

안전한 EDI 시스템 설계

윤 이 중*, 이 정 현*, 김 대 호*, 이 대 기

요 약

본 연구는 SEDI 시스템의 구조 설계에 관한 것이다. 본 논문에서는 SEDI 시스템의 구조 설계를 위해서 EDI 시스템에서 제공해야 하는 정보보호 서비스의 종류 및 기능을 분석하였고, 각 서비스별로 제공 방법을 정의하였다. 제안된 SEDI의 구조는 각각의 정보보호 서비스를 처리하는 SES와 SES가 정보보호 서비스를 처리하는데 필요한 정보의 처리를 담당하는 SMS로 나누어진다.

1. 서 론

네트워크를 이용한 전자 문서 전달 시스템은 기업간의 공식적인 문서 교환을 포함하여 다양한 용도로 사용되고 있고 그 이용률은 계속 증가하고 있다. 이와 더불어 교류되는 문서에 대한 정보보호 서비스 요구 또한 증가하고 있다.

전자 문서 교환 시스템에 대한 표준화 작업은 1984년에 X.400이 발표되었고, 1988년에 X.400이 수정 발표되었다. 이때 수정된 내용은 디렉토리 이름의 사용, 분배 리스트의 사용, OSI 스택의 사용 등과 정보보호 서비스의 추가 등이다. 이후 1990년에 EDI(Electronic Data Interchange)와 그에 관련된 정보보호 서비스가 추가되어 1992년에 개정 발표되었다^[1].

본 논문에서는 EDI 시스템의 정보보호 서

비스를 실현하기 위해 1992년에 개정된 표준을 근거로 하였다. SEDI(Secure Electronic Data Interchange) 시스템의 구조 설계를 위해서 EDI 시스템에서 제공해야 하는 정보보호 서비스의 종류 및 기능을 분석하였고, 각 서비스별로 제공 방법을 정의하였다. 제안된 SEDI의 구조는 각각의 정보보호 서비스를 처리하는 SES(Secure EDI Subsystem)와 SES가 정보보호 서비스를 처리하는데 필요한 정보의 처리를 담당하는 SMS(Secure Management Subsystem)로 나누어진다. 본 논문의 구성은 2장에서 정보보호 서비스의 기능을 분석하고, 3장에서 EDI 시스템 각 컴포넌트별로 수행해야 하는 정보보호 서비스들을 정의하였고, 4장에서 SEDI 시스템의 구조를 제안하고 5장에서 결론을 맺는다.

* 한국전자통신연구소

2. 정보보호 서비스 분석

본 장에서는 X.435에 정의되어 있는 EDI 시스템의 정보보호 서비스 종류 및 그 기능을 분석하였다. X.435는 UA(User Agent)에서 처리할 수 있는 메시지의 형태중 EDI 메시지에 대해서 정의하고 있다. 따라서 EDI 시스템에서 처리하여야하는 정보보호 서비스의 종류는 메시지 종류에 관계 없이 모든 메시지 처리 시스템에서 처리하여야하는 정보보호 서비스를 포함하고 EDI 시스템 특성에 따라 추가로 요구되는 정보보호 서비스를 포함한다³. 모든 메시지 처리 시스템에서 처리하여야하는 정보보호 서비스는 X.402에 정의되어 있고 그 종류는 발신처 인증(Origin Authentication) 서비스, 정보보호 접근 관리(Secure Access Management) 서비스, 데이터 비밀성(Data Confidentiality) 서비스, 데이터 무결성(Data Integrity) 서비스, 부인봉쇄(Non-Repudiation) 서비스, 메시지 정보보호 레이블링(Message Security Labelling), 정보보호 관리(Security Management) 서비스의 일곱 종류로 나누어져 있다. X.435에서는 EDI메시지 특성을 고려하여 X.402에 추가하여 EDIM 책임 인증(EDIM Responsibility Authentication)과 EDIM 책임 부인봉쇄(Non-repudiation of EDIM Responsibility)가 정의되어 있다. 따라서 X.435에서 정의된 정보보호 서비스는 아홉 개의 부류로 나누어진다^{3,15,6,7}.

2.1 발신처 인증 (Origin Authentication)

이 부류는 다섯 개의 서비스가 정의되어 있다. 정의된 서비스는 메시지, 프로브, 리포트의 발신처 인증과 제출 및 배달 증거 서비스들이다. 이 서비스들의 기능은 임의 메시지에 대한 발신자의 신원을 수신자에게 확인시켜주는 기

능을 담당한다.

2.2 정보보호 접근 관리 (Secure Access Management)

이 부류는 두개의 서비스가 정의되어 있다. 정의된 서비스는 EDI 시스템의 컴포넌트들 사이에 바인딩이 이루어지는 시점에서 상호 신원을 확인하게 해주는 상대 실체 인증과 이들 컴포넌트들 사이에서 발생하는 메시지의 전달 시에 전달 가능 여부를 메시지와 컴포넌트들의 정보보호 레이블에 의해서 결정하는 정보보호 문맥 서비스이다. 여기서 정보보호 문맥 서비스는 기본적으로 EDI 시스템의 모든 컴포넌트 및 메시지에 정보보호 레이블이 할당되어야하고, 또한 이들 위해 EDI 시스템에 대한 정보보호 정책이 명확히 정의되어야한다.

