通信情報保護學會誌
第7卷 第3號, 1997. 9

EDI 정보보호 시스템의 구조 및 서비스 환경 분석

Analysis of Secure EDI System Architecture and Sevice Environment

이 정 현*, 윤 이 중*, 이 대 기*, 김 대 호*

요 약

매년 급증하고 있는 통신망을 이용한 EDI 서비스에서 정보보호 서비스의 제공은 필수적인 요소임에는 틀림없다. 이러한 전자문서를 통한 상거래시에 필수적인 정보보호 서비스를 제공하는 EDI 시스템을 SEDI(Secure EDI) 시스템이라 하며, 본 논문에서는 이 SEDI 시스템에서 제공하는 정보보호 서비스를 개발하고자 할 때 사용되는 프로토콜의 구조와 해당 포트 및 관련 오퍼레이션들과 이들 모듈들의 구성, 각 서비스 모듈들의 연관관계들을 분석하였다.

1. 서 론

통신망을 이용한 EDI(Electronic Data Interchange) 서비스의 이용률은 매년 급증하고 있으며 이와 더불어 교류되는 정보에 대한 보호 및 안전성에 대한 요구도 증가되고 있다. 주로 전자 상거래를 목적으로 사용하는 EDI에서는 정보의 불법 누출, 불법변경, 송수신자의 신원조작, 송수신 행위의 부인 등의 위협요소[1][2]가 크게 대두된다. EDI 시스템에서 이러한 위협요소에 대비하여 EDI에서 제공하여야 하는 정보보호 서비스에는 발신처 인증, 데이타 기밀성, 데이타 무결성, 부인봉쇄, 메세지 레이블링, 접근제어 등이 있다[1][3][4].

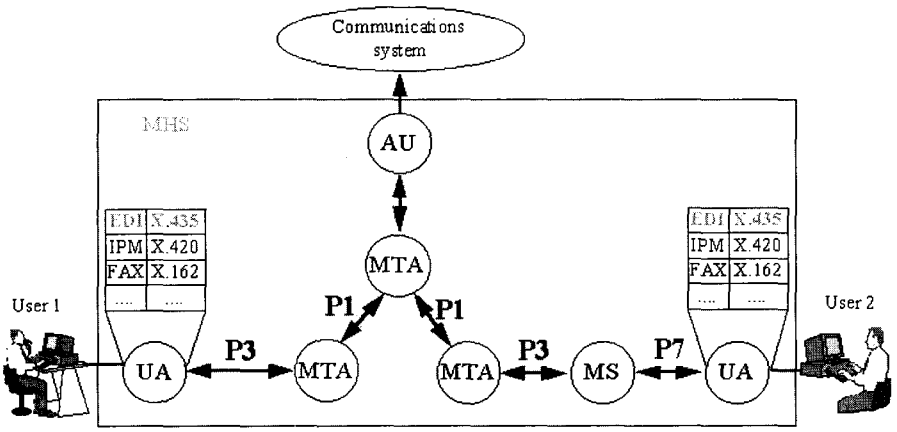
기존의 EDI 시스템에 정보보호 서비스 기능을 부가한 시스템을 SEDI(Secure EDI) 시스템이라 정의한다. 본 논문에서는 SEDI 시스템에서 사용되는 프로토콜들의 구조와 각 프로토콜에 관련한 포트들의 분석을 통하여 EDI 정보보호 서비스를 제공하기 위해 사용되는 해당 포트 및 오퍼레이션을 살펴보고자 한다.

본 논문의 2장에서 EDI 정보보호 서비스에 대하여 분석하였고, 3장에서는 P3 프로토콜 상에서의 정보보호 서비스 요구사항을, 4장에서는 P1 프로토콜 상에서의 정보보호 서비스 요구사항을, 5장에서는 P7 프로토콜상에서의 정보보호 서비스 요구사항을 분석하였으며, 6장에서는 SES 각 모듈들의 구성과 연관관계를 분석하였고, 7장에서 결론을 맺는다.

* 한국전자통신연구원

2. EDI 정보보호 서비스

EDI 시스템이란 MHS(Message Handling System)에서 UA(User Agent)가 처리하는 메세지의 Content 타입이 EDI인 시스템을 말하며, EDI에 관한 표준은 ITU-T X.435[5][6]에 정의되어 있다. 따라서 EDI 시스템에서 제공하는 정보보호 서비스는 크게 EDI의 기반인 MHS 정보보호 서비스[7]와 EDI 정보보호 서비스[6]로 나눌 수 있다. [그림 1]은 EDI 시스템과 기반이 되는 MHS와의 관계를 나타낸 것이다.



[그림 1] EDI와 MHS의 관계

ITU-T X.402에 정의되어 있는 MHS에 관련한 정보보호 서비스에는 크게 발신처 인증(Origin Authentication) 서비스, 안전한 액세스 관리(Secure Access Management) 서비스, 데이타 기밀성(Data Confidentiality) 서비스, 데이타 무결성(Data Integrity) 서비스, 부인봉쇄(Non-Repudiation) 서비스, 메세지 보안 레이블링(Message Security Labelling), 정보보호 관리(Security Management) 서비스를 들 수 있다[2][8].

또한 EDI 시스템에 관련한 정보보호 서비스에는 크게 EDIM 책임 인증(EDIM Responsibility Authentication) 서비스와 EDIM 책임 부인봉쇄(Non-Repudiation of EDIM Responsibility)를 들 수 있는 데[1][7], 이들 두 서비스의 차이점은 신뢰할수 있는 제삼자(trusted third party)의 존재 유무에 따른 분류이다.

3. P3 정보보호 서비스

3.1 MTS 시스템 모델

MHS시스템은 UA, MS(Message Store), MTA(Message Transfer Agent)의 컴포넌트들로 이루어져 있으며, store-and-forward 방식으로 사용자들간의 메세지들을 교환해 준다. 이러한 사용자들간의 메세지 전달을 제공하기 위해서는 반드시 MTS(Message Transfer System)를 통해서만 가능하다.

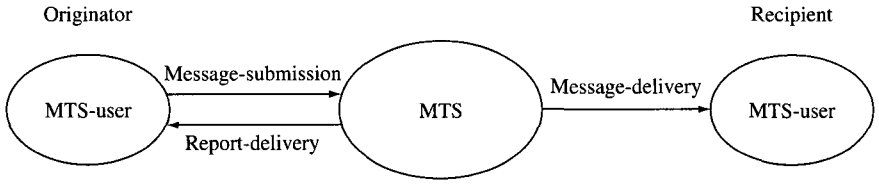
MTS란 하나 또는 그 이상의 MTA들의 집합을 말하며, MTS-user란 UA 또는 MS를 의미한다. 이 MTS와 MTS-user간에 사용되는 프로토콜을 P3 프로토콜이라 한다.

MTS는 내부 구조에 대한 참조없이 모든 동작행위가 기술가능한 객체(object)로 모델링되

고, MTS에 의해 제공되는 서비스는 포트(port)들을 통해 이용가능하다.

MTS에서 지원하는 포트에는 submission-port, delivery-port, administration-port가 있다.

[그림 2]는 MTS 의 시스템 모델을 나타낸 것이다.



[그림 2] MTS 시스템 모델

3.2 P3 정보보호 서비스 개요

P3 프로토콜 상에서의 MHS 서비스중 정보보호와 관련된 서비스를 P3 정보보호 서비스라 정의한다. 이 절에서는 P3 정보보호 서비스를 제공하기 위하여 다음과 같은 서비스들을 정의한다.

3.2.1 MTS Bind

MTS Bind는 MTS-user가 MTS와 association을 설정할때 또는 MTS가 MTS-user와 association을 설정할 수 있도록 하는 기능을 제공한다.

3.2.2 Submission Port

Message-submission 오퍼레이션은 MTS-user가 하나 이상의 수신 MTS-user들에 메세지가 전송 및 배달 될수 있도록 MTS에게 메세지를 제출하는 기능을 제공한다.

