관세청

4세대 국가관세종합정보망

전자문서 표준연계 지침서

2015.12.##

시 스 템	Global Service Gateway
보 안	일반
작 성 팀	GSG

LG CNS컨소시엄

※용어표

4세대 용어	용어 설명	3세대 용어
국가관세종합정보망	전자통관 편의를 증진하고, 외국세관과의 정보 교환을 통하여 수출입의 원활화와 교역안전을 도모하기 위한 전산처리설비와 데이터베이스에 관한 정보통신망의 통합체계 (관세법 327조) 관세행정 업무 뿐 아니라 사용자 서비스, 전자문서 유통, 내외부 연계 등 전체 시스템을 포함	인터넷통관시스템, 국가관세종합정보망
외부 사용자 시스템	수출입통관, 환급, 요건확인 등 관세청과 관련된 업무처리를 위하여 관세청과의 연계를 목적으로 하는 사용자S/W, 서버방식 등 외부 시스템 전체를 통칭	
사용자S/W	관세청과 업무처리를 위하여 개발된 PC기반 Client/Server 연계방식 프로그램의 약칭	
전자서고	관세청에 전자적으로 제출된 신고 첨부서류의 유통 및 보관을 목적으로 구축된 관리 시스템	
서버방식	관세청과 업무처리를 위하여 ebMS서버를 보유하고 관세청과 서버대서버로 전자문서를 연계하는 방식	
본인확인 표준	KISA(전자서명인증관리센터)의 식별번호를 이용한 본인확인 기술규격을 따른 표준으로 [www.rootca.or.kr-->기술규격-->공인전자서명인증체계 기술규격-->프로파일]에서 “1.5 식별번호를 이용한 본인확인 기술규격” 을 참조	
멀티문서	메타XML을 이용하여 n건의 문서를 n개의 페이로드에 적재하여 송수신하는 방법	
다중문서	n건의 문서를 조합하여 하나의 문서로 만들어서 1개의 페이로드에 적재하여 송수신하는 방법	

※본 문서에 사용된 명칭은 향후 4세대 국종망 사업 완료 후 변경될 수 있음

※ 약어표

약어	약어 풀이
ebMS	ebXML Message Service
CPA	Collaboration-protocol Agreement
CPP	Collaboration-protocol Profile
XMLDSIG	XML Digital Signature
SOAP	Simple Object Access Protocol
MIME	Multipurpose Internet Mail Extensions
DLL	Dynamic link library
SSL	Secure Sockets Layer

1. 개요

1.1 지침서 개요

1.1.1 필요성 및 목적

관세청 국가관세종합정보망과 외부 사용자 시스템 간에 원활한 전자문서 유통 및 연계처리를 위하여 관련 기술 규격을 정의한다.

1.1.2 적용 대상

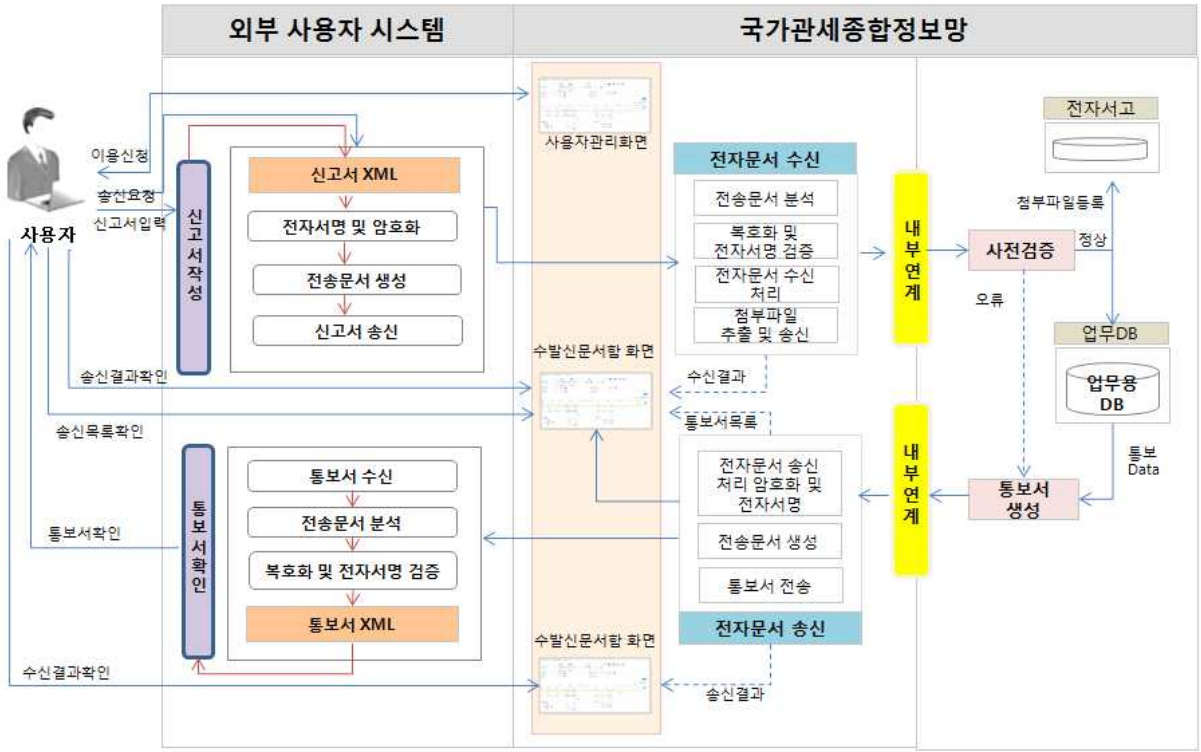
본 지침서는 수출입통관, 환급, 기타 민원, 유관기관 민원 등 신고업무를 처리하기 위하여 관세청 국가관세종합정보망과 연계 처리하는 모든 시스템을 대상으로 한다.

1.1.3 관리주체

본 지침서는 관세청이 유지/관리한다. 관세청은 사용자 환경의 변화, 관계법규의 개정, 기술발전 등으로 필요한 경우 본 지침서를 개정할 수 있다. 이 경우 외부 사용자 시스템은 개정된 지침서에 의해 관세청 국가관세종합정보망과 연계 처리하여야 한다.

1.2 업무처리 절차

1.2.1 연계처리 흐름도



1.2.2 업무처리 절차

□ **사전 준비 사항**

전자문서 연계처리를 위하여 사용자가 사전에 처리하여야 하는 사항으로 국가관세종합정보망에 이용신청사항 및 인증서를 등록하고, 문서함 ID를 부여받는다. (‘제7장 사용자 정보 관리 정책’ 참조)

① 공인인증기관 또는 등록관리기관에 방문하여 인증서(법인용 인증서 또는 서버용 인증서)를 발급받아, 회원가입신청서 작성 시 또는 개인정보 관리에서 인증서를 등록한다. (‘4.1 인증서’ 참조)
② 국가관세종합정보망의 [회원가입] 메뉴에 접속하여 이용신청사항을 등록한다.
③ 업체대표는 세관의 사용승인을 받아야 하며, 업체직원은 업체대표에게 사용승인을 받는다.
④ 문서함이 여러 개 필요한 경우 대표자 권한으로 국가관세종합정보망에 접속 후 [마이페이지 > 문서함관리 > 문서함사용관리] 메뉴에서 문서함ID를 추가 할 수 있다. (이 경우 문서함 ID별 사용할 업체직원 정보를 등록해야 함)
⑤ 전자문서 생성 및 전송 기능의 환경을 설정(사용자 ID, 문서함ID 등)한다.

□ 신고서 전송

① 사용자 시스템(자체 ERP시스템 또는 사용자S/W)에서 제공하는 Data를 이용하여 신고 Data를 생성한다.

② 신고 Data를 XML서식표준에 맞추어 XML전자문서(신고서)로 변환한다.

③ 자체 ERP시스템은 XML보안 표준에 따라 전자서명 및 암호화를 실시하고, 메시지 표준규약에 준한 전송메시지(패키지)를 생성한다.

④ 사용자S/W는 XML보안 표준에 따라 전자서명을 실시하고, 메시지 표준규약에 준한 전송메시지(패키지)를 생성한다.
(※사용자S/W는 SSL(Secure Socket Layer: 채널보안) 적용으로 XML 전자문서는 암호화를 생략한다.)

⑤ 생성된 전송문서를 국가관세종합정보망으로 통신표준에 맞추어 전송한다.

⑥ 국가관세종합정보망은 사용자로부터 신고서가 전송되면, 복호화 및 전자서명검사를 실시하고 신고서를 수록한다.

⑦ 국가관세종합정보망은 신고서 수신완료 여부를 전송한다.

국가관세종합정보망을 통하여 사용자가 직접 전송결과를 확인하는 방법

① 국가관세종합정보망의 [전자신고>처리현황] 메뉴를 이용하여 신고서 처리 과정을 확인한다.

② 정상적으로 전송된 경우 [마이페이지>문서함관리>발신문서함]에서 전송한 문서의 원문을 확인할 수 있다.

□ 통보서 수신

① 문서유통시스템에서 처리된 통보서XML(접수통보, 처리결과통보, 수리통보 등)은 문서함에 보관되어 국가관세종합정보망을 통해 확인 할 수 있다.

② 사용자 S/W를 이용하여 수신할 통보서를 다운로드한다. 서버 방식으로 연계한 경우 국가관세종합정보망의 문서유통시스템에서 직접 사용자 서버로 통보서를 송신한다.

국가관세종합정보망을 통하여 사용자가 직접 수신결과를 확인하는 방법

① 국가관세종합정보망의 [전자신고>처리현황] 메뉴를 이용하여 신고서 처리 과정을 확인한다.

③ 정상적으로 수신된 경우 [마이페이지>문서함관리>수신문서함]에서 수신한 문서의 원문을 확인할 수 있다.

2. 연계 프로토콜

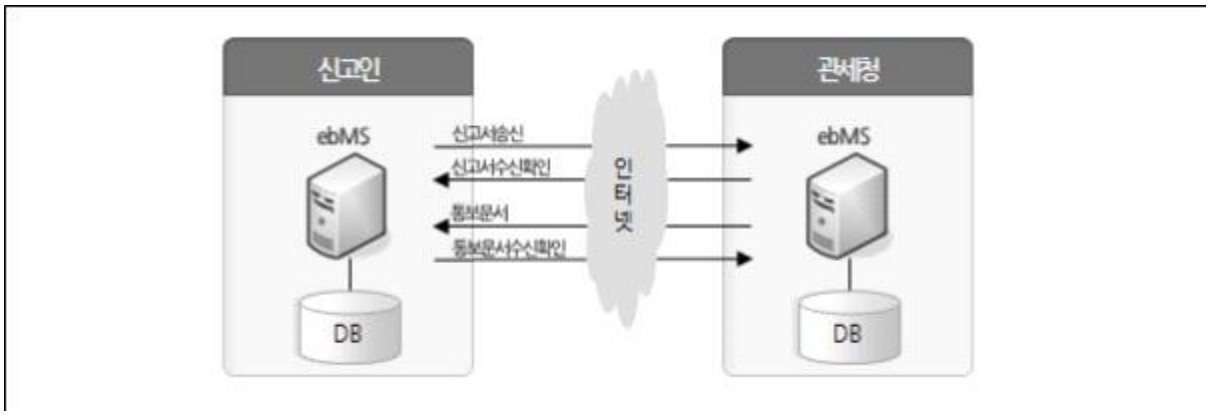
2.1 연계방식

국가관세종합정보망과 전자문서의 교환을 위해 아래의 2가지 ebMS서버방식과 사용자S/W와 연계방식이 있다.

2.1.1 ebMS 서버 방식

관세청의 문서유통시스템과 ebXML Message Service 2.0에 정의된 동기 방식 및 비동기 방식에 의한 메시지 송수신을 지원하는 서버를 구축하여 송/수신하는 방식이다. 서버 대 서버 방식은 ebXML CPA 2.0을 기준으로 작성된 프로파일을 교환하고 프로파일에 맞도록 전자문서를 송/수신한다.

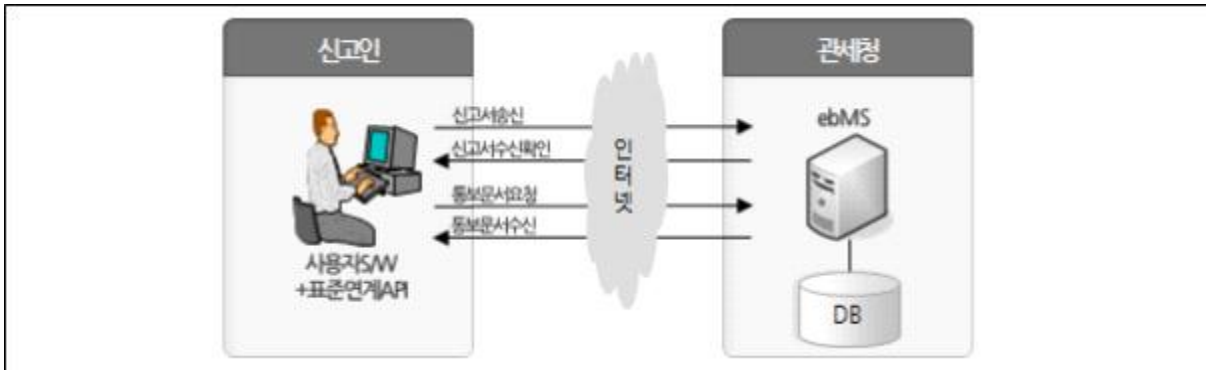
다음의 그림은 각종 신청서를 동기응답 방식에 의하여 송신을 하고 수신확인 메시지를 받은 후, 접수 통보 혹은 오류통보문서들은 CPA에 정의된 endPoint에 전자문서를 직접 송신하여 통보하는 방식이다. 이 방식을 이용하면 자사의 ERP시스템과 직접연계를 통하여 필요에 따라 실시간 전자문서 교환이 가능해지는 장점이 있고 송/수신 과정을 자동화할 수 있는 장점이 있다.



2.1.2 사용자 S/W와 연계방식

ebMS서버 없이 Client 프로그램을 관세청 문서유통서버와 Client/Server 방식 연계 규격에 맞게 개발하여 전자문서를 송수신 하는 방식이다.

사용자S/W는 XML문서를 생성하여 연계 규격에 맞게 문서를 송신하고 통보문서 수신을 위해 관세청 문서유통서버에 주기적으로 요청하여 가져가는 방식이다. 전자문서 송수신은 관세청에서 제공하는 표준연계API를 이용하거나 관세청 개발 규격에 맞게 자체 개발 할 수 있다.



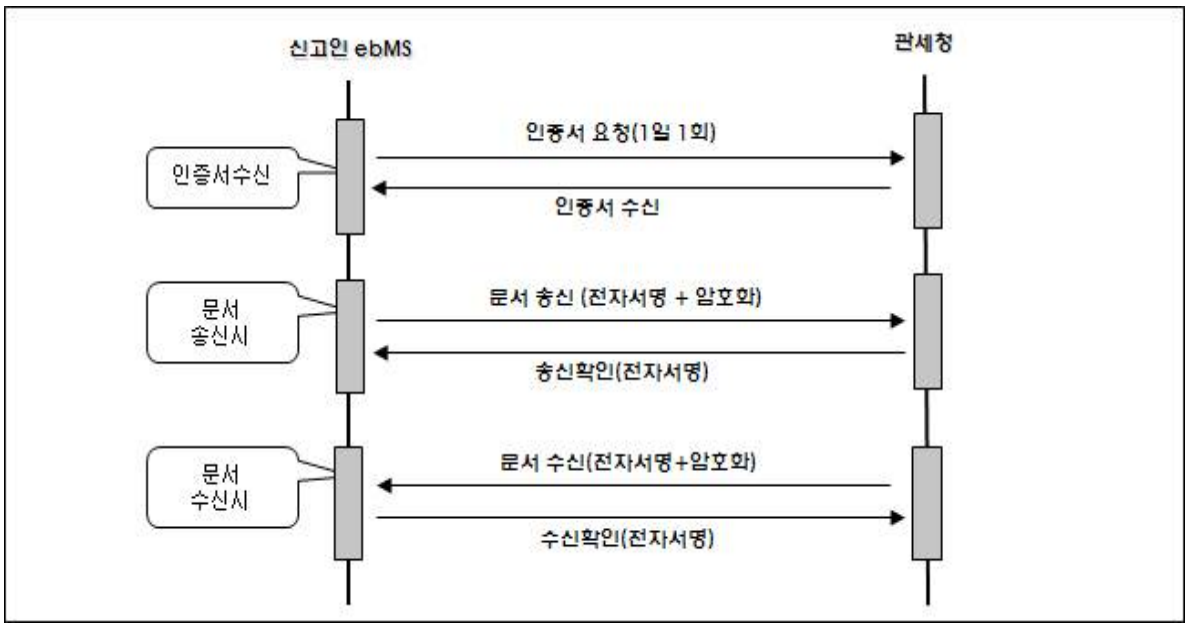
2.2 연계 처리 절차

연계 처리 절차는 ebMS 서버방식과 사용자 S/W연계 방식에 따라 다르며 통신 방식에도 약간의 차이가 있으며 구현 방법도 다르다.

