win the trust of the Users - otherwise the Users will not convert to using EDI.

Nigel stated that among the aims of the Workshop were finding answers to the question of why EDI Security was not being taken up and to find out what could be done to foster the use of applications which implemented EDI Security.

2 STANDARDS IN SECURE EDIFACT

Terry Dosdale, Chair of UN/EDIFACT and Vice-Chair ECA Security Advisory Group.

Terry Dosdale began his presentation with a description of the threats to be considered in an EDI scenario. After this he gave a summary of the services which counter those threats in Secure EDIFACT such as Digital Signature, Hash Functions and Encryption.

Terry then gave a breakdown of commercial and government sectors use of secure EDI, according to those services which were most necessary to them. Included in this list were Customs, the tourist industry, Insurance, NHS and others.

The EDIFACT security structure was then described with details of the secure headers and trailers, AUTACK and KEYMAN messages. Version 4 of the EDIFACT standard has been submitted for approval and should be released later this year. This version incorporates the security documents in their latest form.

The work of the SJWG was briefly described before moving on to a comparison of EDIFACT and X.400 Security showing that EDIFACT provides a more general and comprehensive security solution.

Developers are not implementing full EDIFACT security and the market at the moment seems to consist of only a few customers, though these customers may be large (for example, customs, Mod etc). Faster progress in Standards and the provision of Certification Authorities would stimulate new applications.

There followed a period of discussion on the issues raised, summarised below.

Q. Is there any legal framework for questions of liability?

A. A statement of liability can (and should) be built into interchange agreements but the difficulty is that one must assume that one is liable unless liability is specifically excluded. It is therefore important to protect oneself from possible litigation.

Q. How do the Americans fit in with the International Standard?

A. They have gone through a similar process with their standards (X.12) as we have with EDIFACT. The EDIFACT standards have been developed through the UN, which includes the Americans, so they have been involved in that development also. More work may need to be done to make the various Standards truly international.

Q. Is ISO 9735 v.4 compatible with v.3?

A. The original version was not compatible but following comments from users and others an attempt has now been made to address this concern. Repeating composites are an exception but compatibility can be acheived.

Q. If we did have TTP services how would that fit into present EDIFACT work?

A. TTP will be required for Certification. Some issues might cause problems.

Q. When can we expect to cope with binary data?

A. That has been a difficult issue in EDIFACT. Some work may be approved in September 1996 but it may not satisfy the needs of users.

Q. Next millenium, perhaps? EDI may go the way of Esperanto.

C. A comment was made from the floor that standards in general are not implementable.

3 THE DEVELOPERS VIEW

Alan Fidler *Kewill-Xetal Systems*

AF gave a description of Kewill's work in suppling many branches of the MOD, DRA and local authorities with EDI systems. One of the primary objectives was to reduce costs and in some cases these had been reduced to less than 5p per message.

User concerns were confidentiaity and access control. But these worries are largely unfounded. For example there are simple steps one could take to prevent hacking through modems. E.g. Install gateways, Outgoing BT line, Air Bridges, Batch Modems and others.

Q. Are your systems based on EDIFACT?

A. Yes.

Q. Do you use Secure EDI messaging?

A. No, that is not an issue for us at the moment.

Q. What about Integrity?

A. The market Kewill operates in is not asking for it. We would be happy to provide it if our users were asking for it.

Q. Can you give some idea of the cost of transactions?

A. The Navy now use EDI on about 45 % of their transactions (by value) and estimate that it has saved 3/4 million pounds.

C. A comment was made that hacking through telecoms is very difficult and clerical errors are far more likely.

The following presentation was made later in the workshop but is reported here for consistency of presentation.

Colin Ravenhill. *Wick Hill Business Communications.*

Wick Hill has won a contract to supply Racal Network Services with *Tax Exchange* - an EDI and X.400 software package for the Inland Revenue's Self-Assessment scheme.

Colin Ravenhill said that there is a definite requirement for Secure EDI giving automated facilities. However, Service Providers need to be trusted and there must be good quality assurance and auditing trails.

The requirement was for EDI, with full encryption, to run over an X.400 Network. Colin stated that, although there are export problems with respect to ecnryption, this was not seen to be a restriction for most Inland Revenue work.

The solution proposed by Wick Hill was to use PGP (licensed), which is RSA-based. The Key Distribution problem was solved by sending the private key in plaintext with a verification of the fingerprint by phone. This authenticates the key.

Hence the solution is fully automated, but with checks. The point is not to build secure EDIFACT but to build secure systems.