Probe-submission 오퍼레이션은 MTS-user가 하나 이상의 수신 MTS-user들에 메세지가 전송 및 배달 될수 있는지를 결정하기 위하여 MTS에게 probe를 제출하는 기능을 제공한다.

Submission-control 오퍼레이션은 MTS가 MTS-user들의 submission-port 사용 권한을 제어하는 기능을 제공한다.

3.2.3 Delivery Port

Message-delivery 오퍼레이션은 MTS가 MTS-user에게 메세지를 배달하는 기능을 제공한다.

Report-delivery 오퍼레이션은 MTS가 MTS-user에게 Message-submission 또는 Probe-submission 오퍼레이션에 따른 결과를 알려주는 기능을 한다. 즉, Message-submission의 경우에 있어서, Report-delivery 오퍼레이션은 제출된 메세지가 배달되었는지 안되었는지의 결과를 알려주고, Probe-submission의 경우에는 제출된 메세지가 배달될 수 있을지 없을지의 결과를 알려주는 기능을 제공한다.

Delivery-control 오퍼레이션은 MTS-user가 MTS의 delivery-port 사용 권한을 제어하는 기능을 제공한다.

3.2.4 Administration Port

Register 오퍼레이션은 메세지 배달과 관련하여 MTS가 관리하고 있는 MTS-user들의 장기간 사용하는 파라미터들을 MTS-user가 변

경할 수 있도록 하는 기능을 제공한다.

Change-credentials 오퍼레이션은 MTS-user가 MTS에게 혹은 MTS가 MTS-user에게 자신의 credentials을 변경할 수 있도록 하는 기능을 한다.

3.3 P3 정보보호 서비스 정의

3.3.1 MTS bind

MTS-bind는 association의 applicaton-context와 security-context상에서 상호 동작을 위한 MTS-user와 MTS의 credentials을 설정하는 것이다. bind시 송신측은 initiator-credentials, security-context를 수신측에 전달하고, 수신측에 이에 대한 결과로서 responder-credentials을 송신측에 전달한다. MTS-bind와 관련된 정보보호 아규먼트(security arguments)는 다음[표1]과 같다. 표에서 M은 필수항목(Mandatory), O는 선택항목(Optional), C는 조건항목(Conditional)을 의미한다.

[표 1] MTS-bind관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Initiator-credentials	M	8.1.1.1.2/X.411
	Security-context	O	8.1.1.1.3/X.411
Results	Responder-credentials	M	8.1.1.1.4/X.411

- Initiator-credentials
  initiator-credentials는 송신자의 신분을 인증하기 위해 수신자에 의해 사용된다. 이때, 단순 인증(simple authentication)이 사용되면, intiator-credentials는 단순히 initiator-name과 관련한 패스워드(password)로만 구성되고, 강한 인증(strong authentication)이 사용되면, initiator-credentials는 initiator-bind-token과 선택적으로 intiator-certificate로 구성된다. Initiator-bind-token의 타입은 bind-token이며, bind-token의 구조는 [그림 3]과 같다. 그림에서 [ ]은 선택항목을 의미한다. 또한, Initiator-certificate의 타입은 certificate이며, certificate의 구조는 [그림 4]와 같다.

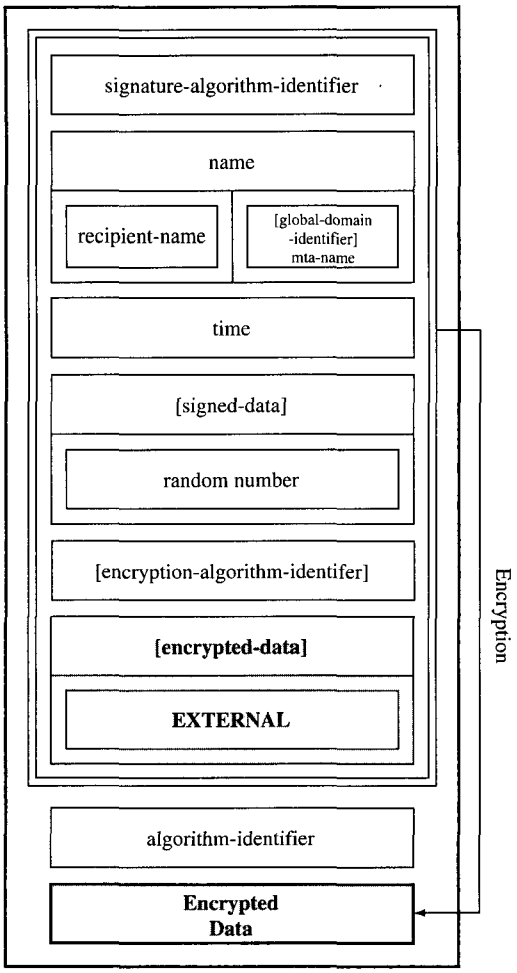
- Security-context
  security-context는 보안정책(security policy)에 따라 association할 동안에 MTS-user와 MTS사이에 발생할 수 있는 상호 동작의 sensitivity을 정의하는 하나 이상의 security-label들로 구성된다.

3.3.2 Submission Port

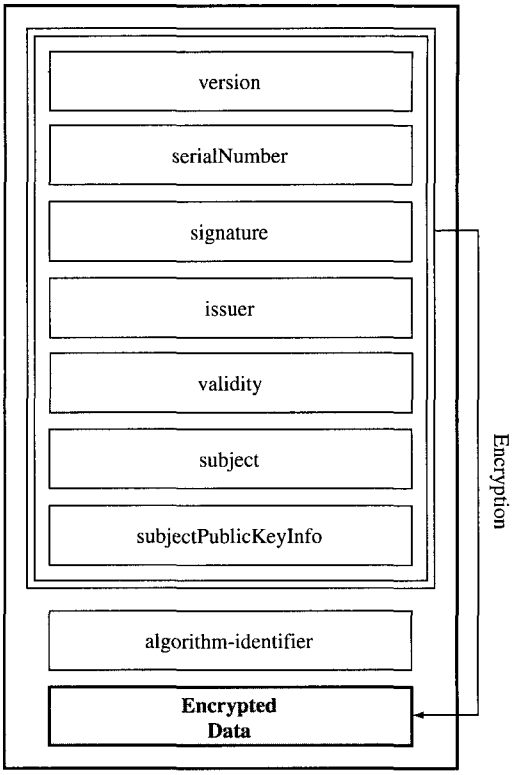
3.3.2.1 Message Submission

Message-submission 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 2]와 같다.

- Originator-certificate
  이 아규먼트는 메세지 송신자의 공개키(public-asymmetric-encryption-key)와 이를 검증하기 위한 증거를 전달하기 위해 사용된다. 송신자의 공개키는 메세지 수신자가 message-token을 검증하거나 메세지가 전달된 MTA와 메세지 수신자가 message-origin-authentication-check를 검증하기 위해 사용된다.