	프로토콜	보안			문서수신방법	
	HTTP	전자서명	전자문서 암호화	채널암호화 (SSL)	직접수신	요청에 의한 수신
서버방식	O	O	O		O	
사용자 S/W 방식	O	O		O		O

2.2.1 ebMS 서버 방식의 연계 처리 절차

ebXML Message Server를 이용한 연계 방식은 다음의 그림처럼 3종류의 트랜잭션이 발생한다.



a. 인증서 수신 - 관세청의 암호화용 인증서를 매일 1회 첫 번째 문서를 전송하기

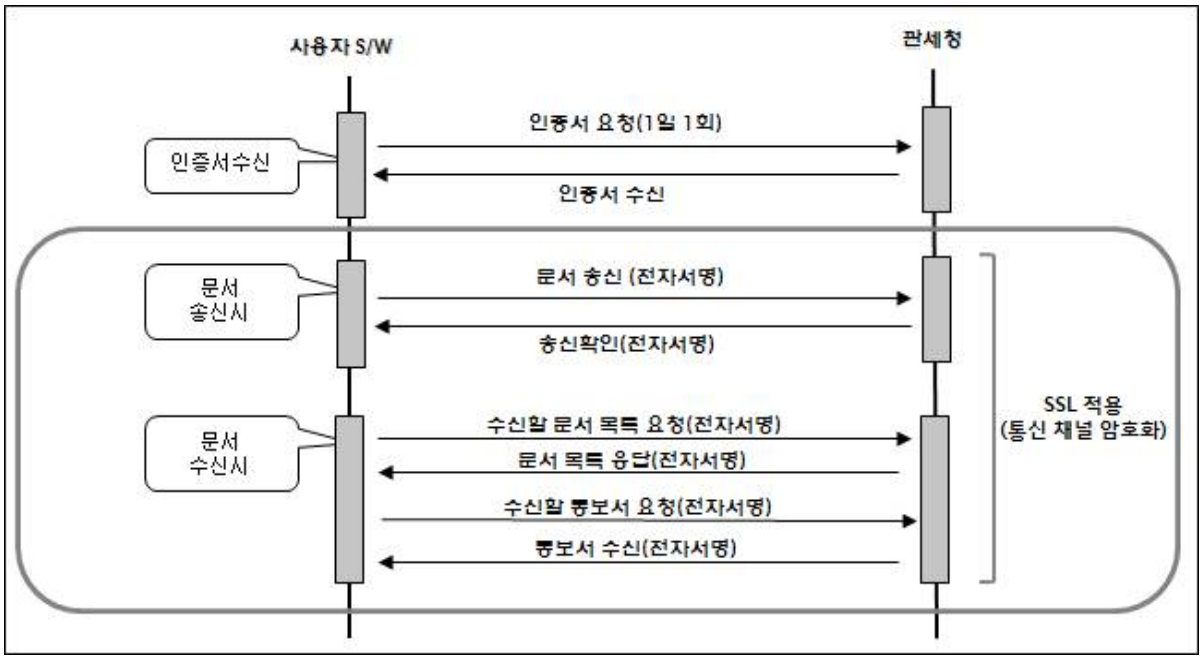
전에 수신하여 서버의 저장소에 저장한다. 이는 관세청 인증서의 갱신에 대비한 꼭 필요한 절차이다

b. 전자문서 송신시 암호화 및 전자서명 처리를 하여 국가관세종합정보망에 전송하고 전자서명된 수신확인 메시지를 받아 서명검증이 끝난 후에 트랜잭션 처리를 종결한다. 만약 문제가 있는 경우 CPA에 정의된 방법대로 오류 처리 및 재전송을 실시하여야 한다.

c. 국가관세종합정보망에서 통보문서를 수신하는 경우에는 관세청에서 CPA에 정의된 EndPoint에 문서를 직접 송신하며, 메시지 서버는 이를 수신 후 즉시 전자서명 수신확인 메시지(ACK메시지)를 응답하여야 한다.

2.2.2 사용자 S/W 연계 처리 절차

사용자 S/W를 이용한 연계 방식은 다음의 그림처럼 3 종류의 트랜잭션을 지원하는 API를 제공한다.



a. 인증서 수신 - 관세청의 암호화용 인증서를 매일 1회 첫 번째 문서를 전송하기 전에 수신하여 PC 및 서버의 저장소에 저장한다. 이는 관세청 인증서의 갱신에 대비한 꼭 필요한 절차이다

b. 전자문서 송신시 전자서명처리 및 SSL(통신 채널 암호화)을 적용하여 국가관세종합정보망에 전송하고, 수신확인 메시지를 받아 트랜잭션 처리를 종결한다. 만약 문제가 있는 경우 관세청이 정한 디폴트 CPA에 정의된 방법대로 오류 처리 및 재전송을 실시 한다.

c. 문서 수신시 SSL(통신 채널 암호화)을 적용하며, 국가관세종합정보망에 수신할 문서 목록을 요청하여 수신할 문서 목록을 응답 메시지로 받고, 그 문서 목록

에 있는 문서들을 수신 요청하여 응답으로 문서를 수신한다. (문서목록 요청과 통보서 수신의 자세한 내용은 부록6 사용자 S/W 개발 가이드 참고)

* 참고 : 사용자 S/W 개발 편의를 위해서 관세청에서 DLL 모듈을 제공한다. ('전자문서 표준연계 API 설명서' 문서 참고)

사용자 S/W를 이용한 연계 방식은 다음의 그림처럼 3 종류의 트랜잭션을 지원하는 API를 제공한다.

2.3 시스템 오류 처리

신고서 1건만 전송하는 경우와 신고서 2건이상 전송하는 경우 동일하게 국가관세종합정보망에서 신고서 수신처리 중에 오류가 발생하면 HTTP헤더에 오류코드를 넣어서 신고인에게 전송한다.

신고서 2건 이상 전송 할 경우에 복호화, 전자서명 검증, 스키마검증에서 오류가 있을시 시스템 오류통보를 신고인에게 전송한다.

구분	오류코드	시스템 오류통보
신고서 1건	HTTP 헤더에 정의해서 전송함	전송하지 않음
신고서 2건 이상	HTTP 헤더에 정의해서 전송함	복호화, 전자서명 검증, 스키마검증 오류발생시 전송함

위에 내용은 ebMS 서버방식과 사용자 S/W 연계방식 동일하게 적용되며 오류를 수정하여 신고서를 재전송하여야 한다. (최초전송일 경우 다시 최초전송으로 송신한다) 자세한 사항은 부록7. 오류코드와 부록8. 시스템 오류통보를 참조한다.

3. 전송 프로토콜

전송 프로토콜은 다양한 네트워크 및 응용 통신 프로그램 환경에서, 데이터의 손실 없이 상대방에게 전송할 수 있도록 규정하는 것으로, ebXML 표준에서는 HTTP, FTP, SMTP등을 사용할 수 있는 통신프로토콜로 제시하고 있다.

이러한 통신프로토콜들은 지원하는 데이터의 형식이나 처리방식 등에 따라 서로 다른 방식을 규정하고 있으므로 국가관세종합정보망에서 전송프로토콜 표준은 HTTP를 사용하도록 한다.

3.1 전송프로토콜 HTTP 통신

HTTP통신 표준은 RFC2616에서 규정하는 HTTP version 1.1을 사용한다.

3.1.1 HTTP를 통한 전자문서 전송

HTTP요청방법에는 GET 방식, POST방식이 존재하나, XML 전자문서를 전송하기 위해서는 아래 예와 같은 HTTP POST방식만 사용한다.

```
POST /servlet/ebXMLHandler HTTP/1.1
```

HTTP프로토콜에서는 이진데이터(binary data)를 지원하도록 되어 있으나, 본 지침서에서는 이진데이터를 사용하지 않도록 규정한다. 만일, 첨부파일과 같이 이진데이터로 구성되어 있는 데이터를 전송시는 Base64인코딩을 실시하여 전송도록 한다.

HTTP 메시지 생성규칙은 '5장 전자문서 패키징 정의'를 참조한다.

3.1.2 응답코드

HTTP응답코드는 RFC2616에서 규정한 응답코드를 사용한다. HTTP POST로 전송된 전자문서가 정상적으로 전송이 완료되면 '200 ok' 코드를 사용하며, 오류가 발생하는 경우 조건에 따라 3XX, 4XX, 5XX를 사용한다.

HTTP 본문에는 전송된 결과에 대한 처리 내용을 MIME의 형태로 전송되므로 정상처리의 경우 본문 확인이 필요 없지만 오류 응답코드가 전송되면 반드시 본문에 기술된 오류내용을 확인하도록 한다.

3.1.3 접근제어

불법사용자에 의한 전자문서 정보의 누출 및 시스템의 오작동을 방지하기 위하여 문서유통서버에 접근하는 모든 사용자에 대해 접근제어를 실시한다. 접근제어는 HTTP 헤더의 'Authorization'필드를 사용한다. 자세한 사항은 4.2 본인확인 표준과 5.2 HTTP헤더 구조를 참조한다.

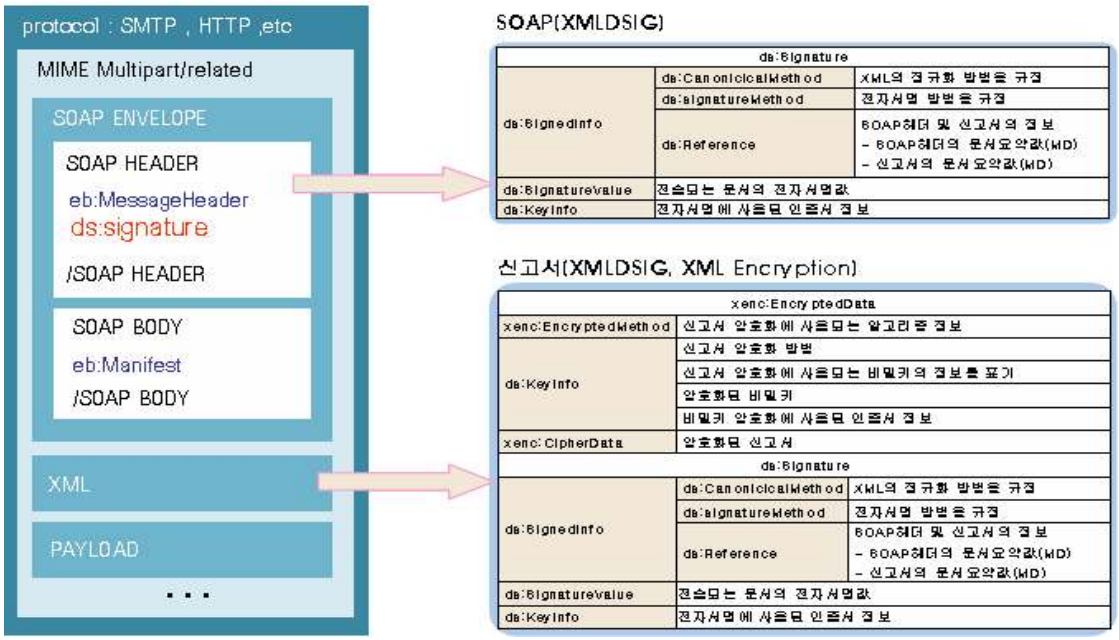
3.1.4 URL 정보

국가관세종합정보망의 URL 정보는 다음과 같다.

방식	운영 URL	테스트 URL
서버방식	http://gsg.customs.go.kr:8110/mediate/gsg/ebms/in/svr/receive	http://tgsg.customs.go.kr:8110/mediate/gsg/ebms/in/svr/receive
사용자 S/W방식	https://gsg.customs.go.kr:38120/mediate/gsg/ebms/in/usw/receive	https://tgsg.customs.go.kr:38120/mediate/gsg/ebms/in/usw/receive

4. 보안 표준

국가관세종합정보망에서 전자문서의 연계시 사용되는 SOAP 전송메시지의 보호를 위하여 SOAP표준과 W3C의 보안표준을 적용하여 전자문서의 신뢰성과 안정성을 향상하도록 한다.



전송메시지의 위변조 여부와 송신자의 신원확인을 위하여 전송헤더(SOAP Header)에 송신자의 전자서명을 실시한다. 전자서명 표준은 XMLDSIG의 표준을 사용도록한다.

또한 신고서의 데이터 누출 방지를 위하여 암호화를 적용하고 신고서의 위변조 여부를 확인하기 위해 송신자의 전자서명을 추가한다. 암호화표준은 W3C의 XML Encryption을 적용하고 전자서명표준은 XMLDSIG를 적용한다.

4.1 인증서

국가관세종합정보망에서 전자문서의 송/수신시 전송되는 데이터의 보호를 위하여 전자서명 및 암호화를 적용한다. 전자서명 및 암호화에 사용하는 인증서는 공인인증기관에서 발급하는 공인인증서 중 공인인증기관간 상호연동을 위한 표준이 적용된 범용인증서와 관세업무용 특별인증서만 사용한다.

4.1.1 사용 인증서 종류

공인인증기관에서 사용용도에 따라 범용, 서버용, 용도제한용으로 구분하고 발급대상에 따라 개인, 법인으로 구분하여 발급한다. 국가관세종합정보망에서는 다음과 같은 인증서만 사용한다.

업무구분	사용가능 인증서
MyCustoms 로그인	전자서명용 인증서(범용, 정부민원업무용, 관세청전자통관용)
송신문서 전자서명	전자서명용 인증서(범용, 정부민원업무용, 관세청전자통관용)
서버간 송수신문서 암호화	키분배용 인증서(범용, 정부민원업무용, 관세청 전자통관용)

*공인인증서 발급기관:

금융결제원(http://www.yessign.or.kr),
한국정보인증(http://www.signgate.com),
한국전자인증(http://www.crosscert.com),
코스콤(http://www.signkorea.com),
한국무역정보통신(http://www.tradesign.net)

4.1.2 인증서유효성 검사 방법

인증서 유효성 검사는 전자서명에 대한 신뢰성 여부를 확인하는 과정에서 가장 중요한 요소로, 전자서명 검사 시 반드시 인증서 유효성을 검사하여야 한다.

인증서 유효성 검증의 대상은 전자서명용 인증서를 대상으로 하며, 암호화에 사용되는 암호화 인증서의 유효성검사는 반드시 수행할 필요는 없으나, 암호화 수행 시 암호화인증서가 정상적인 상대방의 소유인지 확인할 필요가 있다.

인증서유효성검사 프로그램은 인증된 제품 혹은 한국정보보호진흥원의 인증서 유효성 확인 기술 규격을 만족하는 제품을 사용하여야 한다.

인증서 유효성 검증방법은 CRL을 이용한 방법과 OCSP를 이용한 방법이 존재함으로 연계기관(법인)의 편이성에 따라 선택 가능하다.

4.2 본인확인 표준

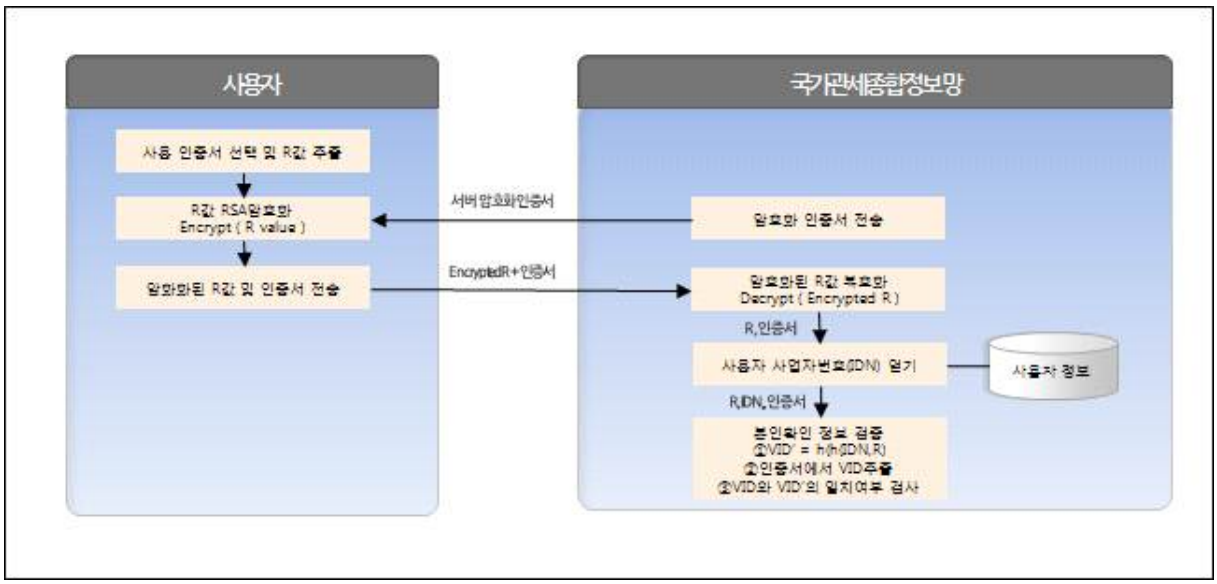
본인확인은 OFF-LINE에서 대면확인을 통하여 사용자의 신원을 확인하는 것과

동일하게 인터넷상에서 인증서를 이용하여 사용자의 신원을 확인할 수 있도록 하는 기능으로 국가관세종합정보망에서는 전자문서 송수신시 접속인증에 사용한다.

접속인증은 HTTP통신프로토콜의 Authorization 필드에 본인확인을 적용하여 보안수준을 높이도록 구성하였다.

본인확인 정보의 생성과 검증하는 방법은 응용프로그램에서 식별번호(사업자번호)의 소유 여부에 따라 검증방법이 달라지게 된다.

국가관세종합정보망에서는 사용자등록시 사용자의 식별번호(사업자번호, 주민등록번호)를 등록/관리함으로 본인확인 표준에서 기술된 "부록B 식별번호 검증예제"의 "2. 응용사이트에서 이미 식별번호를 알고 있는 경우"를 기본 모델로 하여 다음과 같이 본인확인을 처리한다.



a. 사용자는 사용하고자 하는 인증서를 선택한다. 선택된 인증서에서 신원확인에 사용할 R값(난수값:인증서 발급시 인증기관에서 입력함)을 추출한다.
b. 추출된 R값을 서버의 암호화 인증서로 RSA암호화 한다.
c. 암호화된 R값과 인증서를 국가관세종합정보망으로 전송한다.
d. 서버에서 암호화된 R값을 RSA복호화한다.
e. 사용자 DB에서 사용자의 사업자번호(식별번호(IDN))를 얻는다.
f. R값과 IDN을 이용하여 가상식별번호(VID')를 얻은 후 인증서에 포함된 가상식별번호(VID)와 일치여부를 확인한다.

인증서의 VID == 검증을 위해 생성한 값 (VID′ = h(h(IDN, R)))

본인확인정보의 추출방법 및 생성 방법은 본인확인 표준(*http://www.rootca.or.kr > 기술규격 -> 공인전자서명인증체계기술규격 -> 프로파일 -> 1.5번의 식별번호를 이용한 본인확인 기술규격*)을 참조하도록 한다.

4.3 XML 전자서명 표준

전송되는 XML전자문서의 위변조 여부 및 송신자의 신원확인을 위하여 ebXML XMLDSIG(XML Digital Signature)에 기술된 전자서명을 적용한다.

4.3.1 적용 표준

본 지침서에서 사용하는 XML전자서명 표준은 다음과 같다.

구분	설명
XML-Signature Syntax and Processing	XML 전자서명의 구문 정의 및 처리 절차에 관련 표준 ☞ *http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/*

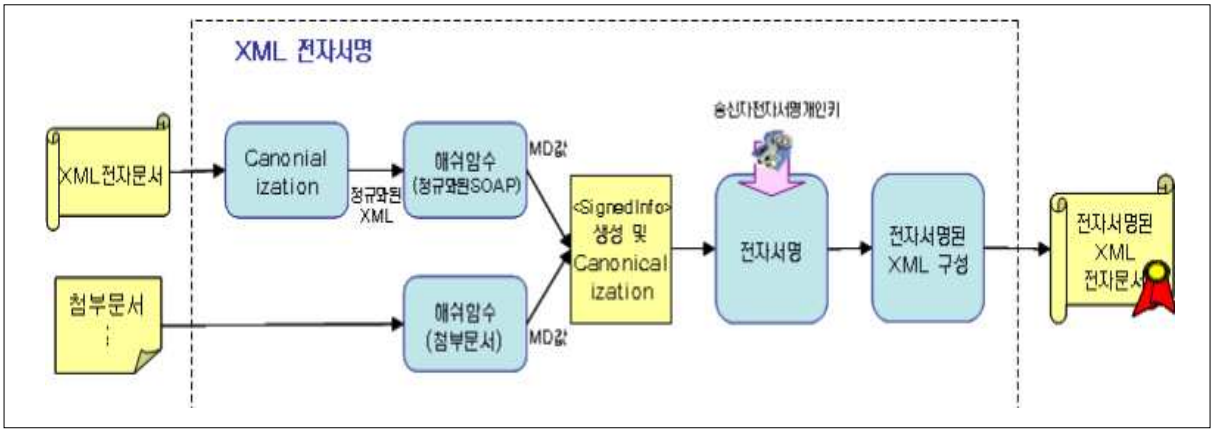
4.3.2 지원알고리즘

국가관세종합정보망의 XML 전자서명을 위하여 지원하는 알고리즘은 다음과 같다.