2.3 데이터 비밀성 (Data Confidentiality)

이 부류는 세개의 서비스가 정의되어있다. 정의된 서비스는 연결 비밀성, 내용 비밀성, 메시지 흐름 비밀성들이다. 이중에서 연결 비밀성은 EDI 시스템에서 필요한 서비스로 정의는 되어 있지만 이를 지원할 수 있는 프로토콜이 EDI 시스템에는 정의되어 있지 않고, 만약 하위 레이어에서 이 서비스를 지원할 수 있는 프로토콜이 제공된다면 바인딩 시에 임의의 변수를 이용하여 지원 요청을 하도록 정의되어 있다. 메시지 흐름 비밀성 서비스는 메시지의 송신량을 일정하게 유지함으로써 메시지의 흐름을 분석하여 발생할 수 있는 위험요소를 방지하고자 정의되었으나 일반적인 사용 환경에서는 거의 사용되지 않을 것으로 예상된다.

2.4 데이터 무결성(Data Integrity)

이 부류는 세계의 서비스가 정의되어 있다. 정의된 서비스는 연결 무결성, 내용 무결성, 메시지 순서 무결성 등이 정의되어 있다. 여기서 연결 무결성은 데이터 비밀성 부류의 연결 비밀성과 같은 특성으로 정의되어 있다.

2.5 부인봉쇄(Non-Repudiation)

이 부류는 세계의 서비스가 정의되어 있다. 정의된 서비스는 발신처, 제출, 배달 부인봉쇄이다. 부인 봉쇄 서비스는 기본적으로 발신처 인증 서비스들과 제공 방법 및 개념은 동일하다. 단지 차이점은 제3자 또는 공신력이 있는 검증 절차가 필요하다는 것이다.

2.6 메시지 정보보호 레이블링 (Message Security Labeling)

이 부류의 서비스는 메시지 정보보호 레이블링이라는 하나의 서비스를 정의하고 있다. 이 서비스 자체로는 정보보호 서비스로의 의미를 갖지 못한다. 이 서비스는 정보보호 문맥 서비스가 지원되어야 한다. 즉 이 서비스는 정보보호 문맥 서비스가 제공되기 위한 선행조건이 되는 것이다.

2.7 정보보호 관리 (Security Management)

이 부류는 세가지 서비스가 정의되어 있다. 정의된 서비스는 신원 정보의 변경, 등록, MS(Message Store) 등록 등이다. 등록에 관련된 서비스는 EDI 시스템 각 컴포넌트들의 정보보호 레이블을 서로 등록하는 기능을 수행하고, 신원 정보의 변경은 바인딩시에 사용되

는 정보의 변경을 수행한다.

2.8 EDIM 책임 인증 (EDIM Responsibility Authentication)

이 부류는 EDI 시스템에만 적용되는 서비스로 세 가지 서비스가 정의되어 있다. 정의된 서비스는 MS에서 UA가 메시지를 검색했다는 증거를 남기는 검색 증명과, MTA(Message Transfer agent)에서 해당 메시지를 전달 했다는 증거를 남기는 전달 증명, 그리고 EDI Notification을 생성 했다는 증거를 생성하는 EDI Notification 증거 서비스들이다. 여기서 검색 및 전달 증거 서비스는 다른 서비스와는 달리 프로토콜을 이용하는 것이 아니라 감사 추적 기법을 이용한다.

2.9 EDIM 책임 부인봉쇄 (Non-repudiation of EDIM Responsibility)

이 부류는 2.8에서 정의된 서비스와 동일하다. 차이점은 제3자 또는 공신력 있는 검증이 요구된다는 것이다.

3. EDI 컴포넌트 별 기능

2장에서 정의한 각 서비스의 기능은 세부적으로 어떤 컴포넌트들 사이에서 적용되어야 하는지 정의되어 있다³⁷⁾. 본 장에서는 이들 서비스가 제공되기 위해서 EDI 시스템 각 컴포넌트들이 어떤 기능을 수행해야 하는지를 분석, 정의하였다. 기본적으로 각 서비스는 데이터의 요청, 생성, 검증의 세가지 기능으로 나누어진다. 예를 들어 제출 증명 서비스의 경우 UA는 메시지를 제출할 때 MTA에게 제출 증명을 요청하게 되고 MTA는 이를 받아 제출 증

명 데이터를 생성하고 UA에게 보낸다. UA는 이를 받아 제출 증명 데이터를 검증한다. 그림 1은 컴포넌트들 사이에 적용되어야 하는 서비스의 분석 결과를 나타낸 것이다. 이와 같은 행위는 EDI 시스템 각 컴포넌트들의 통신을 위해 정의된 P1, P3, P7 프로토콜 상에서 이루어진다. 이 프로토콜들은 세부적인 기능별 포트로 나누어 진다. 따라서 각각의 정보보호 서비스는 적용되어야 하는 포트별로 분류될 수 있다^{13,6)}. 실제적으로 EDI 시스템에서 일어나는 행위는 각 포트별로 이루어진다. 따라서

SEDI 설계를 위해 이러한 분류는 매우 중요하다. 본 논문에서는 이 분석 결과를 3.1.3.2, 3.3에서 컴포넌트별로 기술하였다.