[그림 3] Bind Token의 구조



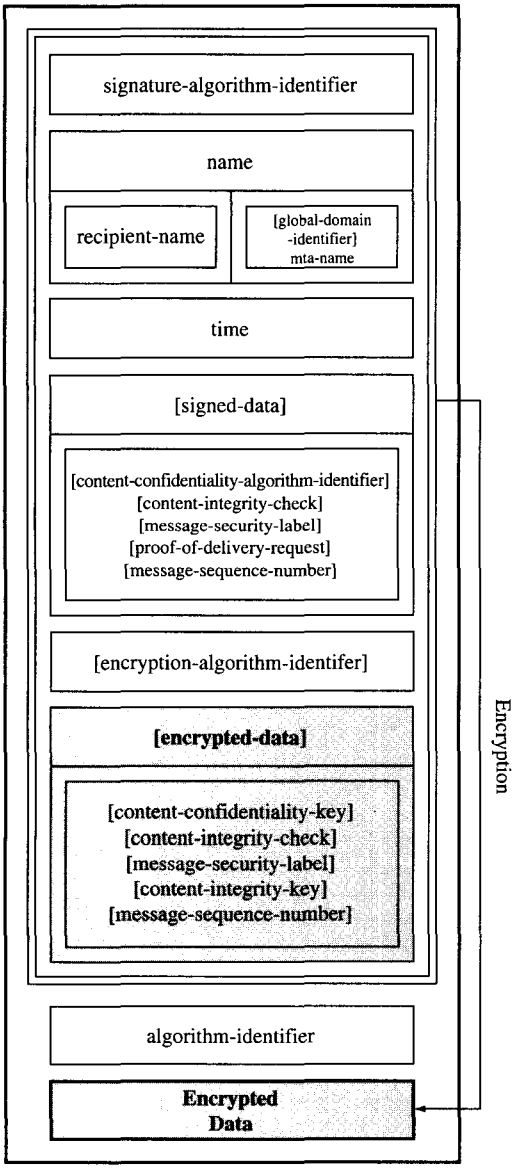
[그림 4] Certificate의 구조

[표 2] Message-submission관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Originator-certificate	O	8.2.1.1.25/X.411
	Message-token	O	8.2.1.1.26/X.411
	Content-confidentiality-algorithm-identifer	O	8.2.1.1.27/X.411
	Content-integrity-check	O	8.2.1.1.28/X.411
	Message-origin-authentication-check	O	8.2.1.1.29/X.411
	Message-security-label	O	8.2.1.1.1.30/X4.11
	Proof-of-submission-request	O	8.2.1.1.1.31/X4.11
	Proof-of-delivery-request	O	8.2.1.1.1.32/X4.11
Results	Originating-MTA-certificate	O	8.2.1.1.2.3/X4.11
	Proof-of-submission	C	8.2.1.1.2.4/X4.11

● Message-token

message-token으로 asymmetric-token을 사용할 경우, signed-data와 encrypted-data로 이루어져 있으며, 이의 구조를 나타낸 것이 [그림 5]이다.



[그림 5] Message Token의 구조

● Content-confidentiality-algorithm-identifier

이 아규먼트는 메세지 송신자가 메세지 내의 Content를 암호화할때 사용한 알고리즘을 식별하기 위한 algorithm-identifier이다.

● Content-integrity-check

이 아규먼트는 content-integrity-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 content-integrity-algorithm-identifier, content가 된다.

● Message-origin-authentication-check

이 아규먼트는 message-origin-authenticaton-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 message-origin-authentication-algorithm-identifier, content, content-identifier, message-security-label이 된다.

● Message-security-label

이 아규먼트는 각 메세지에 부여한 보안 등급을 security-label로 나타낸 것이다. Security-label은 보안 정책에 의해 결정된다.

● Proof-of-submission-request

이 아규먼트는 proof-of-submission-requested와 proof-of-submission-not-requested로 구성되며, proof-of-submission-not-requested을 default값으로 한다.

● Proof-of-delivery-request

이 아규먼트는 proof-of-delivery-requested와 proof-of-delivery-not-requested로 구성되며, proof-of-delivery-not-requested을 default값으로 한다.

● Originating-MTA-certificate

이 아규먼트는 제출된 메세지를 수신한 MTA의 공개키(public-asymmetric-encryption-key)와 이를 검증하기 위한 증거를 메세지 송신자에게 전달하기 위

해 사용된다. MTA의 공개키는 메세지 송신자가 proof-of -submission을 검증하기 위해 사용된다.

- Proof-of-submission

  이 아규먼트는 proof-of-submission-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 proof-of-submission-algorithm-identifier, 수신한 메세지의 message submission arguments, message-submission-identifier, message-submission-time이 된다.

3.3.2.2 Probe Submission

Probe-submission 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 3]와 같다.

[표 3] Probe-submission관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Originator-certificate	O	8.2.1.1.1.25/X.411
	Probe-origin-authentication-check	O	8.2.1.2.1.1/X.411
	Message-security-label	O	8.2.1.1.1.30/X.411
Results	no arguments		

- Probe-origin-authentication-check

  이 아규먼트는 probee-origin-authenticaton-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 probe-origin-authentication-algorithm-identifier, content-identifier, message-security-label이 된다.

3.3.2.3 Submission Control

Submission-control 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 4]와 같다.

[표 4] Submission-control관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Permissible-security-context	O	8.2.1.4.1.5/X411
Results	no arguments		

- Permissible-security-context

  permissible-security-context는 초기 association 설정시에 결정된 security-label들의 부분집합으로 이루어진 security-context이다.

3.3.3 Delivery Port

3.3.3.1 Message Delivery

Message-delivery 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 5]와 같다.

[표 5] Message-delivery관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Originator-certificate	C	8.2.1.1.1.25/X411
	Message-token	C	8.2.1.1.1.26/X411
	Content-confidentiality-algorithm-identifier	C	8.2.1.1.1.27/X411
	Content-integrity-check	C	8.2.1.1.1.28/X411
	Message-origin-authentication-check	C	8.2.1.1.1.29/X411
	Message-security-label	C	8.2.1.1.1.30/X411
	Proof-of-delivery-request	C	8.2.1.1.1.32/X411
Results	Recipient-certificate	O	8.3.1.1.2.1/X411
	Proof-of-delivery	C	8.3.1.1.2.2/X411

- Recipient-certificate
  이 아규먼트는 제출된 메세지를 수신한 수신자의 공개키(public-asymmetric-encryption-key)와 이를 검증하기 위한 증거를 메세지 송신자에게 전달하기 위해 사용된다. 수신자의 공개키는 메세지 송신자가 proof-of -delivery를 검증하기 위해 사용된다.
- Proof-of-delivery
  이 아규먼트는 proof-of-delivery-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 proof-of-delivery-algorithm-identifier, delivery-time, this-recipient-name, originally-recipient-name, content, content-identifier, message-security-label이 된다.

3.3.3.2 Report Delivery

Report-delivery 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 6]와 같다.

[표 6] Report-delivery관련 정보보호 아규먼트

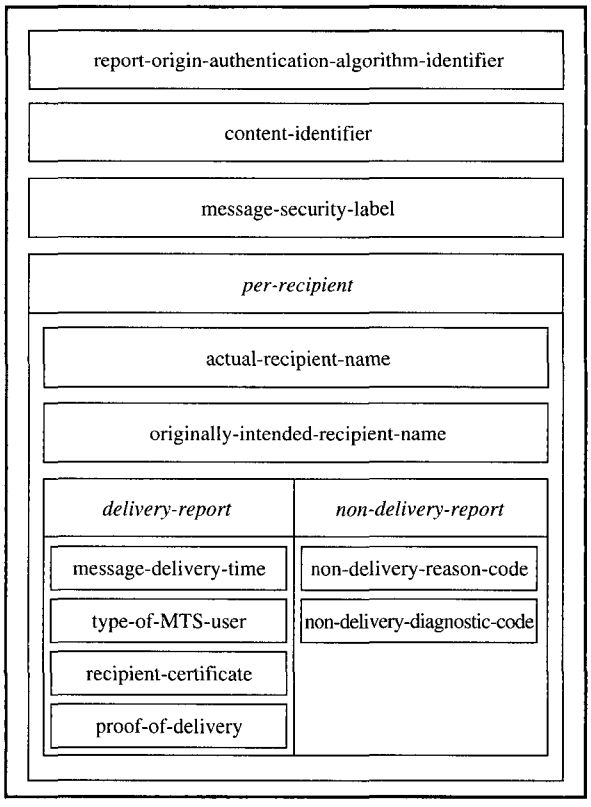
항 목		구 분	참 조
Arguments	Recipient-certificate	C	8.3.1.1.2.1/X.411
	Proof-of-delivery	C	8.3.1.1.2.2/X.411
	Reporting-MTA-certificate	C	8.3.1.2.1.12/X.411
	Report-origin-authentication-check	C	8.3.1.2.1.13/X.411
	Message-security-label	C	8.2.1.1.1.30/X.411
Results	no arguments		

● Reporting-MTA-certificate

이 아규먼트는 제출된 보고서를 송신한 MTA의 공개키(public-asymmetric-encryption-key)와 이를 검증하기 위한 증거를 보고서 수신자에게 전달하기 위해 사용된다. MTA의 공개키는 메세지 송신자와 보고서를 전달받은 MTA가 report-origin-authentication-check을 검증하기 위해 사용된다.