구분	알고리즘명	설명
Digest	SHA-256	전자문서의 문서요약값(Digest value)의 생성을 위해 사용하는 알고리즘 ☞ http://www.w3.org/2001/04/xmlenc#sha256
Signature	RSAwithSHA256	전자서명을 생성하기 위한 알고리즘(PKCS#1) ☞ http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Encoding	Base64	Binary데이터를 전송하기 위해 ASC문자열로 변환하는 알고리즘 (64Byte마다 newline 첨가) ☞ http://www.w3.org/2000/09/xmldsig#base64
Canonicalization	Canonical XML	XML의 정규화에 사용하는 알고리즘 ☞ http://www.w3.org/TR/2001/REC-xml-c14n-20010315
	Canonical XML with Comments	☞ http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
Transform	XPath	☞ http://www.w3.org/TR/1999/REC-xpath-19991116
	XLink	☞ http://www.w3.org/TR/2001/REC-xlink-20010627
	XPointer	☞ http://www.w3.org/TR/2002/WD-xptr-20020816
	Manifest	☞ http://www.w3.org/2000/09/xmldsig#Manifest
	Enveloped Signature	☞ http://www.w3.org/2000/09/xmldsig#enveloped-signature

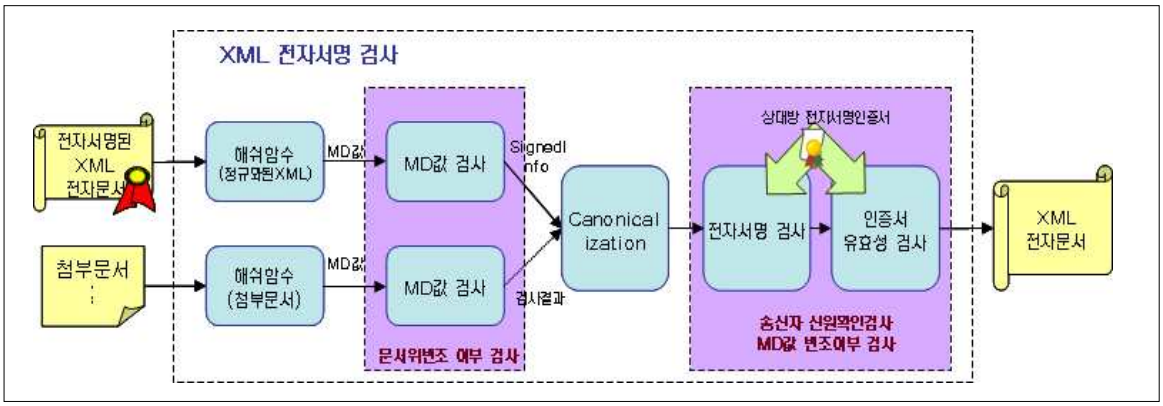
4.3.3 전자서명 및 전자서명 검증 절차

XML 전자서명은 XML전자문서에 대해 생성한 전자서명을 XML전자문서에 추가하는 과정으로 아래의 그림과 같은 절차로 이루어진다.



a. 입력된 XML전자문서와 첨부문서에 대해 해쉬함수를 이용하여 문서요약값(MD : Message Digest Value)을 생성한다. 단, 전자문서의 경우 정규화(Canonicalization)을 통하여 불필요한 리턴 값이나 스페이스를 제거하고 전송 중에 변경될 부분을 제외한 후 문서요약값을 생성한다.
b. 생성된 MD값들을 이용하여 SignedInfo 태그를 생성하고 정규화(Canonicalization)를 실시한다.
c. 정규화된 SignedInfo에 대한 전자서명값을 생성하여 Signature 태그를 생성한다.
d. XML전자문서에 Signature 태그를 추가하여 전자서명된 XML전자문서를 생성한다.

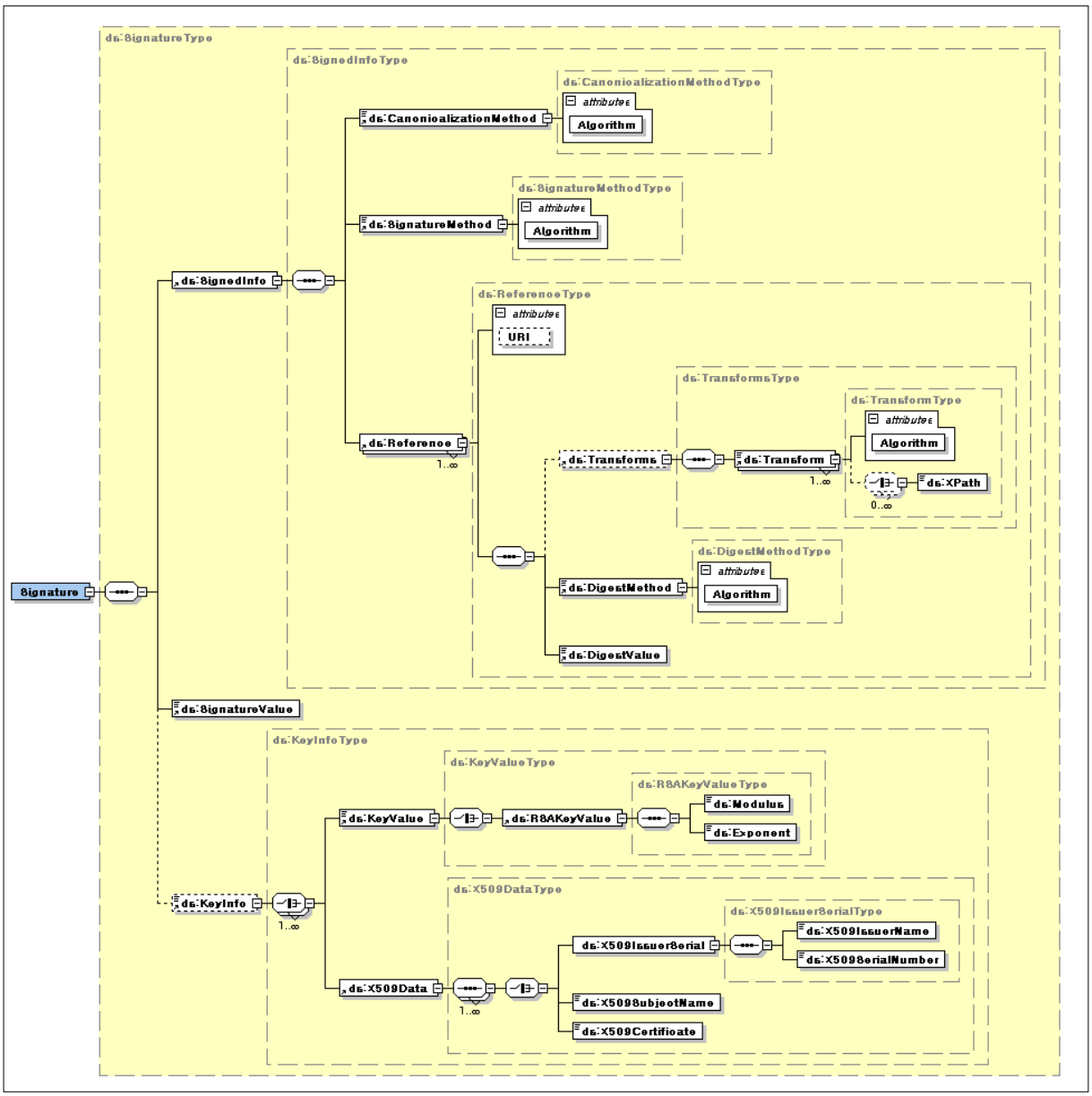
XML전자서명 검사는 수신한 전자문서의 **전자서명값의 검증**과 SignedInfo에 존재하는 **문서요약값의 검증** 과정으로 이루어 진다.



a. 입력된 XML전자문서와 첨부문서에 대해 해쉬함수를 이용하여 MD값을 생성하고 SignedInfo태그에 존재하는 MD값과 비교하여 문서의 위변조 여부를 확인한다.
b. SignedInfo에 대해 정규화(Canonicalization)를 실시하고 전자서명 검사를 수행한다. 전자서명 검사가 완료되면 송신자의 전자서명인증서에 대해 인증서 유효성 검사를 실시한다.

4.3.4 XML 전자서명 구조

XMLDSIG에 규정된 전자서명 구조는 다음과 같다.



전자서명 태그<ds:Signature>를 이용하여 전자문서와 전자서명을 구분하고, 전자서명 태그 하위에 전자서명 정보를 담는 <ds:SignedInfo>, 전자서명값 <ds:Signature Value>와 인증서의 정보<ds:KeyInfo>를 사용한다. 자세한 설명은 아래와 같다.

사용TAG	설명
<ds:Signature>	전자서명을 나타내는 엘리먼트 ☞ xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instan

	ce" xsi:schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"
<ds:SignedInfo>	전자서명 정보를 나타내는 엘리먼트
<ds:CanonicalizationMethod>	SignedInfo에 적용될 정규화 알고리즘 표기 ☞ Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
<ds:SignatureMethod>	전자서명에 사용될 알고리즘 표기 ☞ Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
<ds:Reference>	첨부파일(실제파일)의 정보를 표기 전송헤더(SOAP)를 전자서명하는 경우 ·1번째 <ds:Reference>태그는 SOAP자신을 표기 (URI는 공백으로 처리) ☞ URI="" ·2번째 <ds:Reference>태그는 XML신고서를 표기 ☞ URI="cid:ebxmlpayload00" XML 신고서를 전자서명하는 경우 ·1번째 <ds:Reference>태그는 XML신고서자신을 표기 (URI는 공백으로 처리) ☞ URI=""
<ds:DigestMethod>	첨부파일의 문서요약값(MD값)을 생성하기 위한 해쉬알고리즘 표기 ☞ Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"
<ds:DigestValue>	첨부파일의 문서요약값(MD값: Message Digest value) Transforms태그가 존재하는 경우 Trasforms을 적용 후 문서요약값을 생성한다.
<ds:Transforms>	첨부파일의 문서요약값 생성에 관련된 변환 규약
<ds:Transform>	문서요약값을 생성하기 위한 첨부문서의 변환 규칙을 표기 전송헤더(SOAP)를 전자서명하는 경우 ·1번째 Reference의 경우 SOAP자신을 표기함으로 SOAP에 대한 XPATH와 Canonical에 대해 다음과 같이 알고리즘을 표기한다. ☞ Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116" ☞ Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-2001 0315" ·2번째 Reference는 XML신고서를 표기함으로 다음과 같이 알고리즘을 표기한다. ☞ Algorithm="http://www.w3.org/TR/2001/REC-xml-c

	14n-20010315" XML 신고서를 전자서명하는 경우 ·1번째 Reference는 XML신고서를 표기함으로 다음과 같이 알고리즘을 표기한다. ☞ Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116" ☞ Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
<ds:XPath>	문서요약값을 생성하기 위한 범위를 설정 Transfoem 엘리먼트의 알고리즘을 XPATH로 설정하는 경우 표기한다. 예)전자서명의 범위 제외:*not(ancestor-or-self::Signature)*
<ds:SignatureValue >	<ds:SignedInfo>를 <ds:CanonicalizationMethod>로 정규화하여 <ds:SignatureMethod>에서 규정한 전자서명알고리즘을 이용하여 생성한 전자서명값 ·송신자의 전자서명인증서를 이용하여 생성한다. ·전자서명값은 Base64인코딩하여 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.
<ds:KeyInfo>	전자서명의 검증에 사용될 전자서명 인증서 정보를 나타내는 엘리먼트
<ds:KeyValue>	공개키 정보
<ds:RSAKeyValue>	인증서의 공개키 값
<ds:Modulus>	사용자 인증서의 Modulus 값 ·값은 Base64인코딩하여 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.
<ds:X509Data>	전자서명의 검증에 사용될 전자서명 인증서
<ds:X509SubjectName>	인증서 고유명 ·인증서 고유명에 특수문자가 포함되어 있는 경우 특수문자를 치환하여 입력한다.
<ds:X509IssuerSerial>	인증서 발급자(공인인증기관)의 정보를 표기한다.
<ds:X509IssuerName>	인증서 발급자(공인인증기관)의 인증서 고유명
<ds:X509SerialNumber>	인증서 발급자(공인인증기관)의 인증서 번호
<ds:X509Certificate>	전자서명의 검증에 사용될 전자서명 인증서 ·인증서는 Base64인코딩하여 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.

문서요약값은 전자문서 수신시 전자문서의 위변조여부를 확인하는데 사용된다. 만일, 전자문서 송수신 중에 변경이 발생하는 부분이 있는 경우 문서요약값 생성범위에서 제외하여야 한다.

○ 제외 대상

- 전자서명을 표시하는 <ds:Signature>
- SOAP 헤더에 입력될 수 있는 전자문서 Trace정보

문서요약값 생성범위에 제외된 정보는 <ds:XPath>에 표시하여 문서위변조 여부 검사시에 오류가 발생하지 않도록 한다.

전자서명 검증시 전자서명 정보에 인증서가 포함되어 있지 않는 경우 사용자의 인증서의 고유명을 사용하여 인증서를 발급한 공인인증기관의 LDAP(Directory Server)에서 인증서를 다운로드 하여야 한다. 본 표준에서는 전자문서의 전자서명검증의 편리를 위하여 <ds:X509Certificate>에 전자서명 생성에 사용한 인증서를 포함하도록 하였다.

XMLDSIG에는 표시된 엘리먼트 이외 많은 부분이 정의되어 있으나 본 지침서에서는 사용하지 않도록 하였다.

4.3.5 XML전자서명의 예

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              xsi:schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd">
            <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
                        </ds:CanonicalizationMethod>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha256"></ds:SignatureMethod>
                        <ds:Reference URI="">
                                    <ds:Transforms>
                                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                                                </ds:Transform>
                                                <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                                                            <ds:XPath>not(ancestor-or-self::Signature)</ds:XPath>
                                                </ds:Transform>
                                                <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
                                    <ds:DigestValue>gRsQHSHIUzm6/fZ07Z3PdL39w98=</ds:DigestValue>
                        </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>hx4f2/sgDQgS1v5QxWO9rePRJxI2U9QL/KBbQOpLDYUh1mlnVORLQvLh8sUj+t7n
                        vozD8X81UTzAa3dyumfUNFZwUfWbriPJzE+T6xm03z2/LA9aeKtxwas2oKQuGCMC
                        Azj8rrY3rVkDnjKLaF7a/ZeQT3alWOvsRuVjj1RsK9g=
            </ds:SignatureValue>
            <ds:KeyInfo>
                        <ds:KeyValue>
                                    <ds:RSAKeyValue>
                                                <ds:Modulus>
                                                            AMTVAYp5fXKUhXLy5PsTgt55pev90KGwqo+4A2F9bXcKUXPQIrpqAfwhUWtTh0sq
                                                            8CQ3J5KSHi+MZsatTO0elLXFXG9Xiv2/psFtrt+SQwtluxKtqU10kaLBcZRRHPdF
                                                            hz2QYcc/cgGtASNEQ+wUSIw0vxIWrD7gnDWGt0daXsmV
                                                </ds:Modulus>
                                                <ds:Exponent>AQAB</ds:Exponent>
                                    </ds:RSAKeyValue>
                        </ds:KeyValue>
                        <ds:X509Data>
                                    <ds:X509SubjectName>cn=전자서명,ou=licensedCA,o=kica,c=kr</ds:X509SubjectName>
                                    <ds:X509IssuerSerial>
                                                <ds:X509IssuerName>cn=signGATE CA,ou=licensedCA,o=KICA,c=KR</ds:X509IssuerName>
                                                <ds:X509SerialNumber>2489030</ds:X509SerialNumber>
                                    </ds:X509IssuerSerial>
                                    <ds:X509Certificate>MIIEPDCCA6WgAwIBAgIDJfrGMA0GCSqGSIb3DQEBBQUAMEcxCzAJBgNVBAYTAktS
                                                MQOwCwYDVQQKEwRLSUNBMRMwEQYDVQQLEwpsaWNlbnNlZENBMRQwEgYDVQQDEwtz
                                                ---------- 중간 생략 ----------
                                                pwA0z3GG7oJb2F6tiP5tf7eAP8Vtp6vtaThtA73vlUvBr2IMAvjix21W9yB+4Bbb
                                                nH9aEDQAJ2TUcts2msTBCbyo7l3LEobEjKrUx10JNlM=
                                    </ds:X509Certificate>
                        </ds:X509Data>
            </ds:KeyInfo>
</ds:Signature>
```

신고서에 대한 참조정보

전자서명값

송신자 인증서 정보

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
              si:schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd">
            <ds:SignedInfo>
                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
                         </ds:CanonicalizationMethod>
                        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"></ds:SignatureMethod>
                        <ds:Reference URI="">
                                    <ds:Transforms>
                                                <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature">
                                                </ds:Transform>
                                                <ds:Transform Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116">
                                                            <ds:XPath>not(ancestor-or-self::Signature)</ds:XPath>
                                                </ds:Transform>
                                                <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
                                    <ds:DigestValue>TypK0qmrNMZ8U0v24X+QHclxY5M=</ds:DigestValue>
                        </ds:Reference>
                        <ds:Reference URI="cid:ebxmlpayload00">
                                    <ds:Transforms>
                                                <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
                                    </ds:Transforms>
                                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha256"/>
                                    <ds:DigestValue>l8UdQk4kFGG7NHs0YAPV0AK5eQ4=</ds:DigestValue>
                        </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>CT/CQlOGLUhJ4MMw8GAZDi+AJeVebvHZsi94AxbDlPBfYnoliePXE+zj7bmpe5kd
                        fuqf/8X+avmmQVVcflQLS9q5wtNliCoJWwqvL1VjHdlSzdgpk5jROSE++3seX3j0
                        Rk91eVeZA+xMWlMYjqaftwsWubVMuZzVp1D0Gcjldy4=
            </ds:SignatureValue>
            <ds:KeyInfo>
                        <ds:KeyValue>
                                    <ds:RSAKeyValue>
                                                <ds:Modulus>
                                                            AMTVAYp5fXKUhXLy5PsTgt55pev90KGwqo+4A2F9bXcKUXPQIrpqAfwhUWtTh0sq
                                                            8CQ3J5KSHi+MZsatT00elLXFXG9Xiv2/psFtrt+SQwtluxKtqU10kaLBcZRRHPdF
                                                            hz2QYcc/cgGtASNEQ+wUSlwOvxlWrD7gnDWGt0daXsmV
                                                </ds:Modulus>
                                                <ds:Exponent>AQAB</ds:Exponent>
                                    </ds:RSAKeyValue>
                        </ds:KeyValue>
                        <ds:X509Data>
                                    <ds:X509SubjectName>cn=전자서명,ou=licensedCA,o=kica,c=kr</ds:X509SubjectName>
                                    <ds:X509IssuerSerial>
                                                <ds:X509IssuerName>cn=signGATE CA,ou=licensedCA,o=KICA,c=KR</ds:X509IssuerName>
                                                <ds:X509SerialNumber>2489030</ds:X509SerialNumber>
                                    </ds:X509IssuerSerial>
                                    <ds:X509Certificate>MIIEPDCCA6WgAwIBAgIDJfrGMA0GCSqGSIb3DQEBBQUAMEcxCzAJBgNVBAYTAktS
                                                MQ0wCwYDVQQKEwRLSUNBMRMwEQYDVQQLEwpsaWNlbnNlZENBMRQwEgYDVQQDEwtz
                                                ---------- 중간 생략 ----------
                                                pwA0z3GG7oJb2F6tiP5tf7eAP8Vtp6vtaThtA73vlUvBr2IMAvjix21W9yB+4Bbb
                                                nH9aEDQAJ2TUcts2msTBCbyo7l3LEobEjKrUx10JNIM=
                                    </ds:X509Certificate>
                        </ds:X509Data>
            </ds:KeyInfo>
</ds:Signature>
```

SOAP자신에 대한 참조정보

신고서에 대한 참조정보

송신자 인증서 정보

전자서명값

4.4 XML 암호화 표준

전송되는 XML전자문서의 정보누출 방지를 위하여 W3C의 XML Encryption을 적용한다.