Q. Why PGP?

A. It is secure enough to prevent casual eavesdropping and it is easy to use. Significant resources would be required to break it.

Q. Since the Inland Revenue is a Government Department does this mean that the DTI is endorsing the use of PGP?

A. In the absence of Nigel Hickson, Bronia Szczygiel responded that the DTI was not in a position to endorse particular products.

Q. Is there a level of liability connected to the use of PGP?

A. There is no legal threshold, only a Duty of Care.

4 THE USERS VIEW

William List *Kingswell Partnership*

Willie List began by stating that when changing to EDI a business has to clarify its requirements. These will primarily centre on accounting records and deciding what controls need to be enforced - especially corrections. The requirements should be decided in the light of a proper risk analysis.

Willie discussed the use of codes for information and the great importance to be attached to checking mistakes in these numbers which are often meaningless to a

The areas of security which must be considered are:
physical, organisational/procedural and the presence of logical flaws.

Often the financial risks of loss of confidentiality on one transaction is very low but on a network passing a large number of transactions one begins to see the need for firewalls and other security. When assessing the risks it must be ensured that consequential loss (i.e. loss to other customers) and loss of reputation must be considered.

Splitting the responsibilities and functions of staff is one traditional way of providing protection and this is as suitable for electronic commerce as it is for paper commerce.

The controlled use of message authorisation codes and acknowledgement messages is critical for financial transactions.

A business must ensure that it is protected against fraud, theft, error, loss & collapse.

Q. The Electronic Trade Payments scheme has not been a success? Comments?

A. SWIFT was secure but it has not been used much. But limits on the extent of usage may have been the problem.

Q. Will Nat West use Secure EDIFACT in the future?

A. Not Secure EDIFACT, customers have not asked for it. In our experience, confidentiality is not a critical issue in most transactions.

5 TESTING SECURE EDI APPLICATIONS

Stephen Hehir *National Physical Laboratory*

Stephen Hehir gave a description of Strict Conformance Testing showing a breakdown of the Abstract Test Suite into three parts: the Security Target, Test Purposes and the Test Case Behaviour.

Particular emphasis was given to the Security Target in which Security Objectives were defined together with an analysis of Threats against those Objectives. A list of Services which provide protection against those Threats is taken from the information in the Standard.

Examples of tests from the two recently developed ATS for Secure EDIFACT and Secure X.435 were given. This demonstrated that the test suites reflect the level of detail of the Standard to which they are directly related. Details of the forms of messages to be transmitted are part of the preparatory data for running the test suite.

It was concluded that such a method for testing is useful for providing a low level of assurance at cheap cost. For a higher level of assurance, other aspects of evaluation are required.

human being. Other important checks are authorisations and checks on a purchasing order itself.

It should be noted that once an organisation starts to use EDI it may become wholly dependent on that system with former procedures completely forgotten. Therefore the internal controls must be thoroughly thought out to provide the necessary inbuilt protections for the business.

Q. Is a secure transmission system seen as important in this application area?

A. Yes, definitely.

Q. Should there not be overnight alerting for systems going down?

A. Yes, but that ought to be a standard procedure for protecting the business.

C. It has been found to be the case that computer Authorisations may need 2 independent programs to be fully safe.

Peter Shuttleworth *MOD Secure EDI & the MOD*

Peter began by saying that the main driving force for the MOD to implement EDI has been the reduction of Procurement Costs and, as always with a large organisation, changing the bureaucracy on which the organisation relies requires a lot of effort.

For this purpose it is necessary to develop a proper Business Strategy, working out Business Process changes, deciding on what Information Systems need to be set up, and generally building the proper infra-structure.

It should be realised that getting EDI implemented into such a large organisation needs careful planning.

The main requirement for such a set-up is security with low cost. It has been estimated that an average for the MOD is that security accounts for 25% of the cost of a contract. There is a Secure Open Systems Technology Demonstrator Programme within the MoD aimed at demonstrating a secure messaging system. Most large developers (including Novell and Microsoft) are involved in the manufacturers forum for the TDP.

The use of secure forms of EDI must be taken into account in the Security Policy. For the MOD such a system must continue to be useful in times of war and be totally compatible with National Security generally.

Roger Gate National Westminster Bank (Electronic Cash Management Sales)

The National Westminster Bank can be classed as both users and developers. Roger began by stating that it is not possible to have total security and usability. Amongst other factors one must take into account, the chance of occurrence, cost of solution and an assessment of risk. The solution must be affordable, practical, have aesthetic appeal, meet legal requirements and the impact on other users must be allowed for.