● Report-origin-authentication-check

이 아규먼트는 report-origin-authenticaton-algorithm-identifier와 서명값으로 구성되며, 서명 대상은 report-origin-authenticaton-algorithm-identifier, content-identifier, message-security-label, per-recipients argumet가 된다. 다시, per-recipient 아규먼트로는 actual-recipient-name, originally-intended-recipient-name과 그외 나머지부분은 delivery-report와 non-delivery-report의 경우로 나눠진다. delivery-report의 경우에는 message-delivery-time, type-of-MTS-user, recipient-certificate, proof-of-delivery로 이루어지고 non-livery-report의 경우에는 non-delivery-reseason-code, non-delivery-diagnostic-code로 이루어진다. [그림 6]는 Report-origin-authentication-check의 서명대상을 나타낸 것이다.



[그림 6] Report-origin-authentication-check의 서명대상

3.3.3.3 Delivery Control

Delivery-control 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 7]와 같다.

[표 7] Delivery-control 관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Permissible-security-context	O	8.3.1.3.1.7/X.411
Results	no arguments		

3.3.4 Administration Port

Register 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 8]과 같다.

3.3.4.1 Register

[표 8] Register관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	User-security-labels	O	8.4.1.1.1.7/X.411
Results	no arguments		

- User-security-label

  이 아규먼트는 MTS-user의 security-label들을 포함한다. 수신자 또는 recipient-assigned-alternate-recipient가 메세지를 수신 또는 재전송(redirection)받기 위하여 MTS에 자신의 security-label인 user-security-label을 등록하기 위하여 이 아규먼트가 필요하다. 만약, recipient-assigned-alternate-recipient가 등록되어 있고 user-security-label과 일치되는 message-security-label을 가진 메세지가 MTA에 전달되었을 경우에 이 메세지는 alternate-recipient에게 redirect될 것이다.

3.3.4.2 Change Credentials

Change-credentials 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 9]과 같다.

[표 9] Change-credentials관련 정보보호 아규먼트

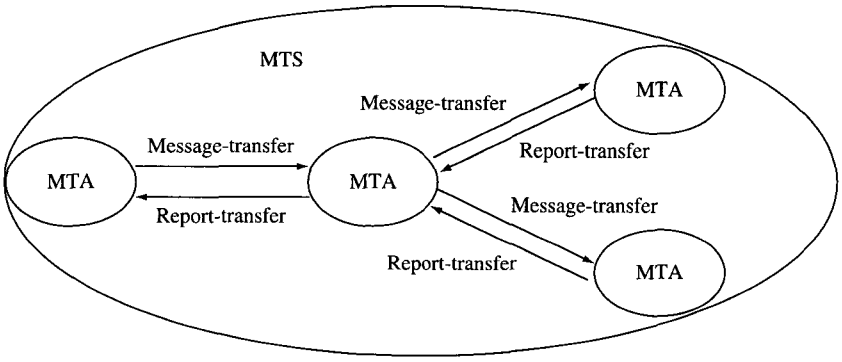
항 목		구 분	참 조
Arguments	Old-credentials	M	8.4.1.2.1.1/X.411
	New-credentials	M	8.4.1.2.1.2/X.411
Results	no arguments		

- Old-credentials
  단순 인증이 사용되면 credentials는 송신자의 user-name 또는 MTA-name과 관련된 password로 구성되고, 강한 인증이 사용되면 송신자의 certificate로 구성된다.
- New-credentials
  New-credentials는 old-credentials와 동일한 타입으로 정의된다.

4. P1 정보보호 서비스

4.1 MTA 시스템 모델

지금까지 정보보호 서비스 제공을 위한 P3 정보보호 서비스에 관하여 요구사항들을 분석하였고, 이 장에서는 MTS를 이루는 MTA간의 프로토콜인 P1 프로토콜 상에서의 정보보호 관련 고려사항들을 정리한다.



[그림 7] MTA 시스템 모델

MTA간의 메세지 혹은 보고서의 전달과 관련한 포트에는 transfer port만 존재한다.

[그림 7]은 MTA 의 시스템 모델을 나타낸 것이다.

4.2 P1 정보보호 서비스 개요

P1 프로토콜 상에서의 MHS 서비스중 정보보호와 관련된 서비스를 P1 정보보호 서비스라 정의한다. 이 절에서는 P1 정보보호 서비스를 제공하기 위하여 다음과 같은 서비스들을 정의한다.

4.2.1 MTA Bind

MTA Bind는 하나의 MTA가 또다른 MTA와 association을 설정할 때 사용된다.

4.2.2 Transfer Port

Message-transfer 오퍼레이션은 MTS-user로부터 메세지를 제출받은 MTA가 인접한 MTA에게 메세지를 전달하는 기능을 한다.

Probe-transfer 오퍼레이션은 MTS-user로 부터 Probe를 제출받은 MTA가 인접한 MTA에게 Probe를 전달하는 기능을 한다.

Report-transfer 오퍼레이션은 MTS가 MTS-user에게 Message-submission 또는 Probe-

submission 오퍼레이션에 따른 결과로서 보고서를 송신 MTS-user에게 알려주기 위하여 MTS내의 MTA사이에서 보고서를 전달하는 기능을 한다.

4.3 P1 정보보호 서비스 정의

4.3.1 MTA bind

MTA-bind는 association의 applicaton-context와 security-context상에서 상호 동작을 위한 MTA와 MTA의 credentials을 설정하는 것이다. bind시 송신측은 initiator-credentials, security-context를 수신측에 전달하고, 수신측에 이에 대한 결과로서 responder-credentials을 송신측에 전달한다. MTA-bind와 관련된 정보보호 아규먼트(security arguments)는 다음 [표 10]과 같다.

- Initiator-credentials

  initiator-credentials는 송신자의 신분을 인증하기 위해 수신자에 의해 사용된다. 이때, 단순 인증(simple authentication)이 사용되면, intiator-credentials는 단순히 initiator-name와 관련한 패스워드(password)로만 구성되고, 강한 인증(strong authentication)이 사용되면, initiator-credentials는 initiator-bind-token과 선택적으로 intiator-certificate로 구성된다.

- Security-context

  security-context는 보안정책(security policy)에 따라 association할 동안에 MTA와 MTA사이에 발생할 수 있는 상호 동작의 sensitivity을 정의하는 하나 이상의 security-label들로 구성된다.

[표 10] MTA-bind관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Initiator-credentials	O	12.1.1.1.1.2/X.411
	Security-context	O	12.1.1.1.1.3/X.411
Results	Responder-credentials	M	12.1.1.1.2.2/X.411

[표 11] Message-transfer관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Originator-certificate	C	8.2.1.1.1.25/X411
	Message-token	C	8.2.1.1.1.26/X411
	Content-confidentiality-algorithm-identifier	C	8.2.1.1.1.27/X411
	Content-integrity-check	C	8.2.1.1.1.28/X411
	Message-origin-authentication-check	C	8.2.1.1.1.29/X411
	Message-security-label	C	8.2.1.1.1.30/X411
	Proof-of-delivery-request	C	8.2.1.1.1.32/X411
Results	no arguments		

4.3.2 Transfer Port

4.3.2.1 Message Transfer

Message-transfer 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 11]와 같다.

4.3.2.2 Probe Transfer

Probe-transfer 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 12]와 같다.

[표 12] Probe-transfer관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Originator-certificate	C	8.2.1.1.1.25/X.411
	Probe-origin-authentication-check	C	8.2.1.2.1.1/X.411
	Message-security-label	C	8.2.1.1.1.30/X.411
Results	no arguments		

4.3.2.3 Report Transfer

Report-transfer 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 13]와 같다.