4.4.1 적용 표준

본 지침서에서 사용하는 보안표준은 다음과 같다.

구분	설명
XML Encryption	XML 전자문서의 암호화 구문의 정의 및 처리 절차에 관련 표준 ☞ http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

4.4.2 지원알고리즘

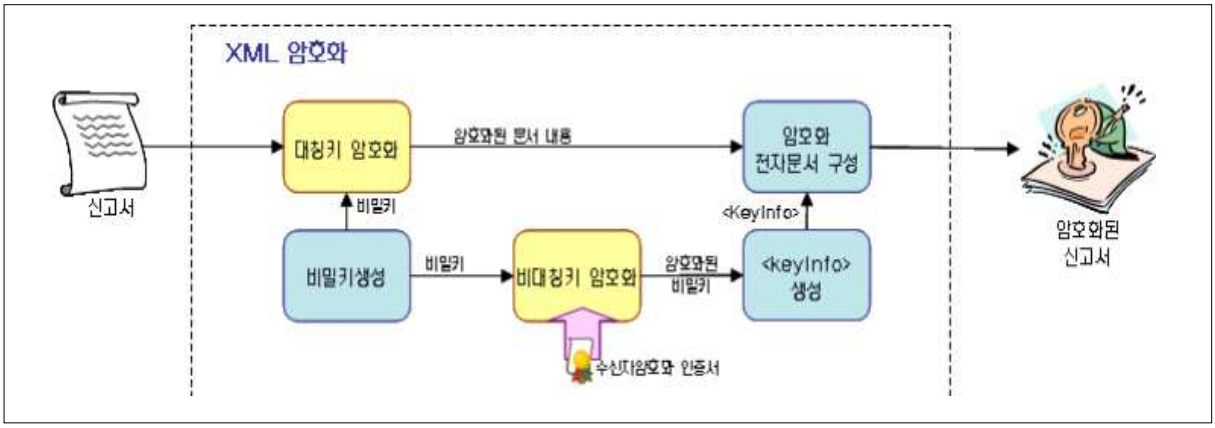
국가관세종합정보망에 전자문서의 보안을 위하여 지원하는 알고리즘은 다음과 같다.

구분	알고리즘명	설명
Block Encryption	SEED	전자문서의 내용을 암호화하기 위한 대칭키 암호화 알고리즘 ☞ http://www.tta.or.kr/2001/04/xmlenc#seed-cbc
Key Transpot	RSA	대칭키 암호화에 사용된 비밀키를 암호화하기 위한 비대칭키 알고리즘(PKCS#1) ☞ http://www.w3.org/2001/04/xmlenc#rsa-1_5
Encoding	Base64	Binary데이터를 전송하기 위해 ASC문자열로 변환하는 알고리즘 (64Byte마다 newline 첨가) ☞ http://www.w3.org/2000/09/xmldsig#base64

XML Encryption 표준에는 기술된 알고리즘이외에 많은 알고리즘이 기술되어 있으나, 국가관세종합정보망에서는 본 지침서에서 제시된 알고리즘만 사용도록 한다.

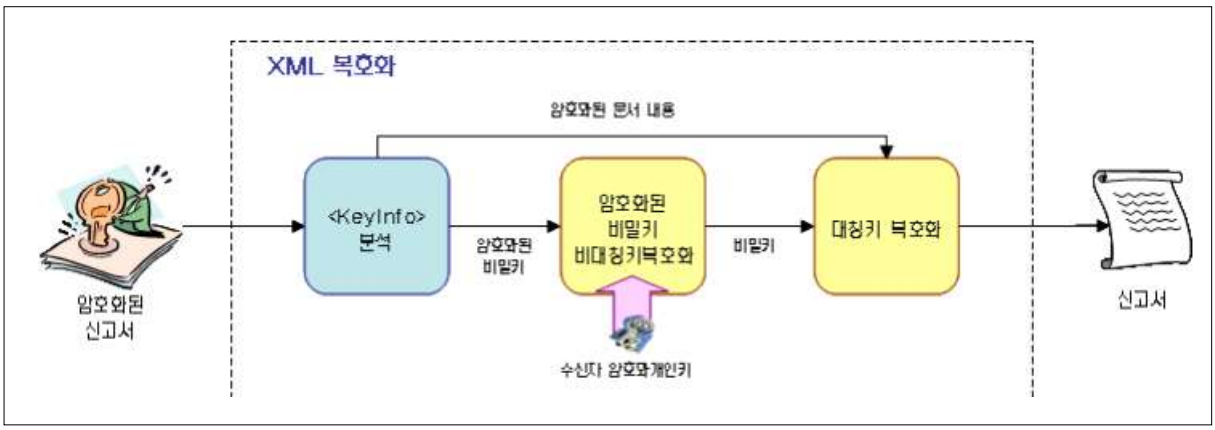
4.4.3 XML암호화 및 복호화 절차

XML암호화는 입력된 XML전자문서를 암호화한 후 결과를 XML형태로 재구성하고, 수신자가 복호화시 사용될 정보를 추가하는 과정으로 되어 있다.



a. 암호화에 사용될 비밀키를 Random함수에 의해 생성하고, 입력된 XML전자문서를 비밀키로 암호화한다. 주의) 입력된 XML전자문서는 정규화(Canonicalization) 되어 있어야 한다.
b. 비밀키를 수신자의 암호화인증서로 암호화한 후 KeyInfo를 생성한다.
c. KeyInfo와 암호화된 문서내용을 이용하여 암호화된 전자문서를 구성한다.
d. CBC운영모드를 이용하여 암호화하는 경우 초기벡터가 사용되며, 이 경우 암호화된 전자문서의 앞에 초기벡터를 연접한 후 Base64인코딩한다.

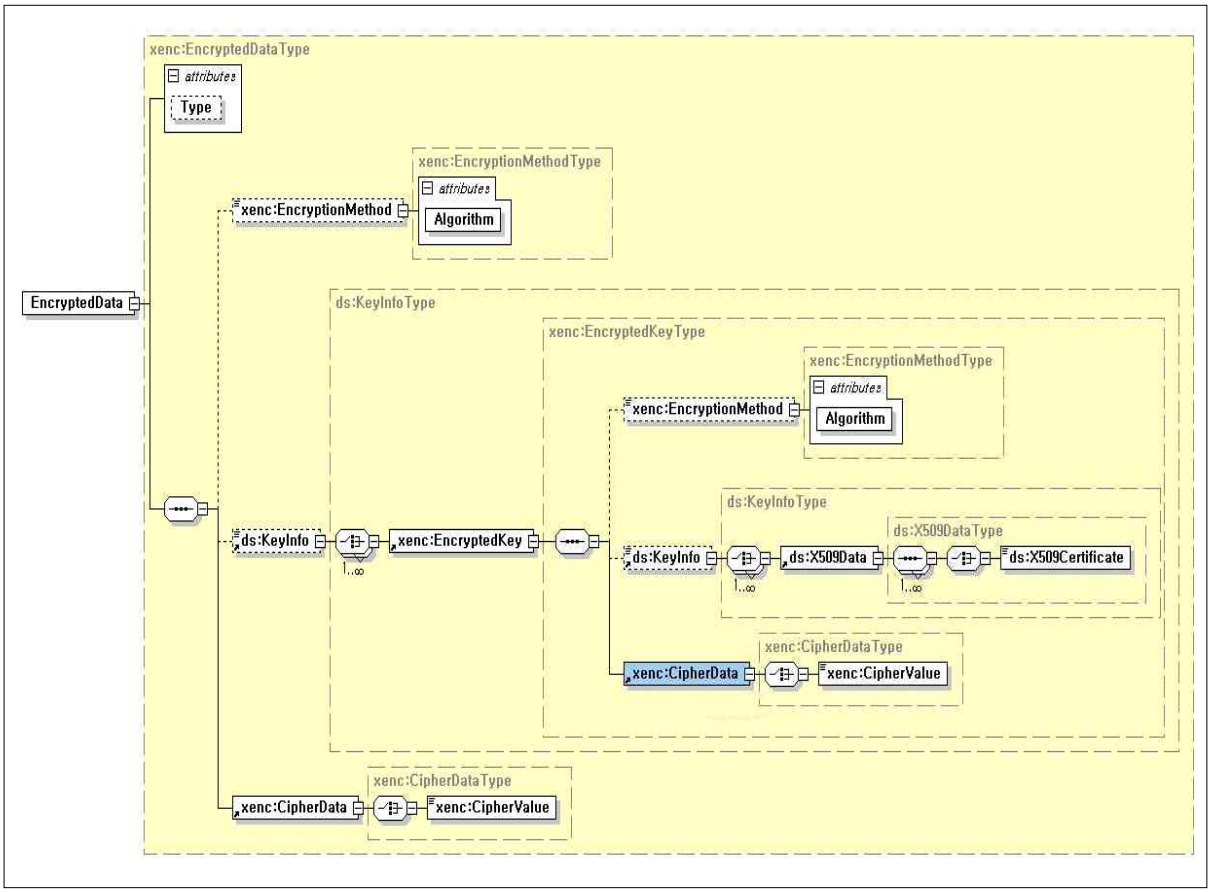
XML전자문서 복호화는 KeyInfo에 존재하는 비밀키를 이용하여 암호화된 신고서내용을 복호화하는 과정으로 이루어 진다.



a. 입력된 암호화된 신고서를 분석하여 KeyInfo와 암호화된 신고서를 분리한다.
b. KeyInfo에 존재하는 암호화된 비밀키를 수신자의 암호화개인키를 이용하여 복호화한다.
c. 복호화된 비밀키를 이용하여 암호화된 문서를 복호화한다.
d. CBC운영모드를 이용하여 복호화하는 경우 암호문에서 초기벡터를 추출하여 사용한다.

4.4.4 XML 암호화 구조

XML암호화 구조는 다음과 같다.



암호화된 정보를 표기하기 위하여 <EncryptedData>태그를 이용하여 암호화된 전자문서를 표기하고, <CipherData> 엘리먼트에 암호화된 데이터를 삽입하고, 암호화에 사용된 인증서 정보와 비밀키 정보를 입력한다. 자세한 설명은 아래와 같다.

사용TAG	설명
<xenc:EncryptedData>	XML 암호화를 나타내는 최상위 엘리먼트 Type속성을 이용하여 Element인지 Content인지를 구분한다. ☞ *Type="http://www.w3.org/2001/04/xmlenc#Element"* 또한 다음과 같은 엘리먼트의 속성 정의를 포함시킨다. ☞ *xmlns:xsi="http://www.w3.org/2001/XMLSchema-inst*

	ance" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" xsi:schemaLocation="http://www.w3.org/2001/03/xml.xsd http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd"
<xenc:EncryptionMethod>	XML내용의 암호화에 사용될 대칭키 암호화 알고리즘 을 표기 ☞ Algorithm="http://www.tta.or.kr/2001/04/xmlenc#seed-cbc"
<ds:KeyInfo>	대칭키 암호화에 사용된 비밀키의 정보를 표기 주) 이 엘리먼트는 반드시 EncryptedKey만 갖는다. ☞ xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
<xenc:EncryptedKey>	대칭키 암호화에 사용된 비밀키의 정보를 표기 주) 비밀키 정보를 표기하기 위해 반드시 KeyInfo 아래에 표기한다.
<xenc:EncryptionMethod>	비밀키의 암호화에 사용되는 비대칭키 알고리즘을 표기 ☞ Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"
<ds:KeyInfo>	비밀키 암호화에 사용된 암호화용 인증서의 정보를 표기
<ds:X509Data>	비밀키 암호화에 사용된 인증서를 표기
<ds:X509Certificate>	비밀키 암호화에 사용된 인증서 ·값은 Base64인코딩하여 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.
<xenc:CipherData>	암호화된 비밀키를 표기
<xenc:CipherValue>	비대칭키 알고리즘으로 암호화된 비밀키 ·수신자의 암호화인증서를 이용하여 생성한다. ·암호화된 값은 Base64인코딩하여 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.
<xenc:CipherData>	암호화된 XML 데이터를 표기
<xenc:CipherValue>	암호화된 XML 데이터 ·KeyInfo에 규정된 비밀키로 비대칭키 암호화하여 생성한다. ·IV를 사용하는 경우 암호문과 연접한다.(IV||암호문) ·Base64인코딩 후 삽입한다. 인코딩시 64byte마다 new line을 삽입한다.

XML Encryption에는 본 지침서에 표시된 엘리먼트 이외 많은 부분이 정의되어 있으나 본 지침서에서는 사용하지 않도록 하였다.

4.4.5 XML암호화의 예

```
<xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element"
            xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
            xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
            xsi:schemaLocation="http://www.w3.org/2001/03/xml.xsd http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/xenc-schema.xsd">

            <xenc:EncryptionMethod Algorithm="http://www.tta.or.kr/2001/04/xmlenc#seed-cbc"/>
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        <xenc:EncryptedKey>
                                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                                    <ds:KeyInfo>
                                                <ds:X509Data>
                                                            <ds:X509Certificate>
                                                            MIID3jCCAOegAwIBAgIDJfrHMA0GCSqGSIb3DQEBBQUAMEcxCzAJBgNVBAYTAktS
                                                            MQ0wCwYDVQQKEwRLSUNBMRMwEQYDVQQLEwpsaWNlbnNlZENBMRQwEgYDVQQDEwtz
                                                            aWduROFURSBDQTAeFw0wNDAyMDIwMjI3MDBaFw0wNTAyMDgxNDAxMDBaMIGNMQsw
                                                            ---------- 중간 생략 ----------
                                                            g+506D8j8Id85Pcs+2CttFA/9KiNQTxEkoLChV3ozPsaEQ==
                                                            </ds:X509Certificate>
                                                </ds:X509Data>
                                    </ds:KeyInfo>
                                    <xenc:CipherData>
                                                <xenc:CipherValue>
                                                            Chy07dr7eRrs0/7dPio4t4+jdXK3yjYQIrXUdxSq6GYx7BbUvigwYqonB/b+woWU
                                                            RwiOK9jdV+LMuGtTarPNvS04Hh0GVOXwxAzS5ronrB7fhRLhrRK8Pp23dSRWhERG
                                                            Ji91jryJ+Ay2loufHqQ3aXAWhd7wWcqQ4sM1X0YiRKw=
                                                </xenc:CipherValue>
                                    </xenc:CipherData>
                        </xenc:EncryptedKey>
            </ds:KeyInfo>
            <xenc:CipherData>
                        <xenc:CipherValue>
                                    9nR6q3zYUfqqoFD1hU5l8glsGEg67Qp8NAjKtgNHom7pJMoGxyF3qbt18SylmL1c
                                    fDiea6KPvocA/PbjyvkGYVFZI5jsHzKMbTzhCdrepUQoCRqjiam6Ekt3pHx8+4i/
                                    GPXNu/GHD0b7kfUQWLCDeLUnR4GUFIH20vAjnix4M1Vkl3HACKFC3Xuh3sGH7nxp
                                    ---------- 중간 생략 ----------
                                    dowmBlqYElo8lylqM+Mh+LSyDxSJj2Q0KueAnmGiVAhk5lZ+JdMNhfh0U+gqFi95
                                    KIzkhn3B3jFwxWDYRHXIVA==
                        </xenc:CipherValue>
            </xenc:CipherData>
</xenc:EncryptedData>
```

비밀키 암호화에 사용된 인증서 정보

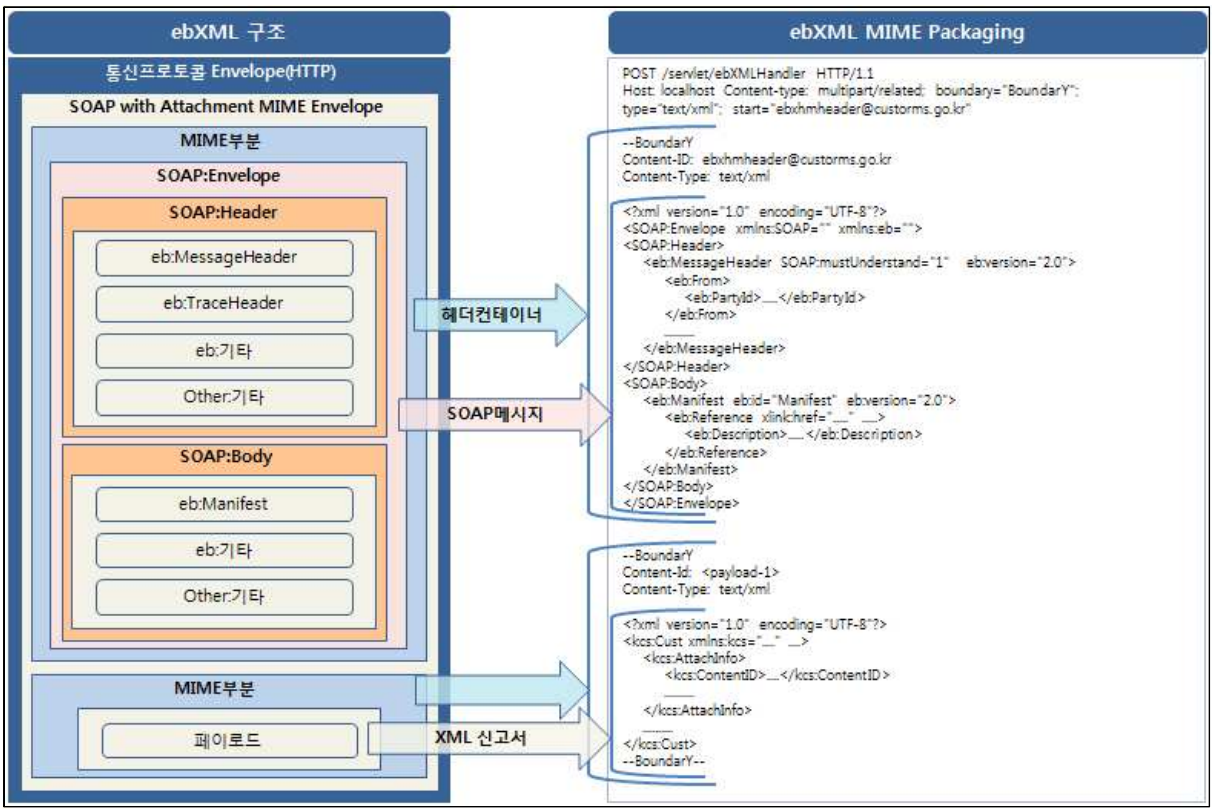
암호화된 비밀키

암호화된 전자문서

5. 전자문서 패키징 정의

5.1 연계 메시지의 구조

연계메시지는 ebXML Message Service 2.0 스펙에 정의된 패키징 표준을 따르며 부가적으로 HTTP헤더에 4.2절에 언급한 Authorization 속성을 추가하는 형식이다. ebXML Message Service에서 정의된 메시지 구조는 다음과 같다.