3.1 UA 기능

본 절에서는 UA가 처리해야 하는 정보보호 서비스의 기능을 EDI 시스템의 각 포트별로 분류하였다. UA는 MS또는 MTA와 통신할 수 있으며 이때 사용되는 프로토콜이 P7과 P3이다. P3는 제출, 배달, 관리, 바인드와 같은 네

Services	UA			MS			MTA			Third
	요청	생성	검증	요청	생성	검증	요청	생성	검증	검증
Message Origin Authentication		*	*			*			*	
Non-Rep of Origin	*						*			*
Content Confidentiality		*	*							
Content Integrity		*	*							
Message sequence Integrity		*	*							
Proof of Submission	*		*					*		
Non-Rep of Submission	*									*
Proof of Delivery	*	*	*		*					*
Non-Rep of Delivery	*									*
Proof of Content	*	*	*							*
Non-Rep of Content	*	*								*
Proof of EDI Notification	*	*	*							*
Non-Rep of EDI Notifion	*	*								*
Probe Origin Authentication		*			*					*
Report Origin Authentication			*			*		*	*	
Change Credentials		*	*			*		*	*	
Register		*				*			*	
MS-Register		*				*				
Proof of Retrieval				Secure Audit Trail						
Non-Rep of retrieval							Secure Audit Trail			
Proof of Transfer							Secure Audit Trail			
Non-Rep of Transfer										
Peer Entity Authentication		*	*		*	*		*	*	
Security Context		*	*		*	*		*	*	
Message Security Labeling		*	*		*	*		*	*	
Message Flow Confidentiality		*	*							
Connection Confidentiality	*			*			*			
Connection Integrity	*			*			*			

그림 1. EDI 시스템 컴포넌트별 기능 분류

개의 포트르 구성된다. 제출 포트는 메시지와 프로브의 제출, 제출제어, 지연배달 취소의 네 가지 동작으로 구성된다. 배달 포트는 메시지와 리포트의 배달, 배달제어와 같은 세 가지 동작으로 구성된다. 관리 포트는 등록과 신원정보의 변경 동작으로 구성된다. 바인드 포트는 바인드 동작만으로 구성된다. 여기서 제출 포트의 지연배달 취소 동작을 제외하고 나머지 모든 동작에 정보보호 서비스가 제공되어야 한다. P7 프로토콜은 간접제출, 검색, 관리, 바인드와 같은 네 가지 포트르 구성된다. 간접제출 포트는 P3 프로토콜의 제출 포트와 동일한 동작으로 구성된다. 검색 포트는 요약, 항

목, 추출, 삭제, 변경, MS 등록의 다섯 가지 동작으로 구성된다. 관리 포트와 바인드 포트는 P3 프로토콜과 동일하다. P7 프로토콜에서는 지연배달 취소, 요약, 항목, 추출, 삭제, 변경 동작을 제외한 나머지 동작에 정보보호 서비스가 제공되어야 한다. 그림 2는 각 동작별로 제공되어야하는 정보보호 서비스의 기능을 나타내었다.