[표 13] Report-transfer관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Recipient-certificate	C	8.3.1.1.2.1/X.411
	Proof-of-delivery	C	8.3.1.1.2.2/X.411
	Reporting-MTA-certificate	C	8.3.1.2.1.12/X.411
	Report-origin-authentication-check	C	8.3.1.2.1.13/X.411
	Message-security-label	C	8.2.1.1.1.30/X.411
Results	no arguments		

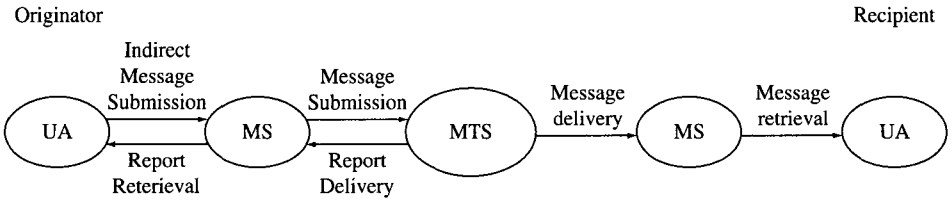
5. P7 정보보호 서비스

5.1 MS 시스템 모델

이 장에서는 MS가 존재할 경우 UA와 MS 간의 프로토콜인 P7 프로토콜 상에서의 정보보호 관련 고려사항들을 정리한다.

MS가 존재할 경우 Retrieval 포트가 UA와 MS 사이에 추가되는 것외에는 기존의 UA와 MTA사이의 포트들을 그대로 적용한다. 따라서 여기서는 Retrieval 포트의 추가에 따른 고려사항들만을 살펴본다.

[그림 8]은 MS 의 시스템 모델을 나타낸 것이다.



[그림 8] MS 시스템 모델

5.2 P7 정보보호 서비스 개요

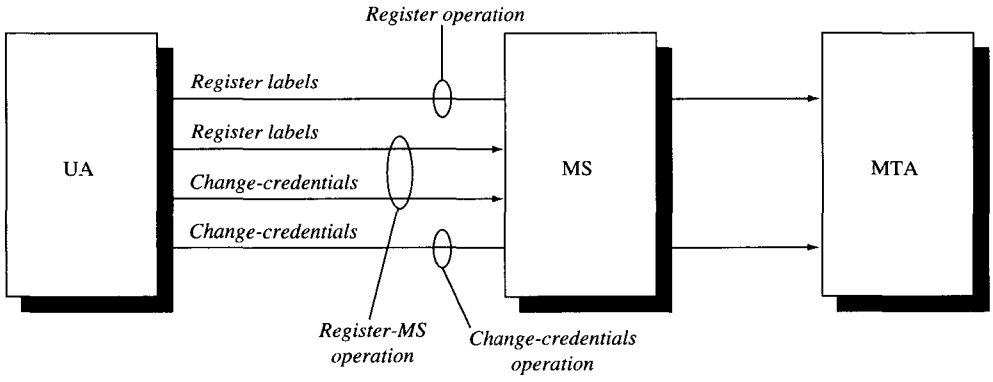
P7 프로토콜 상에서의 MHS 서비스중 정보보호와 관련된 서비스를 P7 정보보호 서비스라 정의한다. 이 절에서는 P7 정보보호 서비스를 제공하기 위하여 다음과 같은 서비스들을 정의한다.

5.2.1 MS Bind

MS Bind는 MS가 MS-user 와 association을 설정할 때 사용된다.

5.2.2 Retrieval Port

Register-MS 오퍼레이션은 UA와 MS간의 Change-credentials 기능과 user-security-labels을 등록하는 기능을 한다. 즉, UA와 MTS간의 Register 오퍼레이션의 기능과 Change-credentials 오퍼레이션의 기능을 동시에 제공한다. MS가 존재할 경우 security-label의 등록 및 credentials의 변경은 Register-MS를 통해서 하며, Register나 Change-credentials의 요구가 UA로 부터 수신되었을 경우에는 MTA에게 통과시켜 주는 기능만을 한다. [그림 9]는 Register, Change-credentials, Register-MS의 차이점을 보여주는 것이다.



[그림 9] Register, Change-credentials, Register-MS의 관계

5.3 P7 정보보호 서비스 정의

5.3.1 MS bind

MS-bind는 association의 applicaton-context와 security-context상에서 상호 동작을 위한 MS와 MS-user의 credentials을 설정하는 것이다. bind 시 송신측은 initiator-credentials, security-context를 수신측에 전달하고, 수신측에 이에 대한 결과로서 responder-credentials을 송신측에 전달한다. MS-bind와 관련된 정보보호 아규먼트(security arguments)는 다음 [표 14]과 같다.

[표 14] MS-bind관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	Initiator-credentials	M	8.1.1.1.1.2/X.411
	Security-context	O	8.1.1.1.1.3/X.411
Results	Responder-credentials	M	8.1.1.1.2.2/X.411

5.3.2 Retrieval Port

5.3.2.1 Register-MS

Register-MS 오퍼레이션과 관련한 정보보호 아규먼트들은 다음 [표 15]와 같다.

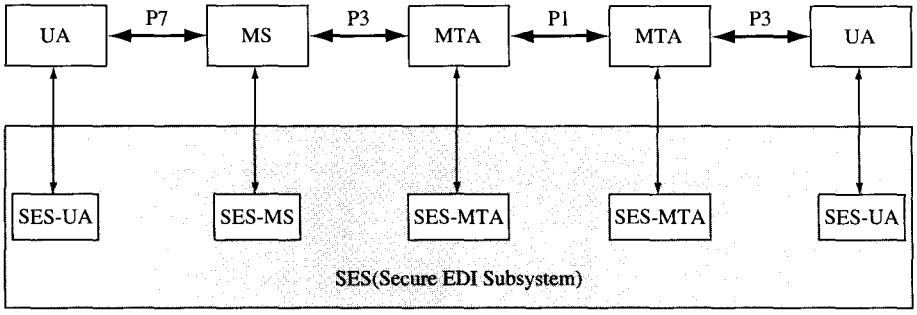
[표 15] Register-MS 관련 정보보호 아규먼트

항 목		구 분	참 조
Arguments	change-credentials	O	8.4.1.2.1/X.411
	user-security-labels	O	8.4.1.1.1.7/X.411
Results	no arguments		