5.2 HTTP 헤더 구조

하이퍼 텍스트 전송 프로토콜 버전 1.1[HTTP 1.1](http://www.ietf.org/rfc/rfc2616.txt)는 사용되어야 할 최소 레벨의 프로토콜이다.

ebXML 메시지 서비스를 지원하기 위한 HTTP 메시지의 형성규칙은 다음과 같다.

a. ebXML 서비스 메시지 봉투의 Content-Type:Multipart/Related MIME헤더가 반드시 HTTP헤더에 표현되어야 한다.
b. ebXML 메시지 봉투를 구성하는 모든 MIME헤더는 HTTP헤더에 표현되어야 한다.

c. 필수 SOAPAction HTTP 헤더도 HTTP헤더에 포함되어야 하고, "ebXML"값을 가질 수 있다.

d. 국가관세종합정보망은 허가 받지 않은 접근을 방지하기 위해 접근제어 메카니즘을 적용한다. Authorization의 속성에 사용자의 신원확인정보를 암호화하여 추가하여야만 메시지 처리를 수행할 수 있다. (※ Authorization값은 [ID(Base64 인코딩):신원확인값((암호화 및 Base64인코딩)]의 규칙으로 생성한다.)

다음은 사용 예이다.

```
POST /service/ebXMLHandler HTTP/1.1
Host: localhost
SOAPAction: "ebXML"
Content-type: multipart/related; boundary="BoundarY"; type="text/xml"; start="ebxhmhead
er@customs.go.kr"
Authorization: Basic 4czqHGdsS4pfHF3BEeo4VF7pLY=:KoYMzj7dLTaQSDRFGHHUIKKJJ...NMHJK
Accept : text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection : keep-alive
Content-Length : 85571
locale : ko_KR
```

5.3 MIME 구조

5.3.1 MIME ROOT

루트 부분은 RFC2045에 준하는 Content-ID MIME헤더를 포함하고 Multipart/Related 미디어 유형에 대한 필수적인 파라미터에 추가하여 Start 파라미터가 항상 존재해야 한다. 미디어 유형은 SOAP 1.1 의 경우 “text/xml”, charset은 UTF-8로 설정한다.

```
Content-Type: multipart/related; type="text/xml"; boundary="boundaryValue";
start=messagepackage-123@example.com

--boundaryValue
Content-ID: <messagepackage-123@example.com>
```

5.3.2 헤더 컨테이너

Start헤더 콘테이너는 ebXML SOAP헤더를 담는 MIME구조이며 Content-Type은 SOAP 버전에 따라 정의된 내용으로 반드시 지정하여야 하고 SOAP메시지의 인코딩선언과 반드시 일치시켜야 한다.

```
Content-ID: <messagepackage-123@example.com>                              ---| Header
Content-Type: text/xml;  charset="UTF-8"                                    |
                                                                           |
<SOAP:Envelope                                                 --|SOAP Message
    xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/">      |          |
  <SOAP:Header>                                                  |          |
    …                                                            |          |
  </SOAP:Header>                                                 |          |
  <SOAP:Body>                                                    |          |
    …                                                            |          |
  </SOAP:Body>                                                   |          |
</SOAP:Envelope>                                               --|          |
                                                                           |
--boundaryValue                                                          ---|
```

5.3.3 페이로드 컨테이너

페이로드 컨테이너는 첨부문서가 있는 경우에 ebXML 메시지의 Manifest엘리먼트에 내용물을 표시하고 여기 표시된 첨부문서를 포함시키고자 할 때 사용하는 컨테이너이다.

```
   Content-ID: <domainname.example.com>  -------------| ebXML MIME       |
   Content-Type: application/xml         -------------|                  |
                                                      |                  | Payload
   <Invoice>                             -------------|                  | Container
     <Invoicedata>                                    |  Payload         |
       …                                              |                  |
     </Invoicedata>                                   |                  |
   </Invoice>                            -------------|                  |
```

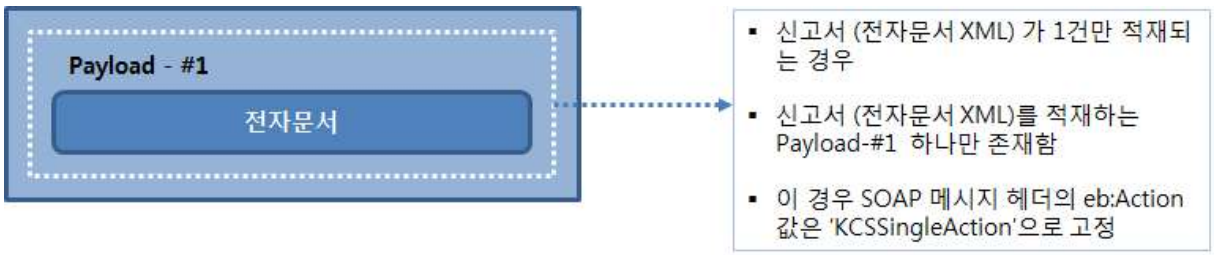
5.3.3.1 페이로드 구조

국가관세종합정보망에서의 페이로드(Payload) 구조는 신고서(or 요건확인신청서) 1건만 적재되는 경우와 그 외 2건 이상 전자문서가 적재되는 두 가지로 구분된다. 예외적으로 신고서(or 요건확인신청서)와 첨부파일이 포함되는 페이로드 구조는 관세청에서 정책적으로 정한 신고서 또는 요건확인신청서만 가능하다.

※첨부파일 동시 전송가능 서식은 관세청 정책에 따라 결정되며 별도 공지한다. 동시전송 허용된 서식만 첨부서류 동시전송 기능을 적용해야한다.

① 신고서(or 요건확인신청서) 1건만 적재되는 경우의 페이로드(Payload) 구조

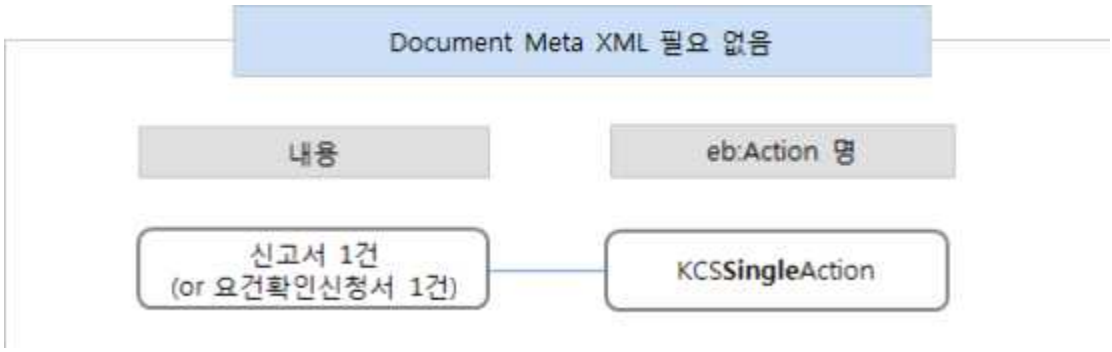
신고서(or 요건확인신청서) 1건만 적재되는 경우의 페이로드(Payload) 구조는 다음과 같다.



위의 경우 Document Meta XML은 생성하지 않아도 되며, 신고서(or 요건확인신

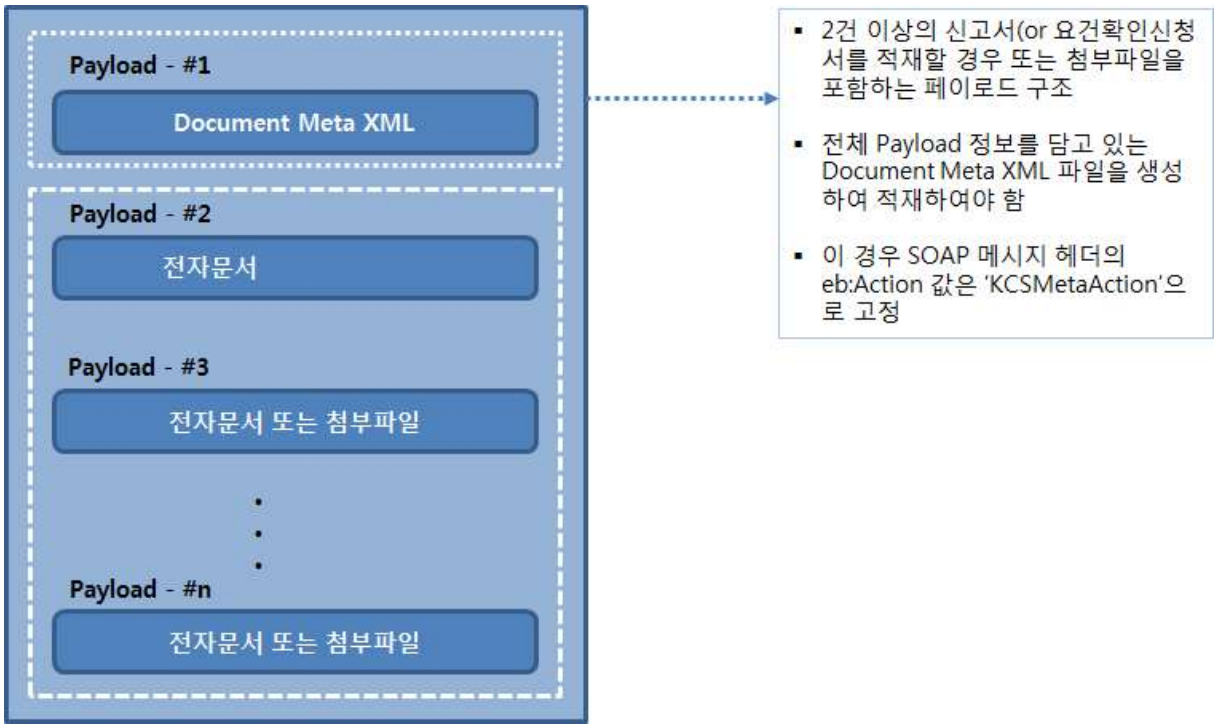
청서)를 적재한 Payload-#1만 존재하면 된다.

이 경우 SOAP 메시지 헤더의 eb:Action 명은 'KCSSingleAction'으로 고정한다.



② 2건 이상의 신고서(or 요건확인신청서)를 적재할 경우 또는 첨부파일을 포함 하는 페이로드(Payload) 구조

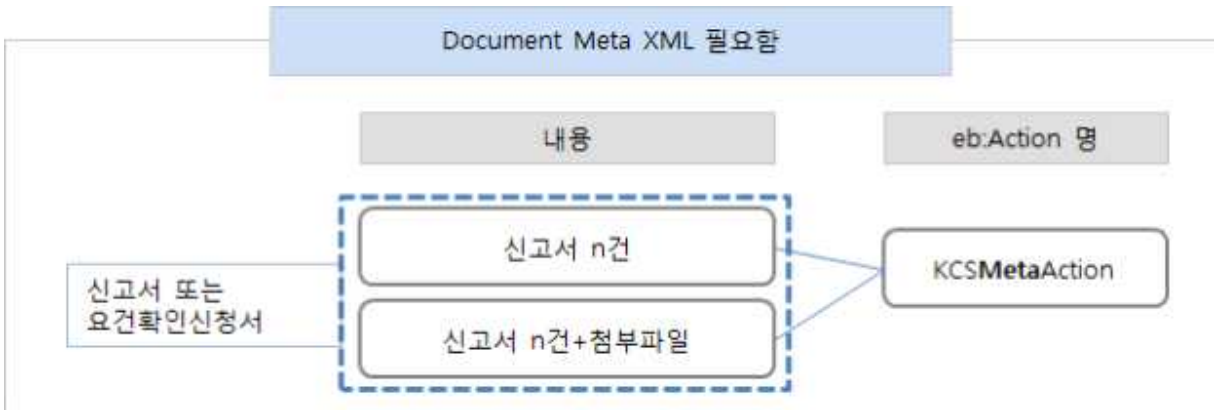
2건 이상의 신고서(or 요건확인신청서)를 적재할 경우 또는 첨부파일을 포함하는 페이로드(Payload) 구조는 다음과 같다.



위의 경우의 Payload-#1은 전체 Payload 정보(전자문서정보, 첨부파일정보)를 담고 있는 Document Meta XML 파일을 생성하여 적재하여야 하며, ebMS 송수신 시 반드시 존재하여야 한다.
(부록5. Document Meta XML 항목 정의서 참조)

Payload-#2 에는 신고서(전자문서XML)가 적재되고 Payload-#3 부터는 신고서(전자문서XML) 또는 첨부파일이 적재된다.

이 경우 SOAP 메시지 헤더의 eb:Action 명은 'KCSMetaAction'으로 고정한다.(신고서1건도 사용가능)



(부록3. Case별 ebMS 메시지 샘플 참조)

5.4 SOAP 헤더 구조

SOAP(Simple Object Access Protocol)은 분산환경에서 구조화된 정보를 교환하기 위한 프로토콜로 국가관세종합정보망에서 신고서(전자문서XML)를 교환하기 위해 사용한다.

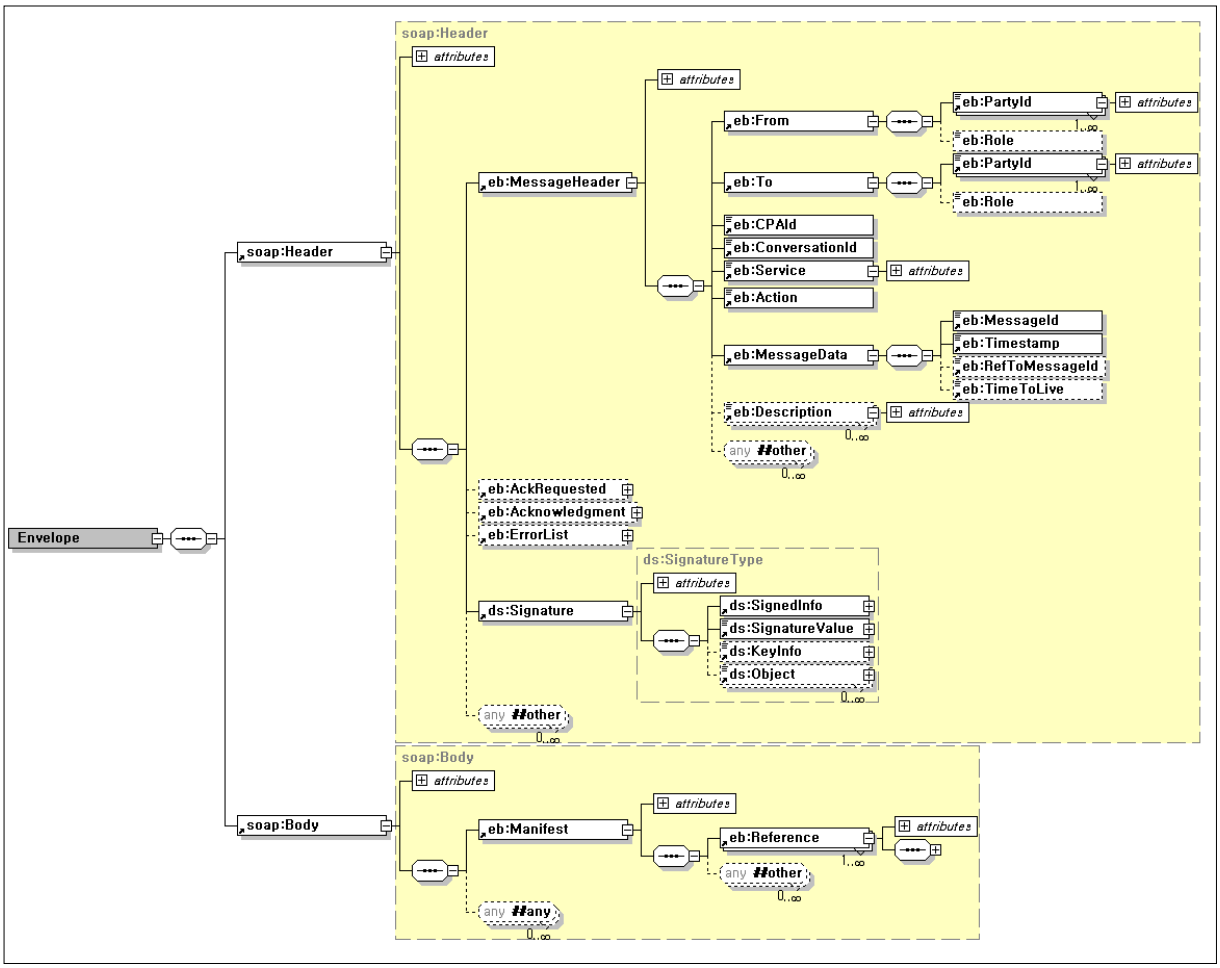
5.4.1 적용 표준

본 지침서에서 사용하는 SOAP Message 표준은 다음과 같다.