3.2 MS 기능

본 절에서는 MS가 처리해야 하는 정보보호 서비스의 기능을 EDI 시스템의 각 포트별로

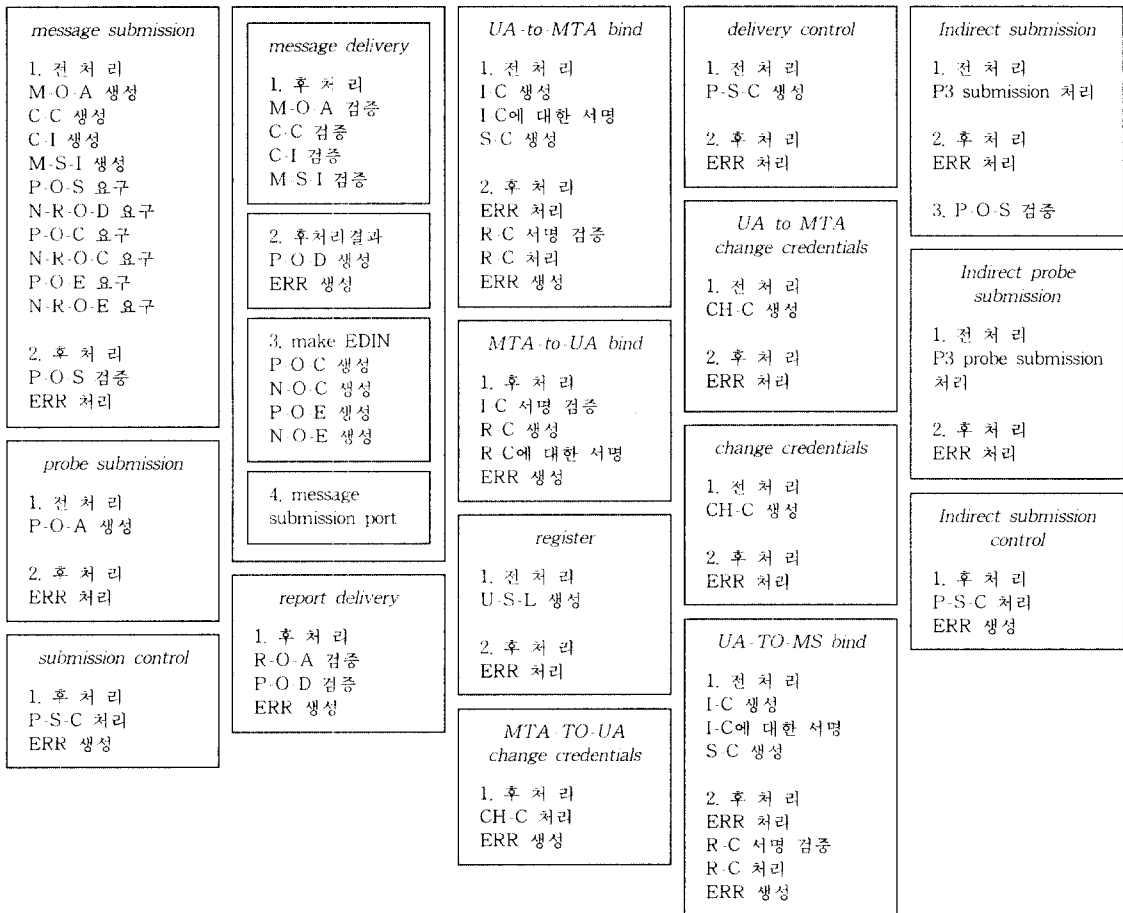


그림 2. UA가 제공하는 정보보호 서비스

분류하였다. MS는 UA또는 MTA와 통신할 수 있으며 이때 사용되는 프로토콜이 P7과 P3다[5]. 따라서 MS가 처리하여야하는 서비스는 UA에서 분석한 프로토콜상의 동작들을 대상으로 한다. 그림 3은 MS가 처리하여야 하는 정보보호 서비스 기능을 각 동작별로 분류한 것이다.

3.3 MTA 기능

본 절에서는 MTA가 처리해야 하는 정보보호 서비스의 기능을 EDI 시스템의 각 포트별로 분류하였다. MTA는 UA, MS, MTA와 통신할 수 있으며 이때 사용되는 프로토콜이 P3와 P1이다. P1 프로토콜은 전달, 관리, 바인드 포트에 구성된다. 전달 포트는 메세지, 프로브, 리포트의 입출력들이 정의되어 여섯개의 동작으로 구성된다. MTA는 P3와 P1 프로토콜을 대상으로 정보보호 서비스를 지원해야하고 이는 그림 4에 정의하였다.

4. SEDI의 구조

EDI 시스템에 정보보호 서비스를 제공하기 위해 본 논문에서는 UA, MS, MTA에 기본적으로 SES(Secure EDI Subsystem)와 SMS(Secure Management Subsystem)가 추가되도록 하고, 별도의 CA(Certification Authority)용 키관리 시스템을 제공하고, 기존의 DSA(Directory Service Agent)가 키관리를 할 수 있도록 변형되도록 제안하였다. 그림 5는 정보보호 서비스를 제공하기 위한 SEDI의 구성도를 보인다.

SES는 EDI 시스템이 제공해야하는 정보보호 서비스를 처리하는 주 기능을 담당한다. UA, MS, MTA는 SES 인터페이스를 이용해서 해당 서비스의 요청을 수행한다. SMS는 SES가 정보보호 서비스를 처리하는데 사용되는 데이터를 제공 저장하는 기능, 감사 추적 기능, 키 관련 정보의 제공 등을 수행한다. CA 키관리 시스템은 정보보호 서비스에서 사용되