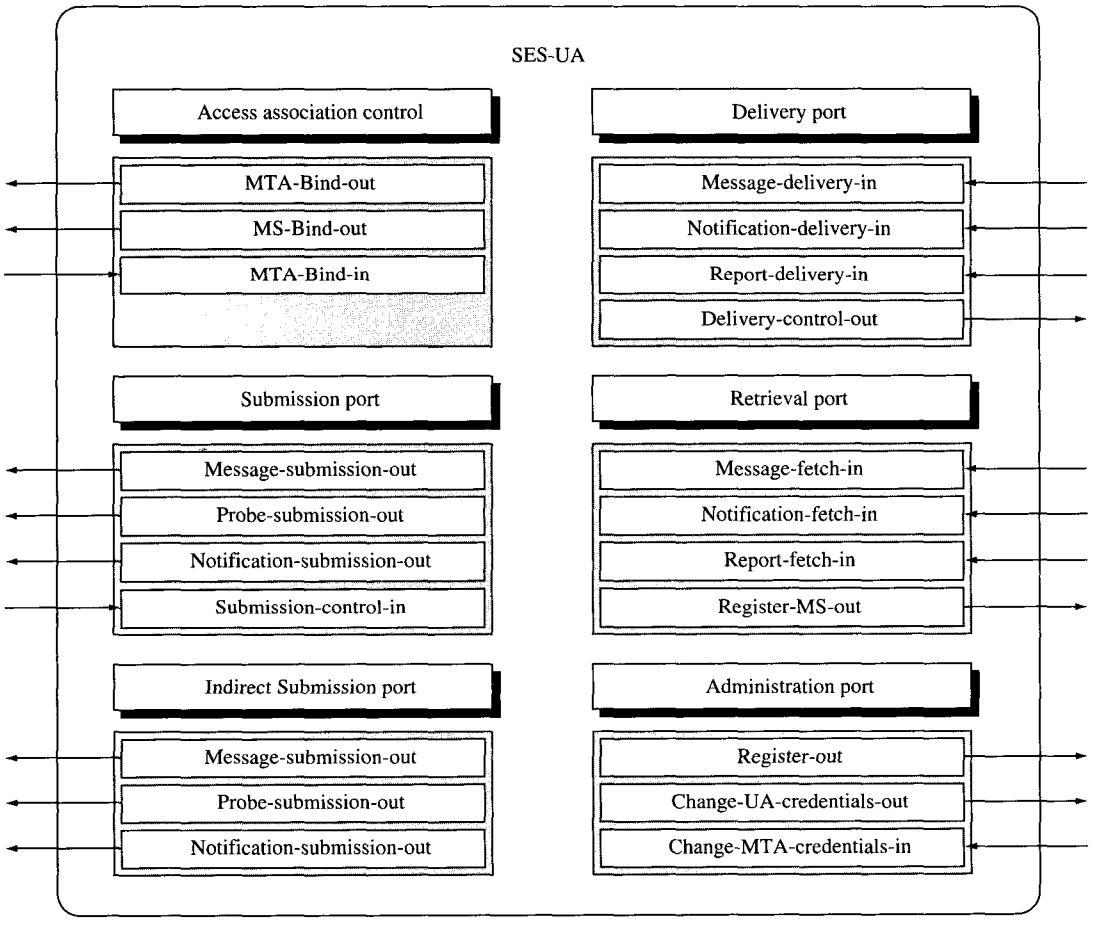
6. SES 모듈 구성

SES(Secure EDI Subsystem)란 EDI의 각 컴포넌트에서 정보보호 서비스를 제공하는 SEDI시스템의 서브시스템이다. SES는 EDI 시스템의 컴포넌트인 UA, MS, MTA에 각각 위치하도록 한다. 그 이유는 EDI 시스템 각각의 컴포넌트가 수행해야 하는 정보보호 서비스의 종류가 다르기 때문이다. 따라서, 이 장에서는 SES의 각 컴포넌트별 정보보호 서비스 처리 모듈인 SES-UA, SES-MS, SES-MTA 각 모듈내에서의 관련 포트 및 오퍼레이션들의 처리와 EDI 모듈과의 관련 고려사항들을 살펴본다.

[그림 10]은 SES 시스템의 구성을 나타낸 것이다.



[그림10] SES 시스템의 구성



[그림 11] SES-UA관련 포트 및 모듈

6.1 SES-UA 모듈

UA 응용 프로세스는 UA와 MS간에 사용되는 오퍼레이션인지, 또는 UA와 MTA간에 사용되는 오퍼레이션인지에 따라 구분된다. 각 오퍼레이션에서의 사용요구 및 수신처리를 담당하는 기본적인 단위를 모듈(module)이라 하고, 이중에서 UA에서 정보보호 서비스를 처리하는 모듈들의 집합을 SES-UA 모듈이라 한다.

SES-UA모듈은 UA를 통하는 메세지, probe, 보고서들의 입출력 및 관련 오퍼레이션들상에서의 정보보호 서비스 지원을 담당한다. [그림 11]은 SES-UA관련 포트 및 모듈을 나타낸 것이다.

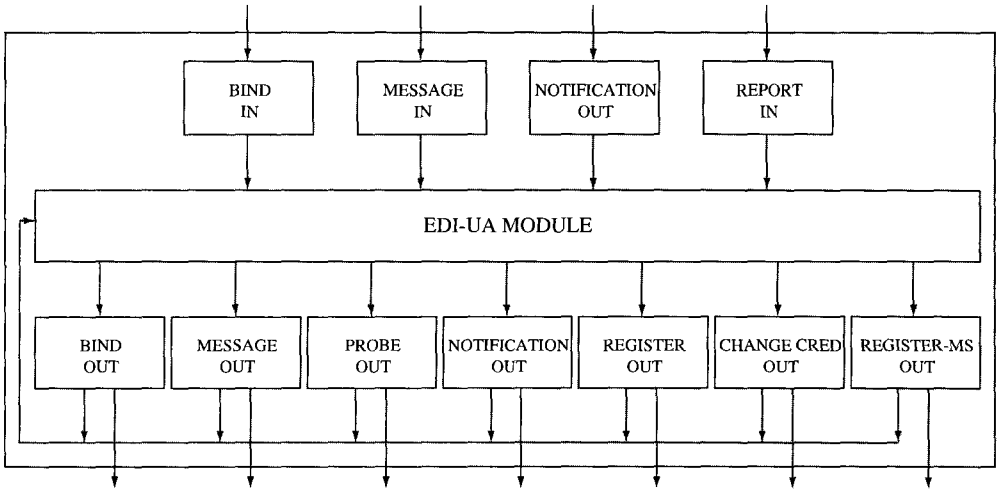
정보보호 서비스의 처리를 담당하는 SES-UA 모듈을 거친 송수신 메세지, probe, 보고서들은 다시 EDI 서비스 처리를 담당하는 EDI-UA 넘겨지는데, 이 EDI-UA 모듈을 호출하는 SES-UA 모듈들은 다음과 같다.

- Bind-in 모듈
- Message-in 모듈
- Notification-in 모듈
- Report-in 모듈

SES-UA 모듈을 통해 정보보호 서비스의 처리중 에러 조건에 해당할 경우 다음 모듈들에 의해 EDI-UA 모듈은 다시 호출될 수 있다.

- Bind-out 모듈
- Message-out 모듈
- Probe-out 모듈
- Notification-out 모듈
- Register-out 모듈
- Change-credenitals-out 모듈
- Register-MS-out 모듈

SES-UA 모듈과 EDI-UA 모듈과의 관계를 나타낸 것이 [그림 12]이다.