Verifying the test suite can be done by several methods - one of which is to run the suite against a real implementation. NPL would be pleased to hear of real implementations from the Developers in the audience.

Q. If nothing is known about the implementation detail of some aspect e.g sequence numbers, how can a test be written for it?

A. The tests are written at the same level of abstraction as the standard and therefore this is not a problem. Implementation details are used to parameterise the test suite at the point where it is made executable.

Q. How do you ensure complete coverage?

A. Complete coverage is not possible since there are potentially a huge number of possible test cases. The security target guides the development of the test suite and therefore there is coverage of all security functionality to some degree. Evaluation requires only evidence of one test case per security mechanism. SCT gives far more than that.

Q. Are there plans to develop a Test Suite for transactions on the Internet?

A. No.

6 GENERAL DISCUSSION

There was only a brief general discussion. Some attendees suggested that the Internet would also be used for large transactions and that should be considered. It was also suggested that Standards are a problem in that they are progressing too slowly to be useful. It was felt by some participants that solutions would be market-led and that Standards might be those set by products rather than Standards Committees.

CONCLUSIONS

There were two overall impressions to be gained from the discussions at the workshop.

The first was that when implementing EDI or other forms of electronic commerce, security is an issue with many businesses. Organisations of many types are looking for ways to implement that security in a manner which is convenient and cheap.

The second was that while EDI was a common form of electronic commerce being used, security was not being implemented according to the Secure-EDIFACT standards but implemented in an ad hoc manner. There was a feeling that the progress of the Secure-EDIFACT Standard was too slow to be useful. In addition, some Developers said that they were not being asked for Secure-EDIFACT solutions and were content to provide security with lower-layer methods.

RECOMMENDATIONS

1. DTI should initiate a campaign, perhaps through the Electronic Commerce Association (ECA) to promote the take up of secure EDIFACT and possibly X.435.

2. User concerns regarding binary data and encipherment should be addressed and the solutions publicised.

3. Awareness raising activities which highlight the importance of secure communications should be a high priority.

4. Efforts should be made to converge to a common solution for Electronic Commerce to avoid future conflicts. Government can play an active role in this.

Names of Attendees for the Secure EDI Workshop ***(March 25th 1996)***

Company	*Name*	*No of Attendants*
Admiral	Paul Williams	1
Alliance & Leicester	JW Cave	2
	JArmstrong	
AVSI	Philip Holt	1
Axiom Services	Terry Dosdale	1
BACS	AM Seymour	1
Bank Relationship Consultancy	AR de Caux	2
	K Lillie	
Barclays Bank	R Kimber	1
BOC	DJ Phillips	1
British Gas	E. Stanley	1
BT	Ian Bramhill, Michael Doherty	2
BTG	Peter Hawkes	1
Bull Inform. Systems	Ian Barrett	1
Camelot Group PLC	Simon Royal	1
Datahealth	Lawrence Ratcliffe	1
Dept. of Transport	Terry Jones	1
DRA	Richard Shore	1
DSL	Steve Betts	1
DTI	Nigel Hickson	2
	Gordon Manning	
Hambros	Arthur Barton	1
HMSO	Robert Megroff	1
HSBC Holdings	CJ Simmons	2
	Neil Chantry	
ICL	Chris Taper	1
Kewill-Xetal Systems	David Cullis	1
Kingswell Partnership	William List	1
Lloyds TSB	WL Whittaker	1
Lond. School Economics	Peter Sommer	2
Midland Bank PLC	John Kerr	1
MOD	S. Cholerton	3
	D Bennison, Peter Shuttleworth	

Nat. West Bank	Roger Gate	1
NCC	Roger Rawlinson	1
NPL	Bronia Szczygiel	3
	S Hehir, G Kelly	
Origin (UK)	Tony Metcalfe	1
Perwill Group	Bill Pugsley	1
Radcliffe Hospital, Oxford	D Nurse, J Kaye	2
SAA Consultants	GP Gledhill	
Siemanns-Nixdorf	Alan Davies, John Ness	5
	Paul Hendon, Mike Brady	
	John Noonan	
Smith Sys. Eng	Dr. Glyn Carter	1
Standard Life Ass. Co.	Ian Hallworth	1
Syntegra	J Fishburn	1
TIS (UK)	AT Liddle	1
Wick Hill Business Comms	Phil Shea	1
Total		**55**