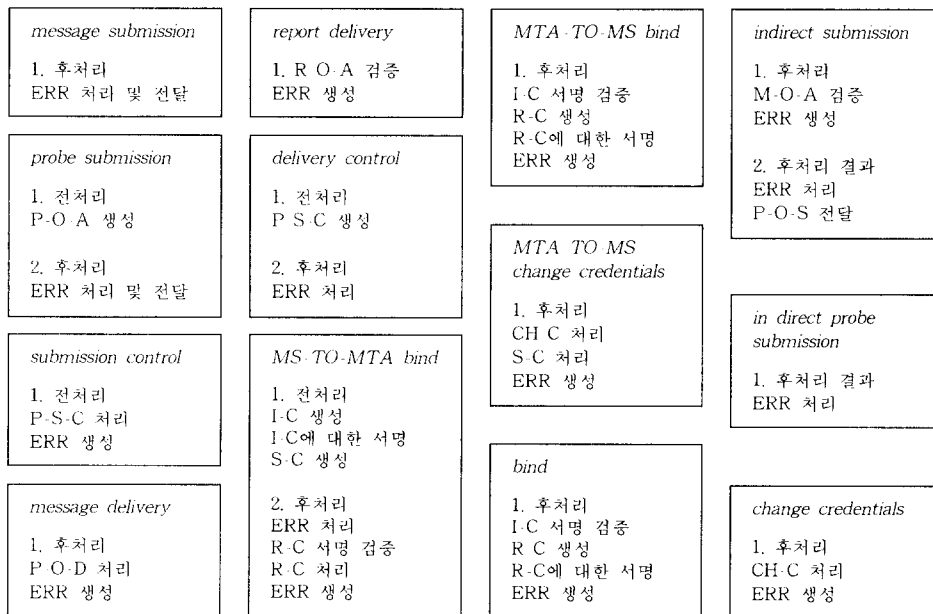


그림 3. MS가 제공하는 정보보호 서비스

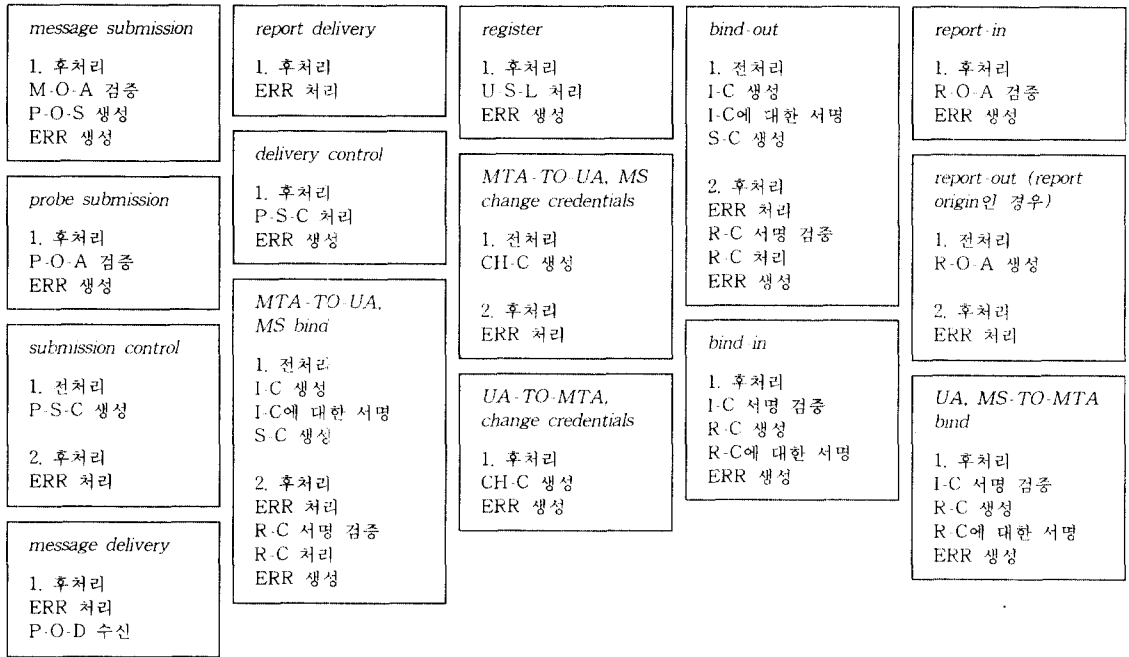


그림 4. MTA가 제공하는 정보보호 서비스

는 키에 관련된 작업을 수행한다. 기본적인 기능은 키의 생성, 분배, 인증서 발급과 같은 일이다. DSA는 EDI 시스템에서 주로 주소에 관련된 작업을 담당한다. 정보보호 서비스의 기능을 수행하기 위해서는 여기에 키관련 정보의 저장 검색 변경 등의 기능이 추가되어야 한다.

4.1 SES의 기능 및 구성

SES는 UA, MS, MTA들이 제공해야하는 정보보호 서비스를 처리해주는 주기능을 담당한다. 이를 위해서 SES는 EDI 시스템 각 컴포넌트들의 서비스 요청 및 결과의 통보를 위한 인터페이스, SMS와의 상호 작업을 위한 인터페이스를 정의하였고, 자체적으로는 여러 가지의 정보보호 서비스에서 공통으로 사용하는 처리과정을 통합한 공통 사용함수 처리부, 각 서비스별 처리 과정을 담당하는 서비스별 함수 처리부로 구성하였다. 이 중에서 SMS와의

상호 작용을 위해서 다음과 같은 세가지 기능을 담당하는 인터페이스를 정의하였다.

정의한 인터페이스는 첫째, 정보보호 서비스의 제공을 위해서 본인의 비밀키 또는 상대방의 공개키 획득을 위한 KMA(Key Management Agent) 인터페이스, 둘째, 인증 데이터를 부인봉쇄시에 사용할 수 있도록 저장하고, 자신과 연결되는 컴포넌트들의 신원 정보, 정보보호 문맥 등을 등록 관리하기 위한 데이터베이스 인터페이스, 셋째, 정보보호 서비스 관련 행위의 감사 추적을 위한 AMA(Audit Management Agent) 인터페이스들이다. 이와 같은 분석을 통해서 SES가 정보보호 서비스의 제공을 위해서는 정보보호 서비스 처리를 위한 주 모듈과 기존 컴포넌트와의 인터페이스, KMA와의 인터페이스, AMA와의 인터페이스, 데이터베이스와의 인터페이스로 구성되어야 한다는 것을 알았다. 그림 6은 이와같은 SES의 개념도이다.