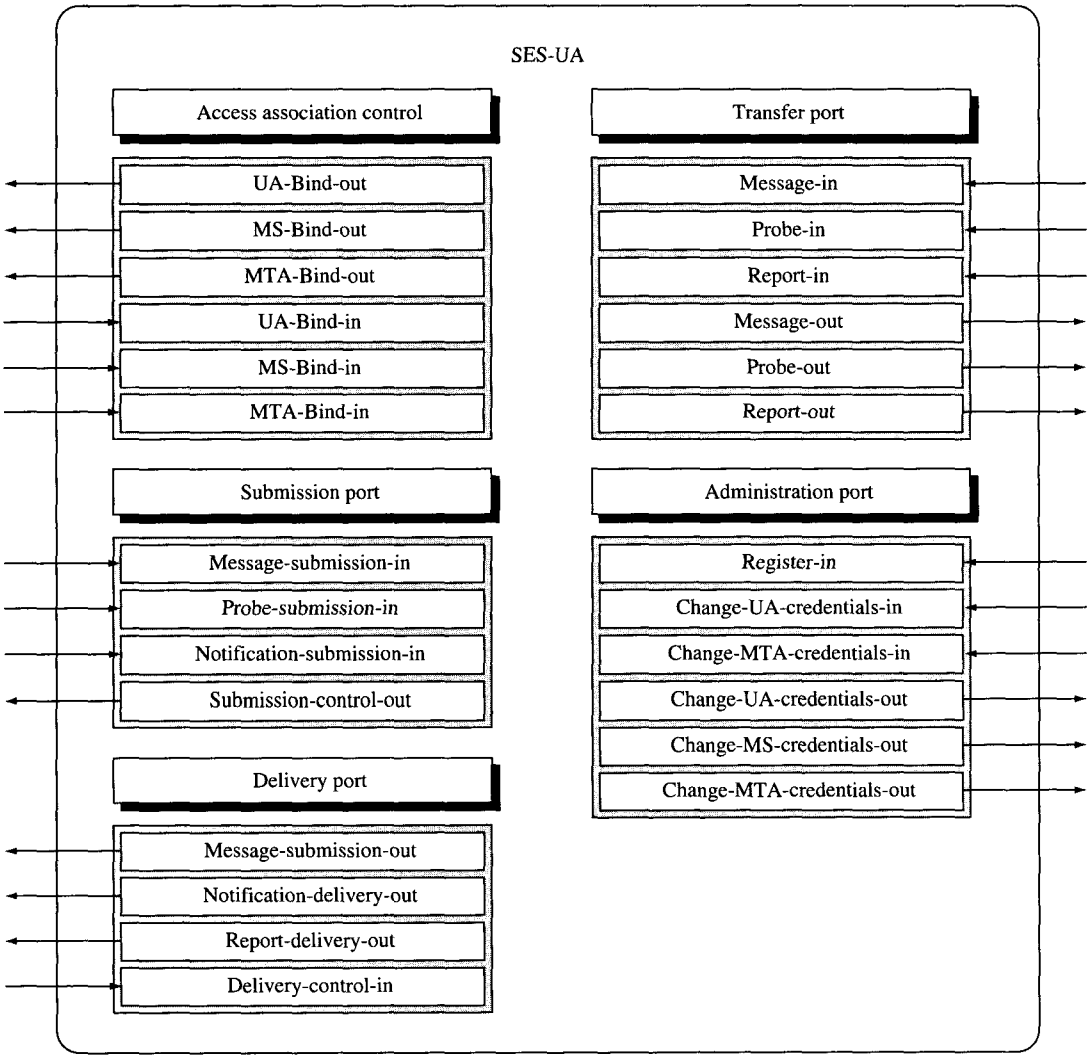


[그림 12] SES-UA모듈과 EDI-UA모듈과의 관계

6.2 SES-MTA 모듈

MTA 응용 프로세스는 MTA와 UA간에 사용되는 오퍼레이션인지, 또는 MTA와 UA간에 사용되는 오퍼레이션인지에 따라 구분된다. 각 오퍼레이션에서의 사용요구 및 수신처리를 담당하는 기본적인 단위를 모듈(module)이라 하고, 이중에서 MTA에서 정보보호 서비스를 처리하는 모듈들의 집합을 SES-MTA 모듈이라 한다.

SES-MTA모듈은 MTA를 통하는 메세지, probe, 보고서들의 입출력 및 관련 오퍼레이션들상에서의 정보보호 서비스 지원을 담당한다. [그림 13]은 SES-MTA관련 포트 및 모듈을 나타낸 것이다.



[그림 13] SES-MTA관련 포트 및 모듈

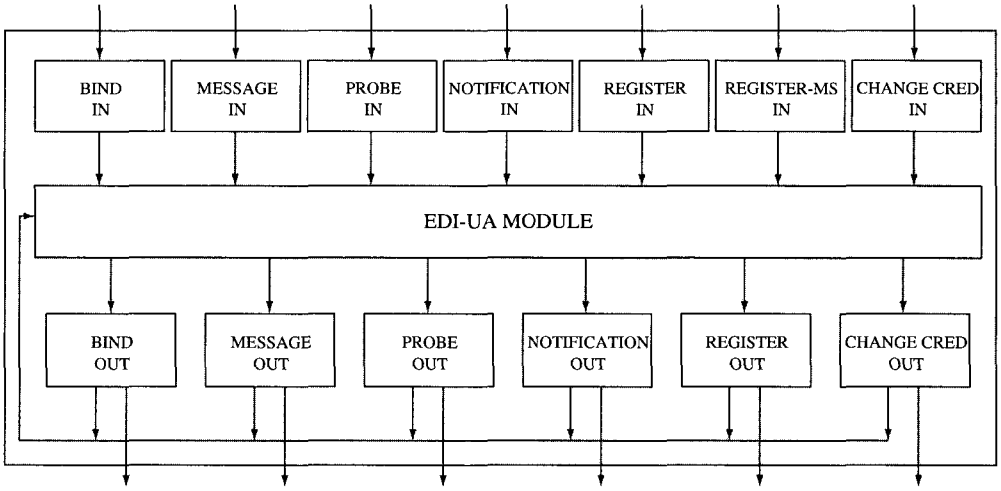
정보보호 서비스의 처리를 담당하는 SES-MTA 모듈을 거친 송수신 메세지, probe, 보고서들은 다시 EDI 서비스 처리를 담당하는 EDI-MTA 넘겨지는데, 이 EDI-MTA 모듈을 호출하는 SES-MTA 모듈들은 다음과 같다.

- Bind-in 모듈
- Message-in 모듈
- Probe-in 모듈
- Notification-in 모듈
- Report-in 모듈
- Register-in 모듈
- Change-credentials-in 모듈

SES-MTA 모듈을 통해 정보보호 서비스의 처리중 에러 조건에 해당할 경우 다음 모듈들에 의해 EDI-MTA 모듈은 다시 호출될 수 있다.

- Bind-out 모듈
- Message-out 모듈
- Probe-out 모듈
- Notification-out 모듈
- Report-out 모듈
- Change-credenitals-out 모듈

SES-MTA 모듈과 EDI-MTA 모듈과의 관계를 나타낸 것이 [그림 14]이다.



[그림 14] SES-MTA모듈과 EDI-MTA모듈과의 관계

6.3 SES-MS 모듈

MS 응용 프로세스는 MS와 UA간에 사용되는 오퍼레이션인지, 또는 MS와 MTA간에 사용되는 오퍼레이션인지에 따라 구분된다. 각 오퍼레이션에서의 사용요구 및 수신처리를 담당하는 기본적인 단위를 모듈(module)이라 하고, 이중에서 MS에서 정보보호 서비스를 처리하는 모듈들의 집합을 SES-MS 모듈이라 한다.

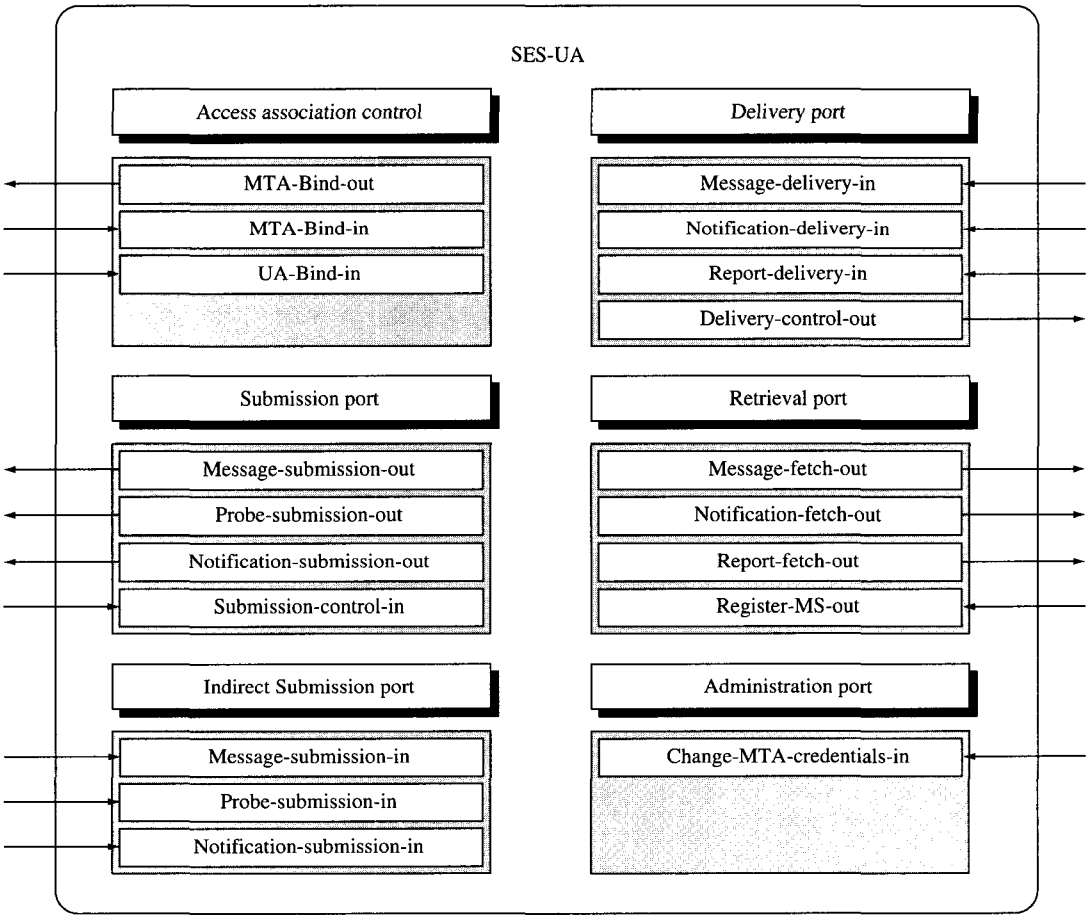
SES-MS모듈은 MS를 통하는 메세지, probe, 보고서들의 입출력 및 관련 오퍼레이션들상에서의 정보보호 서비스 지원을 담당한다. [그림 15]은 SES-MS관련 포트 및 모듈을 나타낸 것이다.