구분	설명
Simple Object Access Protocol (SOAP)	XML 전자문서를 교환하기 위한 프로토콜 ☞ Simple Object Access Protocol (SOAP) 1.1 http://www.w3.org/TR/SOAP/

5.4.2 SOAP 구조

SOAP의 구조는 다음과 같다.



SOAP메시지는 크게 SOAP Envelope, SOAP Header, SOAP Body로 구성되어 있다.

SOAP Envelope는 SOAP 메시지를 감싸는 가장 상위의 Element로 Envelope는 Header와 Body를 가질 수 있다.

- SOAP Header : Header는 응용프로그램이 전달하고자 하는 메시지의 정보 및 메시지의 전송정보를 규정하고 있으며, 이 헤더에는 송신자에서 수신자에게 메시지를 전달하기 위한 정보(송신자 ID, 수신자 ID, 전송방법 등)을 포함 하고 있다.
- SOAP Body : Body는 SOAP을 통해 전송하고자 하는 데이터로 구성된다.

5.4.3 SOAP Envelope

SOAP Envelope은 SOAP 메시지의 Root 항목으로 SOAP 메시지 내의 각종 네

임스페이스들을 선언 한다.
선언해야 할 네임스페이스들은 다음과 같다.

항목	Namespace URL
SOAP	http://schemas.xmlsoap.org/soap/envelope/
xlink	http://www.w3.org/1999/xlink
xsi	http://www.w3.org/2001/XMLSchema-instance
schemaLocation	http://schemas.xmlsoap.org/soap/envelope/ http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd

5.4.4 SOAP Header

SOAP Header는 다음과 같은 엘리먼트를 가진다.

- MessageHeader : 메시지의 라우팅 정보(FROM, TO 등)와 메시지에 대한 컨텍스트 정보를 포함한 필수 엘리먼트
- Signature : 메시지에 대한 전자서명을 포함하는 엘리먼트

SOAP Header의 예는 다음과 같다.

```
<SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_
0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader" eb:version="2.0">
    <eb:From>
      <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
    </eb:From>
    <eb:To>
      <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
    </eb:To>
    <eb:CPAId>KCSIPTJXA0001</eb:CPAId>
    <eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
    <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
    <eb:Action>KCSSingleAction</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20140703103114837</eb:MessageId>
      <eb:Timestamp>2014-08-05T07:10:55.971Z</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
</SOAP:Header>
```

5.4.4.1 MessageHeader

MessageHeader는 ebXML 메시지에 표현되어야 하는 필수 엘리먼트로 SOAP Header의 자식 엘리먼트로 표현되어야 한다. (부록5. SOAP메시지 참조)

MessageHeader는 다음과 같은 엘리먼트를 포함한다.

- FROM
- TO
- CPAID
- ConversationId
- Service
- Action
- MessageData

5.4.4.2 Signature

전송메시지에 대한 보안의 수단으로 송신자의 전자서명을 포함한다. 국가관세종합정보망에서는 모든 메시지 전송 시에 Signature를 포함시킨다. Signature Element는 XMLDSIG의 표준에 의하여 생성된다. (4장 보안표준 참조)

5.4.5 SOAP Body

SOAP Body는 다음과 같은 엘리먼트를 가진다.

- Manifest : Payload 컨테이너 또는 다른장소에 위치한 데이터를 가리키는 엘리먼트

SOAP Body의 예는 다음과 같다.

```
<SOAP:Body
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
        <eb:Manifest eb:id="Manifest" eb:version="2.0">
            <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
xlink:type="simple">
                        <eb:Description xml:lang="ko-kr">
                               C:WKCSIPTWCustomsDrawback.xml
                        </eb:Description>
            </eb:Reference>
        </eb:Manifest>
</SOAP:Body>
```

5.4.6 통보서 SOAP헤더

관세청에서 통보서를 송신하는 경우의 SOAP 헤더부분 예시이다. 통보서는 전자서명, 암호화 및 SOAP 전자서명을 하여 전송된다. 암호화는 사용자의 암호화 인증서를 사용한다. 전자서명, 암호화는 XMLDSIG 와 XMLENC 표준을 준용하며 상세한 내용과 예시, 사용되는 알고리즘은 4장.보안 표준을 참고한다.

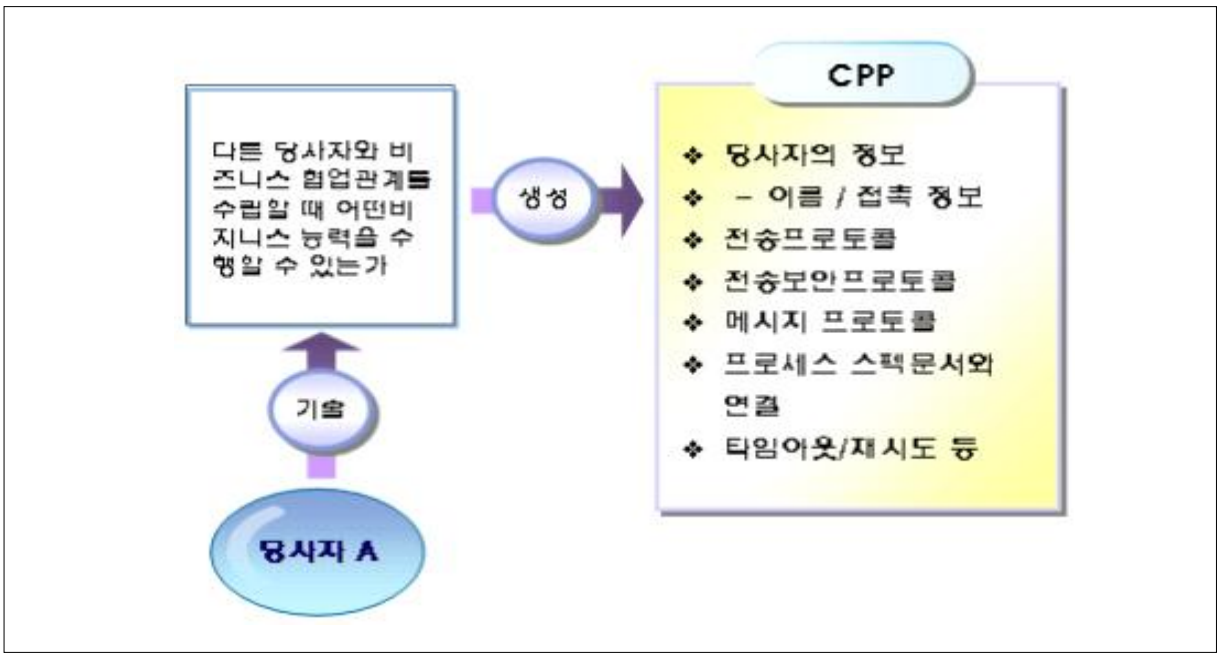
```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
                <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
                        <eb:From>
                                <eb:PartyId
eb:type="urn:kcsipt">KCSIPT00000000</eb:PartyId>

<eb:Role>http://portal.customs.go.kr:8080/xml/ebxml/kcsipt-ebBPSS.xml#DeclarantId_SANCR
T-5EA</eb:Role>
                        </eb:From>
                        <eb:To>
                                <eb:PartyId
eb:type="urn:kcsipt">XX123456789001</eb:PartyId>
<eb:Role>http://portal.customs.go.kr:8080/xml/ebxml/kcsipt-ebBPSS.xml#DeclarantId_SANCR
T-5EA</eb:Role>
                        </eb:To>
                        <eb:CPAId>CPA-XX123456789001</eb:CPAId>
                        <eb:ConversationId>001234567899U</eb:ConversationId>
                        <eb:Service
eb:type="portal.customs.dtml">bpid:kcsipt:portal.customs.go.kr:SANCRT-5EA$1.0</eb:Servi
ce>
                        <eb:Action>KCSSingleAction</eb:Action>
                        <eb:MessageData>
                                <eb:MessageId>20141203155992890689 5</eb:MessageId>
                                <eb:Timestamp>2014-12-03T09:37:31+0900</eb:Timestamp>
                        </eb:MessageData>
                        <eb:Description xml:lang="en-US">GOVCBRR99</eb:Description>
                </eb:MessageHeader>
                <eb:SyncReply SOAP:mustUnderstand="1" eb:version="2.0"
SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"></eb:SyncReply>
                <eb:AckRequested
SOAP:actor="urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH" SOAP:mustUnderstand="1"
eb:signed="true" eb:version="2.0"></eb:AckRequested>
.................................(생략)
```

6. 파트너 프로파일 및 약정서

6.1 CPP

6.1.1 CPP(협업 프로토콜 프로파일)이란

Collaboration-protocol Profile(협업 프로토콜 프로파일)은 관세청과 비즈니스 협업관계를 수립할 때 어떤 비지니스 능력을 수행할 수 있는가를 표현하는 XML문서이다. 여기에는 관세청의 정보, 이름/접촉정보, 전송프로토콜, 전송보안프로토콜, 메시지 프로토콜, 프로세스 스펙문서와 연결, 타임아웃/재시도 등을 기술하는 문서이다. 이는 향후 CPA작성을 목적으로 미리 사전 정보를 공개하는 문서이다.

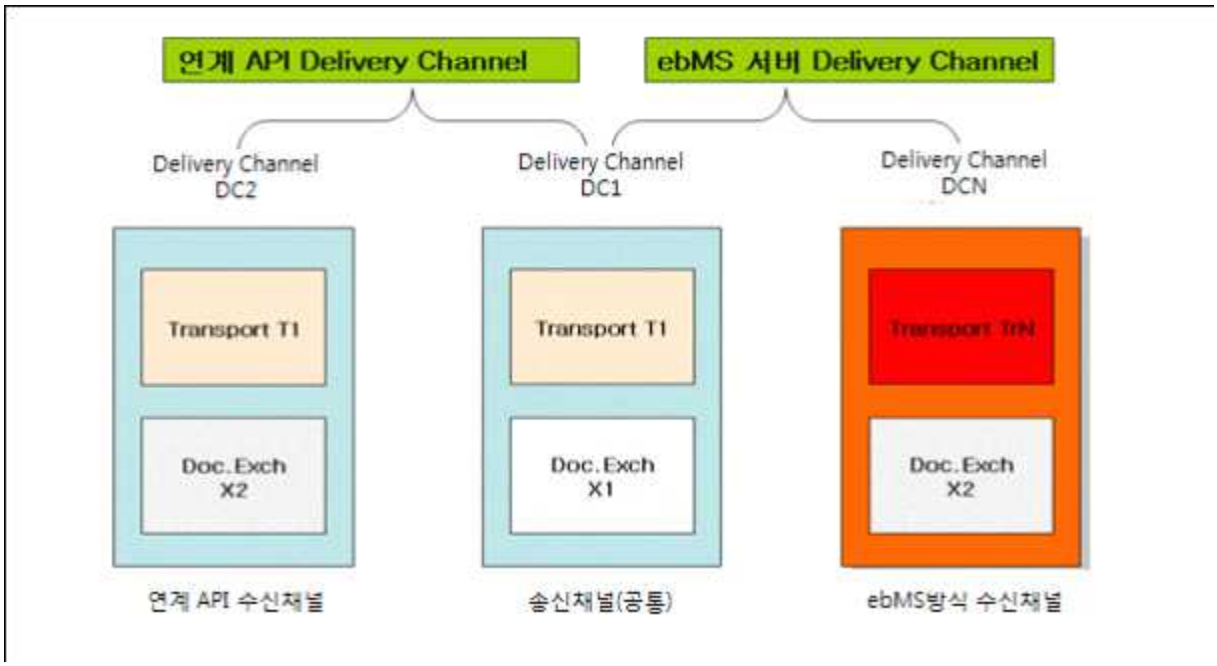


CPP파일은 국가관세종합정보망 자료실에 공개하여 누구든지 참조할 수 있도록 되어 있다.

6.1.2 Delivery Channel 정책

Delivery Channel 은 Transport(전송)와 DocExchange의 조합으로 이루어진다. 메시지 송수신방법은 국가관세종합정보망을 이용하는 고객 입장에서 기술하면 송신채널은 공통으로 이용하고, 수신채널은 고정IP가 없는 표준연계 API를 이용한 방식 또는 연계API를 자체 개발한 경우를 위한 수신채널과 ebMS고정 IP서버를

가진 서버의 직접수신방식을 지원할 수 있는 ebMS방식 수신채널의 2가지로 분류한다. 이렇게 하여 총 3가지의 Delivery Channel을 정의한다.



Transport T1은 SyncReply를 이용한 송신과 수신을 하며, Transport TrN은 ebMS서버 방식의 연결을 원하는 사용자가 준비해야하는 채널이다. 해당 채널을 준비하지 않은 사용자는 수신을 할 수 없다.

Doc.Exchange X1에서는 송신문서의 패키징방법, X2에서는 수신문서의 패키징 방법을 정의한다.

Delivery Channel은 Transport의 T1과 TrN, Document Exchange의 X1, X2의 조합을 통하여 DC1, DC2, DCN을 정의한다.

6.1.2.1 Delivery Channel DC1

Delivery channel DC1은 Transport T1과 Doc.Exchange X1과의 조합이다.

```
<tp:DeliveryChannel tp:channelId="DC1"
                    tp:transportId="T1"
                    tp:docExchangeId="X1"
                    tp:MessagingCharacteristics tp:syncReplyMode="responseOnly"
                    tp:ackRequested="always"
                    tp:ackSignatureRequested="always"
                    tp:duplicateElimination="always"
                    tp:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH">
</tp:DeliveryChannel>
```

SyncReplyMode와 ackSignatureRequested의 요건을 충족하여야한다

6.1.2.2 Delivery Channel DC2

Delivery Channel DC2는 Transport T1과 Doc.Exchane X2와의 조합이다.

```
<tp:DeliveryChannel tp:channelId="DC2"
                    tp:transportId="T1"
                    tp:docExchangeId="X2"
                    tp:MessagingCharacteristics tp:syncReplyMode="responseOnly"
                    tp:ackRequested="always"
                    tp:ackSignatureRequested="always"
                    tp:duplicateElimination="always"
                    tp:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH">
</tp:DeliveryChannel>
```

SyncReplyMode와 ackSignatureRequested의 요건을 충족하여야한다

6.1.2.3 Delivery Channel DCN

Delivery channel DCN은 Transport TrN과 Doc.Exchane X2과의 조합이다.

```
<tp:DeliveryChannel tp:channelId="DCN"
                    tp:transportId="T2"
                    tp:docExchangeId="X2"
                    tp:MessagingCharacteristics tp:syncReplyMode="responseOnly"
                    tp:ackRequested="always"
                    tp:ackSignatureRequested="always"
                    tp:duplicateElimination="always"
                    tp:actor="urn:oasis:names:tc:ebxml-msg:actor:nextMSH">
</tp:DeliveryChannel>
```

SyncReplyMode와 ackSignatureRequested의 요건을 충족하여야한다

6.1.3 Transport element

Transport(전송) element는 네트워크 통신 가능성을 정의한다. 관세청이 준비하는 채널인 T1과 ebMS 방식의 수신서버가 준비해야 할 TrN이 존재하는데 관세청에서는 T1만 정의하고, TrN에 대해서는 표준만 제시한다.

6.1.3.1 T1

Authorization은 Basic으로 되어 있으나 본문서의 4.2본인확인표준을 적용하여야 한다. T1을 이용하여서는 SyncReply방식으로 송신과 수신을 동시에 수행한다.

```
<tp:Transport tp:transportId="T1">
        <tp:TransportSender>
                <tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
                <tp:AccessAuthentication>basic</tp:AccessAuthentication>
        </tp:TransportSender>
        <tp:TransportReceiver>
                <tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
                <tp:AccessAuthentication>basic</tp:AccessAuthentication>
                <tp:Endpoint tp:uri="http://portal.customs.go.kr/ebms/msh"
                        tp:type="allPurpose"/>
        </tp:TransportReceiver>
</tp:Transport>
```

6.1.3.2 TrN

TrN은 ebMS 서버방식의 송수신을 원하는 사용자가 자신의 endPoint를 반드시 다음과 같은 방법으로 정의하여야 한다.

```
<tp:Transport tp:transportId="TrN"> <!--TrN 은 관세청에서 부여함-->
        <tp:TransportSender>
                <tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
<!--AccessAuthentication의 값 'basic' 은 5.2 본인확인 표준을 따라야 함-->
                <tp:AccessAuthentication>basic</tp:AccessAuthentication>
        </tp:TransportSender>
        <tp:TransportReceiver>
                <tp:TransportProtocol tp:version="1.1">HTTP</tp:TransportProtocol>
                <tp:AccessAuthentication>basic</tp:AccessAuthentication>
<!--tp:uri 의 endPoint는 관세청에 사용신청시 등록함-->
                <tp:Endpoint tp:uri="http://portal.customs.go.kr/ebms/msh"
                                tp:type="allPurpose"/>
        </tp:TransportReceiver>
</tp:Transport>
```

6.1.4 Doc Exchange

DocExchange는 문서를 주고 받는 문서에 대하여 상대방에게 동의를 구하기 위한 정보이다. 관세청에서는 국가관세종합정보망에 필요한 문서교환의 유형에 따라서 DocExchange를 정의하며 X1은 고객 입장에서 송신 시, X2는 수신 시 적용해야 할 Element이다

6.1.4.1 X1

X1은 문서 송신에 필요한 정의이며 다음과 같다. 유의할 사항은 XMLDSIG를 적용하여 수발신부인방지 처리를 하겠다는 부분을 적용하여야 한다.

tp:securityId 는 Security인증서 적용방안을 참고해야 한다.

```
<tp:DocExchange tp:docExchangeId="X1">
  <tp:ebXMLSenderBinding tp:version="2.0">
    <tp:ReliableMessaging>
      <tp:Retries>5</tp:Retries>
      <tp:RetryInterval>PT30M</tp:RetryInterval>
      <tp:MessageOrderSemantics>NotGuaranteed</tp:MessageOrderSemantics>
    </tp:ReliableMessaging>
    <tp:PersistDuration>P1D</tp:PersistDuration>
    <tp:SenderNonRepudiation>
      <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
      <tp:HashFunction>http://www.w3.org/2001/04/xmlenc#sha256</tp:HashFunction>
      <tp:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</tp:SignatureAlgorithm>
      <tp:SigningCertificateRef tp:certId="CompanyA_SigningCert"/>
    </tp:SenderNonRepudiation>
  </tp:ebXMLSenderBinding>
  <tp:ebXMLReceiverBinding tp:version="2.0">
    <tp:ReliableMessaging>
      <tp:Retries>5</tp:Retries>
      <tp:RetryInterval>PT30M</tp:RetryInterval>
      <tp:MessageOrderSemantics>NotGuaranteed</tp:MessageOrderSemantics>
    </tp:ReliableMessaging>
    <tp:PersistDuration>P1D</tp:PersistDuration>
    <tp:ReceiverNonRepudiation>
      <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
      <tp:HashFunction>http://www.w3.org/2001/04/xmlenc#sha256</tp:HashFunction>
      <tp:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</tp:SignatureAlgorithm>
      <tp:SigningSecurityDetailsRef tp:securityId="CompanyA_MessageSecurity"/>
    </tp:ReceiverNonRepudiation>
  </tp:ebXMLReceiverBinding>
</tp:DocExchange>
```