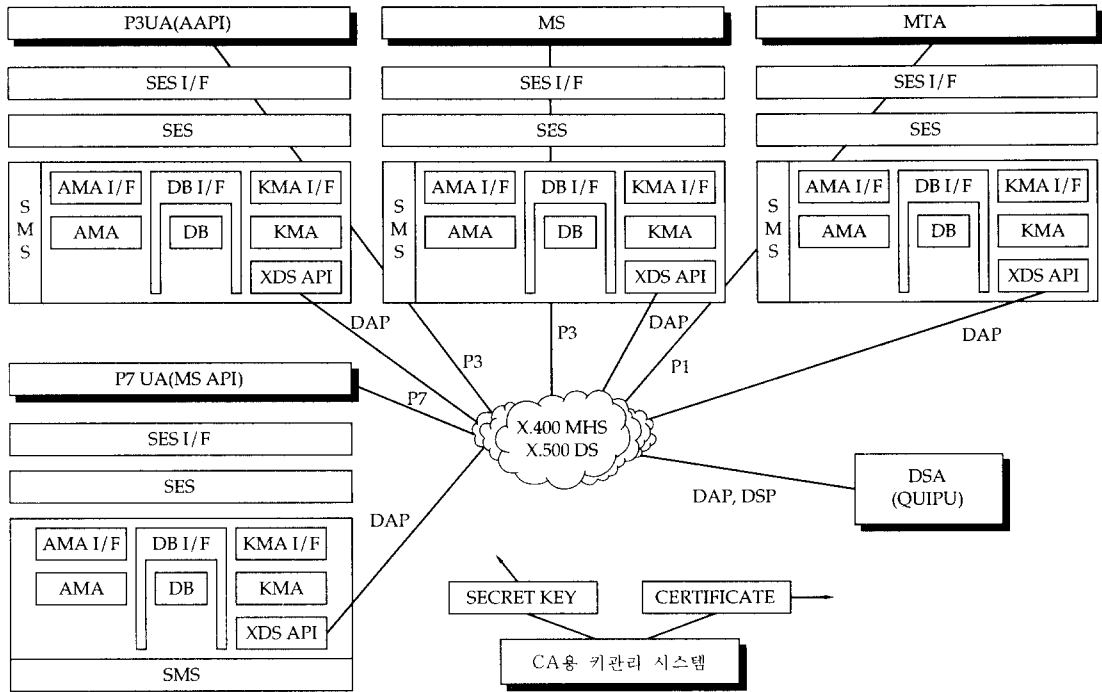


그림 5. SEDI의 구성도

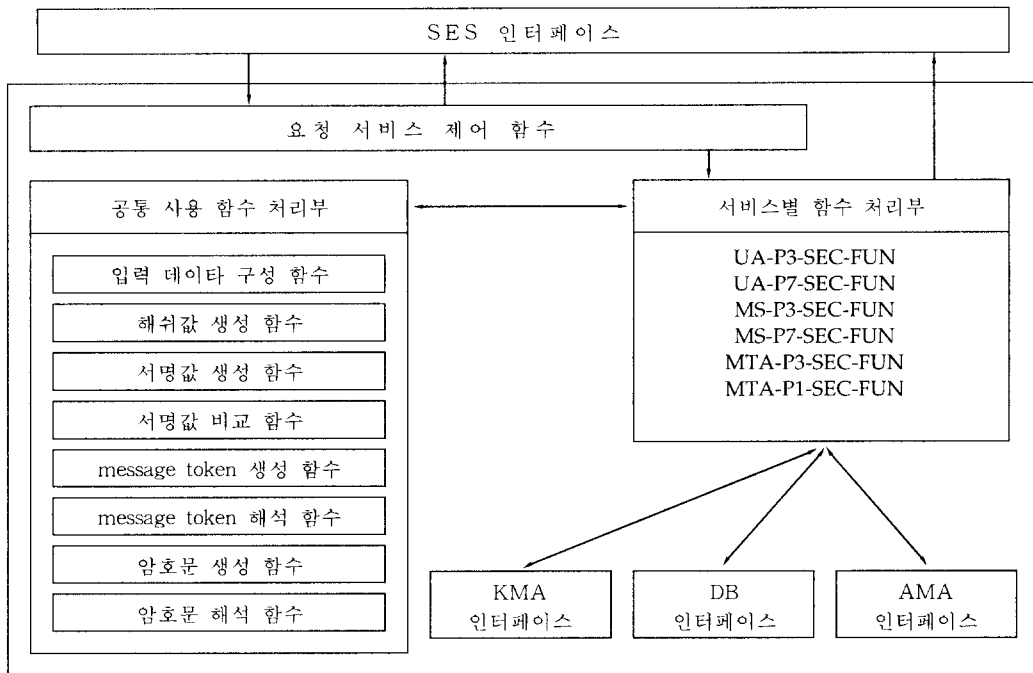


그림 6. SES의 구성도

4.1.1 SES 인터페이스

여기서 정의해야 할 인터페이스는 EDI 시스템의 각 컴포넌트와 SES와의 통신을 위한 시스템 호출 형태의 함수를 정의한다. 기본 골격은 메시지 송수신에 관련된 행위 별로 하나의 함수 호출을 제공하고, 이 함수의 입력 변수에 요청 서비스의 종류, 서비스 제공을 위해 필요한 입력 데이터를 설정하고, 출력 변수에는 요청된 서비스의 결과 값을 담은 데이터, 처리 결과의 상태를 설정하도록 설계하였다.

4.1.2 요청 서비스 제어함수

이 함수는 요청된 서비스들간의 관계를 조사하여 서비스처리 순서의 결정 또는 서비스들간의 충돌성 등을 조사 결정하여 서비스별 함수처리부로 서비스를 요청하든지 서비스 처리에 문제가 있다고 판단된 경우는 SES 인터페이스를 통해서 거절한다. 즉 본 함수는 UA, MS, MTA별 SES의 관리 임무를 수행한다.