정보보호 서비스의 처리를 담당하는 SES-MS 모듈을 거친 송수신 메세지, probe, 보고서들은 다시 EDI 서비스 처리를 담당하는 EDI-MS 넘겨지는데, 이 EDI-MS 모듈을 호출하는 SES-MS 모듈들은 다음과 같다.

- Bind-in 모듈
- Message-in 모듈
- Probe-in 모듈
- Notification-in 모듈
- Report-in 모듈
- Change-credentials-in 모듈
- Register-MS-in 모듈

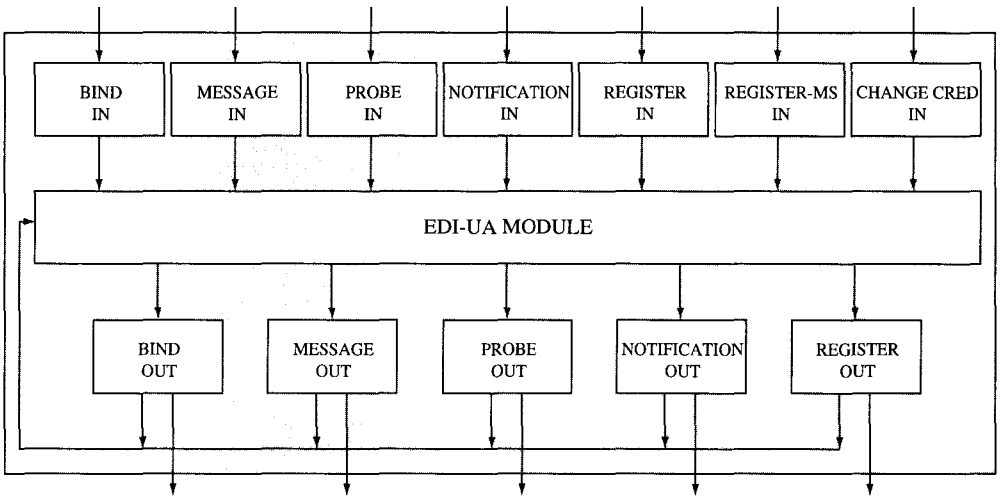
SES-MS 모듈을 통해 정보보호 서비스의 처리중 에러 조건에 해당할 경우 다음 모듈들에 의해 EDI-MS 모듈은 다시 호출될 수 있다.

- Bind-out 모듈
- Message-out 모듈
- Probe-out 모듈
- Notification-out 모듈
- Report-out 모듈



[그림 15] SES-MS관련 포트 및 모듈

SES-MS 모듈과 EDI-MS 모듈과의 관계를 나타낸 것이 [그림 16]이다.



[그림 16] SES-MS모듈과 EDI-MS모듈과의 관계

7. 결론

EDI 시스템에 정보보호 기능을 부가한 시스템을 SEDI 시스템이라 하며, 이 시스템에서 제공하는 정보보호 서비스를 분석하였다. 또한 이러한 시스템을 개발하는데 사용되는 통신 프로토콜에는 P3, P7, P1의 기존 MHS 프로토콜을 그대로 사용하며, 이 프로토콜들 상에서 정보보호 서비스를 제공하는데 사용되는 포트와 해당 오퍼레이션들의 구조를 분석하였다. 이러한 프로토콜상에서 인증서비스, 기밀성 서비스, 부인봉쇄 서비스 등의 일반적인 정보보호 서비스를 실현하기 위하여 앞서 언급된 정보보호 서비스용 데이타 구조들을 이용한다면, 향후 메세지 처리 시스템을 개발하고자 하는 개발자들에게 유용하게 사용될 수 있을 것이다.

참 고 문 헌

[1] Chang Goo Kang, E Joong Yoon, Dae Ho Kim, Dai Ki Lee, "A Design of Secure EDI Systems," 8th Annual Canadian Computer Security Symposium, pp.397-416, 1996.

[2] 강창구, "EDI 정보보호 서비스 분석", 제2차 안전한 EDI 관련기술 심포지움, pp. 3-18, 1996.3.

[3] 이정현, 윤이중, 김대호, 이대기, "X.435 EDI 정보보호 서비스 데이타 구조 분석", 한국통신 정보보호학회지 제5권 제3호, pp.69-85, 1995.9.

[4] 이정현, "안전한 EDI 시스템의 데이타 구조", 제2차 안전한 EDI 관련기술 심포지움, pp. 19-30, 1996.3.

[5] ITU-T F.435, Message handling systems:

Electronic data interchange messaging service, 1991.

[6] ITU-T X.435, Message handling systems: Electronic data interchange messaging system, 1992.

[7] ITU-T X.402, Message handling systems: Overall architecture, 1992.

[8] ITU-T X.411, Message handling systems - Message transfer system: Abstract service definition and procedures, 1992.

[9] 윤이중, "안전한 EDI 시스템의 구조 설계", 제2차 안전한 EDI 관련기술 심포지움, pp. 31-43, 1996.3.

[10] 윤이중, "EDI용 안전성 서버 구현", 제3차 안전한 EDI 관련기술 심포지움, pp. 5-12, 1996.8.

[11] ITU-T X.413, Message handling systems - Message store: Abstract service definition and procedures, 1992.

[12] 이정현, 윤이중, 김대호, 이대기, "SEDI 시스템 데이타 구조 분석", 한국정보처리학회 추계 학술 발표회 논문집 제2권 제2호, pp.456-461, 1995.10.EDI 정보보호 시스템의 구조 및 서비스 환경 분석

□ 著者紹介

이 정 현

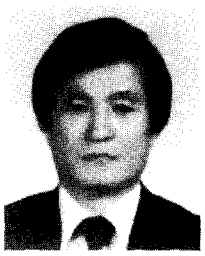
1993년 숭실대학교 전자계산학과(공학사)
1995년 숭실대학교 대학원 전자계산학과(공학석사)
1995년 ~ 현재 한국전자통신연구원

※ 주관심분야 : 컴퓨터/네트워크 보안

윤 이 중

1988년 인하대학교 전산학과(공학사)
1990년 인하대학교 대학원 전산학과(공학석사)
1990년 ~ 현재 한국전자통신연구원

※ 주관심분야 : 컴퓨터/네트워크 보안, DBMS



이 대 기

1966년 한양대학교 전자공학과(공학사)
1987년 한양대학교 산업대학원 전자공학과(공학석사)
1980년 ~ 현재 한국전자통신연구원 책임기술원

※ 주관심분야 : 정보시스템 감사, 통제 및 보안

김 대 호

1977년 한양대학교 전자공학과(공학사)
1984년 한양대학교 산업대학원 전자공학과(공학석사)
1993년 Visiting Scholar(University of Maryland at College Park Dept. of Computer Science)
1977년 ~ 현재 한국전자통신연구원 책임연구원

※ 주관심분야 : 전송분야, 통신 및 컴퓨터 보안