6.1.4.2 X2

X2은 문서 수신에 필요한 정의이며 다음과 같다. 유의할 사항은 XMLDSIG를 적용하여 수발신부인방지 처리를 하겠다는 부분을 적용하여야 한다.

tp:securityId 는 Security인증서 적용방안을 참고해야 한다.

```
<tp:DocExchange tp:docExchangeId="X2">
  <tp:ebXMLSenderBinding tp:version="2.0">
    <tp:ReliableMessaging>
      <tp:Retries>5</tp:Retries>
      <tp:RetryInterval>PT30M</tp:RetryInterval>
      <tp:MessageOrderSemantics>NotGuaranteed</tp:MessageOrderSemantics>
    </tp:ReliableMessaging>
    <tp:PersistDuration>P1D</tp:PersistDuration>
    <tp:SenderNonRepudiation>
      <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
      <tp:HashFunction>http://www.w3.org/2001/04/xmlenc#sha256</tp:HashFunction>
      <tp:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</tp:SignatureAlgorithm>
      <tp:SigningCertificateRef tp:certId="CompanyA_SigningCert"/>
    </tp:SenderNonRepudiation>
  </tp:ebXMLSenderBinding>
  <tp:ebXMLReceiverBinding tp:version="2.0">
    <tp:ReliableMessaging>
      <tp:Retries>5</tp:Retries>
      <tp:RetryInterval>PT5M</tp:RetryInterval>
      <tp:MessageOrderSemantics>NotGuaranteed</tp:MessageOrderSemantics>
    </tp:ReliableMessaging>
    <tp:PersistDuration>P1D</tp:PersistDuration>
    <tp:ReceiverNonRepudiation>
      <tp:NonRepudiationProtocol>http://www.w3.org/2000/09/xmldsig#</tp:NonRepudiationProtocol>
      <tp:HashFunction>http://www.w3.org/2001/04/xmlenc#sha256</tp:HashFunction>
      <tp:SignatureAlgorithm>http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</tp:SignatureAlgorithm>
      <tp:SigningSecurityDetailsRef tp:securityId="CompanyB_MessageSecurity"/>
    </tp:ReceiverNonRepudiation>
  </tp:ebXMLReceiverBinding>
</tp:DocExchange>
```

6.1.5 SimplePart

Simple Part는 MIME content-type과 Namespace에 대한 참조를 정의한다. 모든 네임스페이스를 정의하진 않지만 기본이 되는 헤더와 Exception 그리고 기본적으로 사용하는 MIME Type을 정의하였다.

```
<tp:SimplePart
  tp:id="customs_MsgHdr"
  tp:mimetype="text/xml">
  <tp:NamespaceSupported
    tp:location="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
    tp:version="2.0">
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  </tp:NamespaceSupported>
</tp:SimplePart>
<!-- SimplePart corresponding to a Receipt Acknowledgment business signal -->
<tp:SimplePart
  tp:id="customs_ReceiptAcknowledgment"
  tp:mimetype="text/xml">
  <tp:NamespaceSupported
    tp:location="http://www.ebxml.org/bpss/ReceiptAcknowledgment.xsd"
    tp:version="2.0">
    http://www.ebxml.org/bpss/ReceiptAcknowledgment.xsd
  </tp:NamespaceSupported>
</tp:SimplePart>
<!-- SimplePart corresponding to an Exception business signal -->
<tp:SimplePart
  tp:id="customs_Exception"
  tp:mimetype="text/xml">
  <tp:NamespaceSupported
    tp:location="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
    tp:version="2.0">
    http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd
  </tp:NamespaceSupported>
</tp:SimplePart>
<!-- SimplePart corresponding to a request action -->
<tp:SimplePart
  tp:id="customs_Request"
  tp:mimetype="text/xml">
</tp:SimplePart>
<!-- SimplePart corresponding to a response action -->
<tp:SimplePart
  tp:id="customs_Response"
  tp:mimetype="text/xml">
</tp:SimplePart>
```

6.1.6 Packaging element

Packaging element는 메시지 헤더와 Payload(s)에 대한 정보를 정의한다.

```
<tp:Packaging tp:id="customs_MshSignalPackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite tp:id="customs_MshSignal" tp:mimetype="multipart/related"
        tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
<!-- An ebXML message with a SOAP Envelope plus a request action payload -->
<tp:Packaging tp:id="customs_RequestPackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite tp:id="customs_RequestMsg" tp:mimetype="multipart/related"
         tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
      <tp:Constituent tp:idref="customs_Request"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
<!-- An ebXML message with a SOAP Envelope plus a response action payload -->
<tp:Packaging tp:id="customs_ResponsePackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite  tp:id="customs_ResponseMsg" tp:mimetype="multipart/related"
      tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
      <tp:Constituent tp:idref="customs_Response"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
<!-- An ebXML message with a Receipt Acknowledgment signal, plus a business response,
     or an ebXML message with an Exception signal -->
<tp:Packaging tp:id="customs_SyncReplyPackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite tp:id="customs_SignalAndResponseMsg" tp:mimetype="multipart/related"
      tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
      <tp:Constituent tp:idref="customs_ReceiptAcknowledgment"/>
      <tp:Constituent tp:idref="customs_Response"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
<!-- An ebXML message with a SOAP Envelope plus a ReceiptAcknowledgment payload -->
<tp:Packaging tp:id="customs_ReceiptAcknowledgmentPackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite tp:id="customs_ReceiptAcknowledgmentMsg" tp:mimetype="multipart/related"
      tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
      <tp:Constituent tp:idref="customs_ReceiptAcknowledgment"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
<!-- An ebXML message with a SOAP Envelope plus an Exception payload -->
<tp:Packaging tp:id="customs_ExceptionPackage">
  <tp:ProcessingCapabilities tp:parse="true" tp:generate="true"/>
  <tp:CompositeList>
    <tp:Composite tp:id="customs_ExceptionMsg" tp:mimetype="multipart/related"
      tp:mimeparameters="type=text/xml">
      <tp:Constituent tp:idref="customs_MsgHdr"/>
      <tp:Constituent tp:idref="customs_Exception"/>
    </tp:Composite>
  </tp:CompositeList>
</tp:Packaging>
```

6.2 CPA

6.2.1 CPA(협업 프로토콜 약정)

Collaboration-protocol Agreement(협업 프로토콜 약정)은 관세청과 비즈니스 협업관계를 수행 할 때 맺는 약정서이다. 6.1.1에서 언급된 CPP를 기준으로 CPA를 작성하며 이는 국가관세종합정보망과 전자적으로 비즈니스를 수행하기 위하여 작성되는 XML문서이며 보통은 다음의 그림과 같은 절차를 따른다.

위 그림 3번, 4번 절차를 생략하기 위하여 사용자가 사용 신청을 하고 관세청에서 승인을 하면 CPA파일이 자동으로 작성되며, 이를 CPA협약이 완료된 것으로 간주하여 처리 할 수 있도록 국가관세종합정보망을 구축한다. 사용자 신청의 승인이 나면 CPA를 승인한 것으로 간주하며 CPA파일을 다운로드 받아서 자신의 환경에 맞도록 설치하여 사용한다.

CPA파일은 ebXML 메시지 서버 혹은 클라이언트 환경의 Config파일로 사용할 수 있다. 관세청은 CPA에 명시되지 않은 메시지 헤더나 첨부문서 등에 대하여는 수신을 거부하며, 오직 CPA에 명시된 방법에 의해서만 메시지를 주고 받을 수 있다. 따라서 CPA에 맞도록 적절하게 동작하도록 시스템을 구축하여야 하며, 적절하게 동작하는지의 여부는 ebXML의 메시지 서버 혹은 클라이언트 라이브러리가 ebXML에서 정한 기술 규격을 준수하느냐의 여부에 달려 있다고 볼 수 있다.

국가관세종합정보망은 ebXML에서 정하는 기술규격을 충족하여 전송하고 응답하는지 여부만 확인하여 처리하는 정책을 취한다.

6.2.2 ebMS 서버와 CPA와의 연관성

Collaboration-protocol Agreement(협업 프로토콜 약정)은 ebMS 서버에서 헤더 생성 및 문서첨부, 통신채널 등에 대한 정의를 하는 XML파일이며 일반적으로 ebMS서버들은 이 CPA파일을 참조하여 동작한다. CPA파일의 설정값에 의하여 정해진 표준을 준수하여 송수신을 하라는 의미이며 이를 어떻게 구현하는 지에 대해서는 관여하지 않는다. 이와 관련한 기술적인 부분은 ebXML 관련 기술 문서인 ebCPP2.0을 참조하여야 한다.

○ 클라이언트 서버용 CPA 생성방법은 아래와 같다.
- 국가관세종합정보망(URL미정) 로그인 한다.
- 마이페이지>서비스관리>문서함사용관리로 이동한다.
- 서버방식으로 사용할 문서함번호를 클릭한다.
- CPA생성 버튼을 클릭하면 CPA를 다운로드 할 수 있다.

7. 사용자 정보 관리 정책(4세대 오픈 전 최종버전 확정 후 배포 예정)

7.1 사용자 정보 관리

관세청과 전자문서를 연계하고자 하는 사용자는 본인이 속해있는 업체의 정보와 인증서 정보가 반드시 국종망의 사용자 포탈인 국가관세종합정보망에 등록이 되어 있어야 한다.

사용자등록 과정은 업체정보와 대표자정보를 등록하는 이용신청 과정과 해당업체의 사무원 정보를 등록하는 업체직원(사무원) 등록 과정으로 나뉘어 진다.

❍ **이용 신청 과정**

이용신청은 국가관세종합정보망에 업체정보와 대표자정보를 등록하고, 관할 세관으로부터 사용승인을 받는 과정으로 이루어지며, 사용승인이 완료되면 업체에서 사용하고자 하는 공인인증서를 등록한다. (이용신청시 공인인증서 등록 가능)

이용신청 과정은 **웹 화면으로 신고업무를 처리하는 사용자뿐만 아니라 사용자 S/W, 연계 서버 사용자 등 모든 사용자가 국가관세종합정보망에 접속하여 이용 신청하여야 한다.**

국가관세종합정보망 이용신청등록은 업체의 기본 정보와 대표자의 정보를 입력하고 처리하고자 하는 업무영역을 선택하여 등록한다. 만일 신고자 부호가 없는 경우 신규 신고자부호 발급요청을 하도록 한다. 이용신청 후 세관의 사용승인(신고자부호 발급 및 기본문서함 생성)을 받는다.

등록 가능한 공인인증서는 하나의 업체에 해당업체에 발급된 한 개의 인증서만 등록할 수 있다. 업체직원(사무원)이 여러 명 등록되어 있는 경우 등록된 공인인증서를 공유하여 사용하여야 한다. 인증서 공유시 공인인증서는 해당 업체의 인감도장과 동일한 효력이 가짐으로 인증서의 공유에 의한 불법사용 및 인증서의 누출이 없도록 관리를 하여야 한다.

국가관세종합정보망에 인증서가 등록되면, 시스템에서는 등록된 인증서를 이용하여 사용자의 접속요청시 신원확인 처리, 전자문서 송수신시 전자서명검사, 통보서의 암호화 등에 사용되므로, 전자문서 연계시 등록된 인증서를 이용하여 전자문서의 보안처리를 수행하여야 한다. **인증서가 변경되는 경우 국가**

관세종합정보망에 접속하여 변경된 인증서를 등록하여야 한다.

인증서 등록에 사용될 수 있는 인증서는 상호연동이 가능한 법인용 1등급인증서와 서버용 인증서만 사용이 가능하다. (5.1장 공인인증서 참조)
주) 연계서버 사용자의 경우 공인인증서는 서버용 인증서를 발급받아 등록하여야 한다.

❍ **업체직원(사무원) 등록과정**

하나의 업체에 신고업무를 처리하는 업체직원(이하 사무원)이 여러명 존재하는 경우 사무원은 국가관세종합정보망에 "업체직원"으로 이용신청 후 업체대표로부터 이용승인을 받아 국가관세종합정보망을 이용할 수 있다.

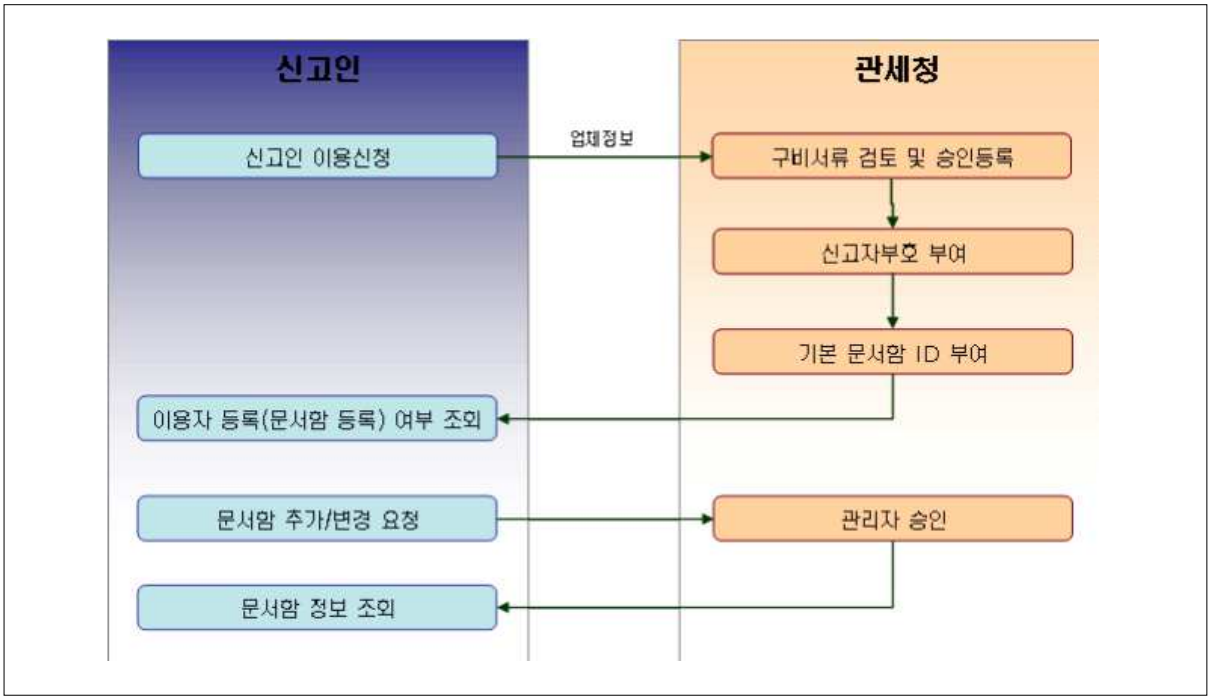
사무원 등록이 완료되면 국가관세종합정보망에 등록된 공인인증서를 공유하여 사용하여야 한다. 인증서는 매우 중요한 업체의 신용자산임으로 공유시 발생할 수 있는 불법사용 및 인증서의 누출이 없도록 하여야 한다.

등록된 사무원들이 처리한 신고내역은 사무원들간에 공유가 가능하도록 되어 있다. 업무적인 필요에 의하여 분리하여야 하는 경우 문서함을 추가로 설정하여 업무적으로 구분도록 한다.

7.2 문서함 관리

문서함은 전자문서를 송수신하기 위한 관세청 시스템과 사용자의 접점으로 전자문서 연계를 위해서 필수적으로 문서함을 부여 받아야 한다.

문서함은 사용자 등록과정에서 관할세관의 신고자부호 등록 및 승인 과정에서 기본문서함을 자동적으로 부여한다. 자세한 문서함의 개설과정은 다음과 같다.



사용자가 국가관세종합정보망을 사용하기 위해 이용신청 후 세관으로부터 사용승인을 받게 된다. 세관의 사용승인 시, 신청한 신고자부호 및 문서함ID가 생성되며
사용자는 부여된 문서함 ID를 국가관세종합정보망의 [마이페이지>서비스관리>문서함사용관리] 메뉴에서 조회할 수 있다.

만일, 사용자가 업무처리를 위하여 여러개의 문서함이 필요하거나, 사용 중인 문서함의 정보를 변경하고자 하는 경우 업체대표가 [마이페이지>서비스관리>문서함사용관리] 메뉴를 이용하여 문서함을 추가 및 변경 요청할 수 있으며, 관세청의 업무담당자가 승인시 추가/변경된 문서함을 사용할 수 있다.

8. 표준연계 API

8.1 표준연계 API 기능

표준연계 API의 주요기능은 아래와 같으며 전자문서 표준연계 API설명서를 참고하여 상세한 내용을 확인 할 수 있다.

기능	설명	비고
전자문서 유통 기능	문서유통시스템과 연계하여 신고서를 송/수신할 수 있는 기능 - 전송헤더의 생성 및 문서 Packing - 문서유통시스템과 통신기능	
전자문서 보안기능	전자문서 송수신시 데이터의 누출 방지 및 위변조 방지 기능 - 전자문서의 전자서명 및 암호화 기능 - 공인인증서를 이용한 본인확인 기능	

부록 1. 적용표준

전자문서 연계를 위한 적용표준은 다음과 같다.