4.1.3 서비스별 함수 처리부

서비스별 함수 처리부는 SES의 핵심 부분이라고 할 수 있다. 이 부분은 어떤 컴퍼넌트와 결합하느냐에 따라서 달라질 수 있다. 즉 이 부분은 각 컴포넌트들에 관련된 서비스들을 처리하는 부분이다. 각 컴포넌트에 관련된 서비스의 종류 및 기능은 3장에서 정의하였다.

4.1.4 공통 사용 함수 처리부

이 함수는 정보보호 서비스를 제공하는데 사용되는 함수들 중에서 많은 서비스가 공통적으로 사용하는 것들을 모아놓은 부분이다. 공통 사용 함수 처리부를 정의함으로서 해쉬 함수, 서명 알고리즘, 암호 알고리즘 등의 변

경, 교체, 관리면에서 많은 장점이 있다.

4.1.5 KMA와의 인터페이스

EDI 컴포넌트용 정보보호 모듈에서 일부 정보보호 서비스를 제공하기 위해서는 발신자의 비밀키 또는 수신자의 공개키가 필요하고 이들 정보는 디렉토리 시스템을 이용해서 제공 받는다. 따라서 디렉토리 시스템과의 인터페이스가 필요하다.

4.1.6 DB 인터페이스

정보보호 서비스의 처리과정에서 처리 결과 또는 서비스 제공을 위해서 부가 기능이 필요하다. 부가 기능은 인증 데이터를 부인봉쇄시에 사용할 수 있도록 저장하는 기능, 자신과 연결되는 컴포넌트들의 신원 정보, 정보보호 문맥 등을 등록, 관리하는 기능 등이 포함된다.

4.1.7 AMA 인터페이스

이 인터페이스를 통해서 정보보호 서비스 처리과정에서 발생한 감사추적 정보의 저장, 검색, 변경등이 이루어진다.

4.2 SMS의 기능 및 구성

SMS는 SES에서 정보보호 서비스의 처리과정에서 필요한 기능을 제공한다. 제공하여야 하는 기능은 크게 세 가지로 분류된다. 첫째가 키 관련 기능으로 인증관련 서비스의 처리시 송신자의 비밀키 또는 상대방의 공개키가 필요하게 되고 이를 위해서 각 컴포넌트에 KMA가 제공되어야 한다. 둘째는 인증 데이터를 부인봉쇄시에 사용할 수 있도록 저장하는 기능, 자신과 연결되는 컴포넌트들의 신원 정보, 정보보호 문맥 등을 등록, 관리하는 기능 등이 필요하게 된다.

이를 위하여 데이터베이스가 관리되어야 한다. 셋째는 정보보호 서비스의 제공시 또는 정보보호 정책에 의해서 정해진 항목에 대해서 감사 추적 할 수 있는 기능이 제공되어야 한다. 그림 7은 이와같은 SMS의 개념도이다.

4.2.1 KMA(Key Management Agent)

KMA 인터페이스를 통해서 요구되는 키 관련 요청을 처리해 주는 곳으로 기능은 크게 발신자의 비밀키 및 공개키의 요구, 수신자의 공개키 요구, 관련 정보의 효율적인 처리를 담당하는 optimization 처리부, 신원 정보의 인증을 위한 validation 처리부, 디렉토리 시스템과의 접속을 위한 DSA 호출부로 나누어진다.

4.2.2 데이터베이스 관리부

데이터베이스 인터페이스를 통한 요구를 처리해주는 부분으로 이들 기능은 데이터베이스

의 검색, 변경, 저장 등의 기능을 수행한다.

4.2.3 데이터베이스

현재 SES가 정보보호 서비스를 제공하는 측면에서 관리가 필요한 데이터는 부인봉쇄에 사용할 데이터, 신원 정보 변경 서비스 및 바이딩 시에 처리되는 신원 정보, 정보보호 문맥을 위한 정보보호 레이블링, 감사 추적을 위한 정보 등을 관리한다.

4.2.4 AMA(Audit Management Agent)

정보보호 서비스를 처리하는 과정에서 발생하는 정보보호관련 행위중 정보보호 정책이 정한 바에 따라 정의된 행위들이 감사 추적되어야 한다. 특히 EDI 시스템에서 요구되는 정보보호 서비스들 중에서 명시적으로 검색 및 전달 증거, 검색 및 전달 부인 봉쇄는 AMA를 통해서 지원한다.

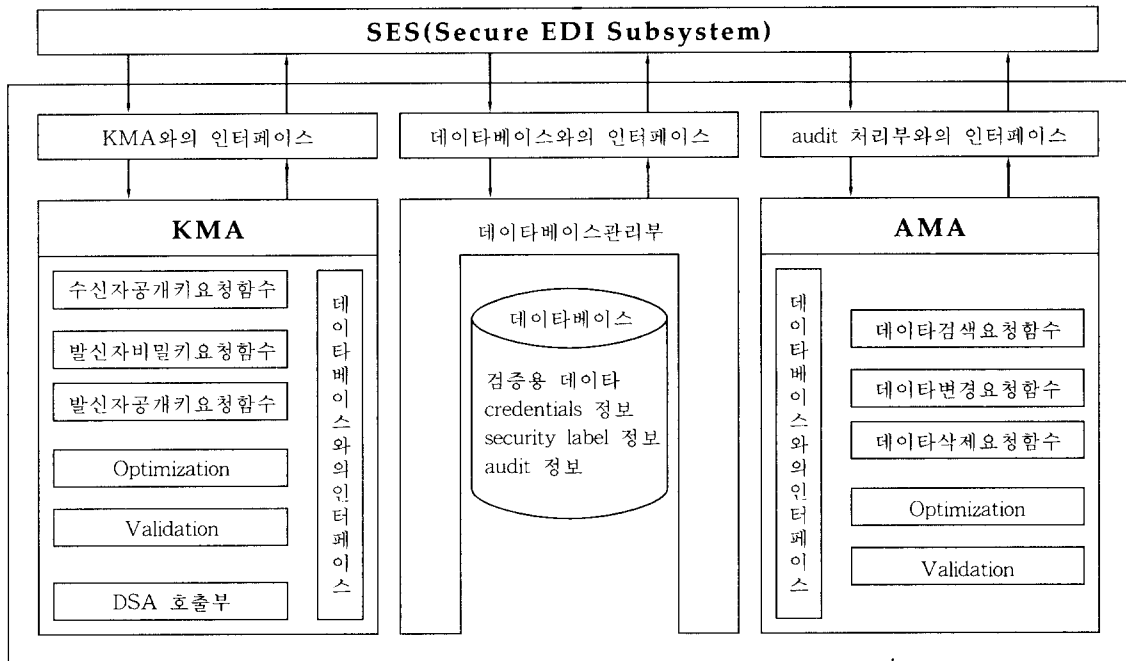


그림 7. SMS의 구성도

5. 결론

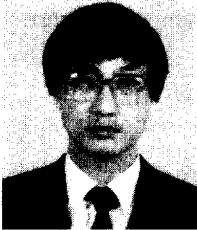
본 논문에서 제안한 SEDI는 기존 시스템과 독립적인 별도의 모듈로 구성하였고 이를 사용할 수 있는 인터페이스를 제공하였다. 따라서 EDI 시스템에 정보보호 서비스를 추가하기 위해서는 해당 프로토콜의 각 동작별로 정의된 인터페이스를 이용하면되기 때문에 기존 시스템에 많은 변경을 요구하지 않는다. SEDI는 SES, SMS, CA, DSA의 네가지 컴포넌트로 구성된다. 정보보호 서비스 처리를 위한 이들 컴포넌트들 사이의 동작도 기존 시스템에서 요구하지 않고 SEDI 자체에서 처리하기 때문에 기존 시스템의 변경을 요구하지 않는다. SES는 요청 서비스 제어함수와 공동 사용 함수 처리부가 정보보호 서비스의 추가, 삭제 또는 사용 알고리즘의 변경들을 담당하도록 설계하여 정보보호 서비스에 대한 유지 보수를 효율적으로 수행하게 하였다. 따라서 제안된 SEDI는 기존 EDI 시스템의 변경을 최소화하고 이식성을 높였으며 SEDI의 유지 보수성을 향상시켰다.

향후 부인 봉쇄 서비스를 제공하기 위한 절차 및 방법의 정의, 정보보호 문맥 서비스의 제공을 위한 정보보호 정책의 수립, 키 분배를 위한 방법의 정립을 위한 연구가 수행되어야 한다.

참 고 문 헌

- [1] ITU-T F.400 / X.400, Message handling services : Message handling system and Service overview, 1993.
- [2] ITU-T F.435, Message handling systems: Electronic data interchange messaging service, 1991.
- [3] ITU-T X.402, Message handling systems: Overall architecture, 1992.
- [4] ITU-T X.411, Message handling systems - Message transfer system: Abstract service definition and procedures, 1992.
- [5] ITU-T X.413, Message handling systems - Message store: Abstract service definition and procedures, 1992.
- [6] ITU-T X.419, Message handling systems: Protocol specification, 1992.
- [7] ITU-T X.435, Message handling systems: Electronic data interchange messaging system, 1992.

□ 著者紹介



윤 이 중

1988년 인하대학교 전산학과(학사)
 1990년 인하대학교 전산학과(석사)
 1990년 ~ 현재 한국전자통신연구소 선임연구원

※ 관심분야 : 컴퓨터/네트워크 보안, DBMS



이 정 현

1993년 숭실대학교 전자계산학과(학사)
 1995년 숭실대학교 전자계산학과(석사)
 1995년 ~ 현재 한국전자통신연구소 연구원

※ 관심분야 : 컴퓨터/네트워크 보안, ATM 트래픽 제어



김 대 호

1977년 한양대학교 전자공학과(학사)
 1984년 한양대학교 산업대학원 전자공학과(석사)
 1993년 Univ. of Maryland at College Park
 Dept. of Computer Science Visiting Scholar
 1977년 ~ 현재 한국전자통신연구소 책임연구원

※ 관심분야 : 전송분야, 통신 및 컴퓨터 보안



이 대 기

1966년 한양대학교 전자공학과(학사)
 1987년 한양대학교 전자공학과(석사)
 1980년 ~ 1992년 한국전자통신연구소 산업기술개발부장, 지상시스템연구부장
 1992년 ~ 현재 한국전자통신연구소 책임기술원
 한국통신정보보호학회 산학이사