구분		적용 표준
통신표준	전송프로토콜	통신프로토콜 규정 http://www.w3.org/Protocols/ Hypertext Transfer Protocol -- HTTP/1.1 http://www.ietf.org/rfc/rfc2616.txt
보안표준	XML 전자서명	W3C XML-Signature Syntax and Processing *http://www.w3.org/TR/2002/REC-xmldsig-core-20020212*
	XML 암호화	XML Encryption Syntax and Processing *http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/*
메시징구조표준	ebXML전송 규약	ebXML Message Service 2.0 *http://www.ebxml.org/specs/ebMS2.pdf*
	전송 Message 구조	SOAP Message *http://www.w3.org/TR/SOAP/*
	첨부를 가진 전송 Message 구조	SOAP Messages with Attachments *http://www.w3.org/TR/SOAP-attachments*
적용알고리즘	Digest	SHA256 *http://www.w3.org/2001/04/xmlenc#sha256*
	Signature	RSAwithSHA256 *http://www.w3.org/2001/04/xmldsig-more#rsa-sha256*
	Encoding	Base64 *http://www.w3.org/2000/09/xmldsig#base64*

	Canonicalization	Canonical XML http://www.w3.org/TR/2001/REC-xml-c14n-20010315
		Canonical XML with Comments http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments
	XPath	XML Path(XPath) http://www.w3.org/TR/1999/REC-xpath-19991116
	XLink	XML Linking Language (XLink) Version 1.0 http://www.w3.org/TR/2001/REC-xlink-20010627/
	XPointer	XML Pointer Language (XPointer) http://www.w3.org/TR/2002/WD-xptr-20020816/
	Manifest	Manifest http://www.w3.org/2000/09/xmldsig#Manifest
	Enveloped Signature	Enveloped Signature Transform http://www.w3.org/2000/09/xmldsig#enveloped-signature
	Block Encryption	SEED http://www.rootca.or.kr/technical/down01/2.3-128-bit Symmetric Block Cipher(SEED).pdf
	Key Transpot	RSA http://www.w3.org/2001/04/xmlenc#rsa-1_5

부록 2. SOAP 메시지

1. SOAP 메시지 구조

XML		
	version	"1"
	encoding	"UTF-8"
SOAP:Envelope		
	xmlns:SOAP	"http://schemas.xmlsoap.org/soap/envelope/"
	xmlns:xlink	"http://www.w3.org/1999/xlink"
	xmlns:xsi	"http://www.w3.org/2001/XMLSchema-instance"
	xsi:schemaLocation	"http://schemas.xmlsoap.org/soap/envelope/ http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd"
	SOAP:Header	
		xmlns:eb: "http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
		xsi:schemaLocation: "http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
		eb:MessageHeader
		env:mustUnderstand: "1"
		eb:id: "MessageHeader"
		eb:version: "2.0"
		eb:From
		eb:PartyId
		eb:type: *송신자의 유형*
		송신자 ID
		eb:Role: *송신자의 역할*

			eb:To			
				eb:PartyId		
					eb:type	*수신자의 유형*
					수신자 ID	
				eb:Role	*수신자의 역할*	
			eb:CPAId	*CPA ID*		
			eb:ConversationId	*Conversion ID* *(신고서1건:제출번호* *신고서N건:UUID사용권고)*		
			eb:Service			
				eb:type	*서비스가 기술된 URL*	
				서비스 구분		
			eb:Action	*(신고서1건: "KCSSingleAction"* *신고서N건:KCSMetaAction")*		
			eb:MessageData			
				eb:MessageId	*message id*	
				eb:Timestamp	*문서 생성시간*	
		ds:Signature				
	SOAP:Body					
		xmlns:eb	"http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"			
		xsi:schemaLocation	"http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"			
		eb:Manifest				
			eb:id	"Manifest"		
			eb:version	"2.0"		
			eb:Reference			

				eb:id	*첨부문서의 참조 ID*
				xlink:href	*첨부문서의 CID*
				xlink:type	"simple"
				eb:Description	
				xml:lang	"ko-kr"
				전자문서 파일명	

2. SOAP 메시지 정의

ELEMENT	설명	구분	VALUE	필요	반복
XML	XML 선언	attribute	version="1"	M	1
		attribute	encoding="UTF-8"	M	1
SOAP:Envelope	Envelope선언 Element	attribute	xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"	M	1
		attribute	xmlns:xlink="http://www.w3.org/1999/xlink"	M	1
		attribute	xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"	M	1
		attribute	xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/ http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd"	M	1
SOAP:Envelope/SOAP:Header	SOAP Header선언 Element	attribute	xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"	M	1
		attribute	xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd	M	1

			http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"		
SOAP:Envelope/SOAP:Header/eb:MessageHeader	Message의 라우팅 정보를 표기하는 Element	attribute	SOAP:mustUnderstand="1"	M	1
		attribute	eb:id="MessageHeader"	M	1
		attribute	eb:version="2.0"	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:From	Message의 송신자를 표기하는 Element	element	-	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:From/eb:PartyId	송신자ID를 표기	attribute	*수신자의 유형*	M	1
		element	*송신자 ID*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:From/eb:Role	송신자의 ROLE	element	*송신자의 역할*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:To	Message의 수신자를 표기하는 Element	element	-	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:To/eb:PartyId	수신자ID를 표기	attribute	*수신자의 유형*	M	1
		element	*수신자 ID*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:To/eb:Role	수신자의 ROLE	element	*수신자의 역할*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:CPAId	CPA ID를 표기	element	*CPA ID*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:ConversationId	일련의 관련 Message를 규정하는 Element	element	*신고서1건:제출번호* *신고서N건:UUID사용권고)*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:Service	Message의 행위에 따라 처리되는 서비스를 규정하는	attribute	eb:type="*서비스가 기술된 URL*"	M	1
		element	*서비스 구분*	M	1

	Element				
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:Action	Message서비스에서 절차를 구별	element	*(신고서1건: "KCSSingleAction" 신고서N건:KCSMetaAction")*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:MessageData	Message 정보를 나타내는 Element	element	-	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:MessageData/eb:MessageId	Message ID	element	*Message ID* *사용자 프로그램이 생성하는 전자문서의 ID를 사용*	M	1
SOAP:Envelope/SOAP:Header/eb:MessageHeader/eb:MessageData/eb:Timestamp	Message 생성시간	element	*YYYY-MM-DDTHH:MI:SS.MicroSECZ (UTC)*	M	1
SOAP:Envelope/SOAP:Header/ds:Signature	전자서명 정보		*전자서명 element 참조*	M	1
SOAP:Envelope/SOAP:Body	SOAP Body선언 Element	attribute	xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"	M	1
		attribute	xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"	M	1
SOAP:Envelope/SOAP:Body/eb:Manifest	페이로드 컨테이너에 표기된 첨부문서를 식별	attribute	eb:id="Manifest"	M	1
		attribute	eb:version="2.0"	M	1
SOAP:Envelope/SOAP:Body/eb:Manifest/eb:Reference	첨부문서의 링크 정보	attribute	eb:id="Reference-*[첨부순서]*" *첨부순서는 1부터 시작*	M	n
		attribute	xlink:href="cid:payload-*[첨부순서]*" *첨부순서는 1부터 시작*		
		attribute	xlink:type="simple"		
SOAP:Envelope/SOAP:Body/eb:M	Message 로컬	attribute	xml:lang="ko-kr"	M	n

anifest/eb:Reference/eb:Description	파일명	element	*전자문서 파일명*		

3. SOAP 메시지 전자서명 구조

ds:Signature			
	xmlns:ds	"http://www.w3.org/2000/09/xmldsig#"	
	xmlns:xsi	"http://www.w3.org/2001/XMLSchema-instance"	
	xsi:schemaLocation	"http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"	
	ds:SignedInfo		
		ds:CanonicalizationMethod	
			Algorithm	"http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
		ds:SignatureMethod	
			Algorithm	"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"
		ds:Reference(1)	
			URI	""
			ds:DigestMethod	
				Algorithm	"http://www.w3.org/2001/04/xmlenc#sha256"
			ds:DigestValue	*SOAP 자신의 MD 값*
			ds:Transforms	
				ds:Transform(1)	
					Algorithm	"http://www.w3.org/TR/1999/REC-xpath-19991116"
					ds:XPath	"not(ancestor-or-sel

						f::Signature)"
				ds:Transform(2)		
					Algorithm	"http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
		ds:Reference(2)				
			URI	*SOAP:Envelope/SOAP:Body/eb:Manifest/eb:Reference.xlink:href 값*		
			ds:DigestMethod			
				Algorithm	"http://www.w3.org/2001/04/xmlenc#sha256"	
			ds:DigestValue	*첨부문서의 MD 값*		
			ds:Transforms			
				ds:Transform		
					Algorithm	"http://www.w3.org/TR/2001/REC-xml-c14n-20010315"
	ds:SignatureValue	*전자서명 값*				
	ds:KeyInfo					
		ds:KeyValue				
			ds:RSAKeyValue			
				ds:Modulus	*인증서의 Modulus값*	
				ds:Exponent	*인증서의 Exponent값*	
		ds:X509Data				
			ds:X509IssuerSerial			
				ds:X509IssuerName	*인증서 발급자(인증기관)의 고유명*	
				ds:X509Seria	*인증서 발급자(인증기관)의 인증서*	

				lNumber	*번호*
			ds:X509SubjectName	*인증서의 고유명*	
			ds:X509Certificate	*인증서*	

4. SOAP 메시지 전자서명 정의

ELEMENT	설명	구분	VALUE	필요	반복
ds:Signature	전자서명을 나타내는 element	attribute	xmlns:ds="http://www.w3.org/2000/09/xmldsig#"	M	1
		attribute	xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"	M	1
		attribute	xsi:schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"	M	1
ds:Signature/ds:SignedInfo	전자서명 생성 정보를 나타내는 element	element	-	M	1
ds:Signature/ds:SignedInfo/ds:CanonicalizationMethod	Canonicalization 알고리즘 표기	attribute	Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"	M	1
ds:Signature/ds:SignedInfo/ds:SignatureMethod	전자서명 알고리즘을 표기	attribute	Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"	M	1
ds:Signature/ds:SignedInfo/ds:Reference	첨부문서의 정보를 표기	attribute	*자기 자신을 나타내는 경우* URI="" *첨부문서를 나타내는 경우* URI="cid:payload-*[순번]*"	M	n
ds:Signature/ds:SignedInfo/ds:Referenceds:DigestMethod	해쉬함수의 알고리즘을 표기	attribute	Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"	M	1
ds:Signature/ds:SignedInfo/ds:Referenceds:DigestValue	해쉬값을 표기	element	*자기 자신 및 첨부문서의 해쉬값*	M	1
ds:Signature/ds:SignedInfo/ds:Referenceds:Transforms	해쉬값 생성을 위한 변환규약을 표기하는 element	element	-	C	1
ds:Signature/ds:SignedInfo/ds	해쉬값 생성을	attribut	*XPATH를 표기하는 경우*	M	n

:Referenceds:Transforms/ds:Transform	위한 변환 알고리즘을 표기	e	Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116" *Canonicalization 알고리즘을 표기하는 경우* Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/		
ds:Signature/ds:SignedInfo/ds:Referenceds:Transforms/ds:Xpath	해쉬값 생성을 위한 xpath	element	"not(ancestor-or-self::Signature)"	C	n
ds:Signature/ds:SignatureValue	전자서명값을 표기	element	*전자서명 값*	M	1
ds:Signature/ds:KeyInfo	전자서명의 검증에 사용될 전자서명 인증서 정보를 나타내는 엘리먼트	element	-	M	1
ds:Signature/ds:KeyInfo/ds:KeyValue	공개키 정보	element	-	C	1
ds:Signature/ds:KeyInfo/ds:KeyValue/ds:RSAKeyValue	인증서의 공개키 값	element	*인증서의 Modulus 값*	M	1
ds:Signature/ds:KeyInfo/ds:X509Data	전자서명 인증서	element	-	M	1
ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509IssuerSerial	인증서 발급자(공인인증기관)의 정보를 표기	element	-	M	1
ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509IssuerSerial/ds:X509IssuerName	인증서 발급자(공인인증기관)의 고유명	element	*인증서 발급자(공인인증기관)의 고유명*	M	1
ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509IssuerSerial/ds:X509SerialNumber	인증서 발급자(공인인증기관)의 인증서 번호	element	*인증서 발급자(공인인증기관)의 인증서 번호*	M	1
ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509SubjectName	인증서의 고유명	element	*인증서의 고유명*	M	1
ds:Signature/ds:KeyInfo/ds:X509Data/ds:X509Certificate	인증서	element	*인증서*	M	1

부록 3 Case별 ebMS 메시지 패키징 예시

1. 신고서(or 요건확인신청서) 1건을 제출하는 경우

```
------=_Part_18_16197505.1407225023761
Content-ID:<SOAPPART>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
      </eb:To>

<eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
      <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
      <eb:Action>KCSSingleAction</eb:Action>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.x
sd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-hea
der-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:Manifest eb:id="Manifest" eb:version="2.0">
      <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample.xml</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

------=_Part_18_16197505.1407225023761
```

```
Content-ID:<payload-1>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.1407225023761--
```

2. 신고서 1건과 첨부파일 n건을 제출하는 경우

```
------=_Part_18_16197505.1407225023761
Content-ID:<SOAPPART>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
      </eb:To>

<eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
      <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
      <eb:Action>KCSMetaAction</eb:Action>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.x
sd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-hea
der-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:Manifest eb:id="Manifest" eb:version="2.0">
      <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">meta.xml</eb:Description>
      </eb:Reference>
```

```
      <eb:Reference eb:id="Reference-2" xlink:href="cid:payload-2"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-3" xlink:href="cid:payload-3"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">image.tiff</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-4" xlink:href="cid:payload-4"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">a.pdf</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

------=_Part_18_16197505.1407225023761
Content-ID:<payload-1>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<kcs:DocumentMetaData>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000001</kcs:MessageID>
      <kcs:ContentID>payload-2</kcs:ContentID>
      <kcs:ID>10526131532549</kcs:ID>
      <kcs:TypeCode>GOVCBR929</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample.xml</kcs:FilePath>
    </kcs:Document>
    <kcs:ElectronicLibrary>
      <kcs:SubTypeCode>XXX001</kcs:SubTypeCode>
      <kcs:AttachedDocument>

<kcs:AttachedDocumentID>201411240924521230000001001</kcs:AttachedDocumentID>
   <kcs:ContentID>payload-3</kcs:ContentID>
        <kcs:FilePath>C:₩KCSIPTModule₩image.tiff</kcs:FilePath>
        <kcs:ID>10526131532549</kcs:ID>
        <kcs:Name>image.tiff</kcs:Name>
        <kcs:TypeCode>2</kcs:TypeCode>
        <kcs:UseTypeCode>1</kcs:UseTypeCode>
        <kcs:SubReference>
          <kcs:SubReferenceID>001</kcs:SubReferenceID>
```

```
          </kcs:SubReference>
          <kcs:FileInformation>
            <kcs:TypeCode>XXX001001</kcs:TypeCode>
            <kcs:StartPageNumeric>1</kcs:StartPageNumeric>
          </kcs:FileInformation>
        </kcs:AttachedDocument>
      </kcs:ElectronicLibrary>
      <kcs:ElectronicLibrary>
        <kcs:SubTypeCode>XXX001</kcs:SubTypeCode>
        <kcs:AttachedDocument>

<kcs:AttachedDocumentID>20141124092452123000001002</kcs:AttachedDocumentID>
  <kcs:ContentID>payload-4</kcs:ContentID>
          <kcs:FilePath>C:₩KCSIPTModule₩a.pdf</kcs:FilePath>
          <kcs:ID>10526131532549</kcs:ID>
          <kcs:Name>a.pdf</kcs:Name>
          <kcs:TypeCode>2</kcs:TypeCode>
          <kcs:UseTypeCode>1</kcs:UseTypeCode>
          <kcs:SubReference>
            <kcs:SubReferenceID>001</kcs:SubReferenceID>
          </kcs:SubReference>
          <kcs:FileInformation>
            <kcs:TypeCode>XXX001001</kcs:TypeCode>
            <kcs:StartPageNumeric>1</kcs:StartPageNumeric>
          </kcs:FileInformation>
        </kcs:AttachedDocument>
      </kcs:ElectronicLibrary>
  </kcs:PayloadInfomation>
</kcs:DocumentMetaData>

------=_Part_18_16197505.1407225023761
Content-ID:<payload-2>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-3>
Content-Type: image/tiff
Content-Transfer-Encoding: base64
…Base64 encoding TIFF image
```

```
------=_Part_18_16197505.5407221023761
Content-ID:<payload-4>
Content-Type: application/pdf
Content-Transfer-Encoding: base64
…Base64 encoding PDF file

------=_Part_18_16197505.5407221023761--
```

3. 신고서 n건을 제출하는 경우

```
------=_Part_18_16197505.5407221023761
Content-ID:<SOAPPART>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
      </eb:To>

<eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
      <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
      <eb:Action>KCSMetaAction</eb:Action>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.x
sd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-hea
der-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:Manifest eb:id="Manifest" eb:version="2.0">
      <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">meta.xml</eb:Description>
```

```
      </eb:Reference>
      <eb:Reference eb:id="Reference-2" xlink:href="cid:payload-2"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample1.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-3" xlink:href="cid:payload-3"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample2.xml</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-1>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<kcs:DocumentMetaData>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000001</kcs:MessageID>
      <kcs:ContentID>payload-2</kcs:ContentID>
      <kcs:ID>10526131532549</kcs:ID>
      <kcs:TypeCode>GOVCBR929</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample1.xml</kcs:FilePath>
    </kcs:Document>
  </kcs:PayloadInfomation>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000002</kcs:MessageID>
      <kcs:ContentID>payload-3</kcs:ContentID>
      <kcs:ID>10526131532548</kcs:ID>
      <kcs:TypeCode>GOVCBR929</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample2.xml</kcs:FilePath>
    </kcs:Document>
  </kcs:PayloadInfomation>
</kcs:DocumentMetaData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-2>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
```

```
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-3>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761--
```

4. 요건확인신청서 n건을 제출하는 경우(동일기관만 가능)

```
------=_Part_18_16197505.5407221023761
Content-ID:<SOAPPART>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="ok-customs.dtm1">XX102344456778</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
      </eb:To>

<eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
      <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
      <eb:Action>KCSMetaAction</eb:Action>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.x
sd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-hea
der-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
    <eb:Manifest eb:id="Manifest" eb:version="2.0">
      <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
```

```
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">meta.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-2" xlink:href="cid:payload-2"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample1.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-3" xlink:href="cid:payload-3"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample2.xml</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-1>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<kcs:DocumentMetaData>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000001</kcs:MessageID>
      <kcs:ContentID>payload-2</kcs:ContentID>
      <kcs:ID>10526131532549</kcs:ID>
      <kcs:TypeCode>GOVCBRBR1</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample1.xml</kcs:FilePath>
    </kcs:Document>
  </kcs:PayloadInfomation>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000002</kcs:MessageID>
      <kcs:ContentID>payload-3</kcs:ContentID>
      <kcs:ID>10526131532548</kcs:ID>
      <kcs:TypeCode>GOVCBRBR1</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample2.xml</kcs:FilePath>
    </kcs:Document>
  </kcs:PayloadInfomation>
</kcs:DocumentMetaData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-2>
```

```
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-3>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761--
```

5. 요건확인신청서 1건과 요건확인 첨부파일 n건을 함께 제출하는 경우

```
------=_Part_18_16197505.5407221023761
Content-ID:<SOAPPART>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<SOAP:Envelope>
  <SOAP:Header>
    <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader"
eb:version="2.0">
      <eb:From>
        <eb:PartyId eb:type="ok-customs.dtm1">XX402815416601</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
      </eb:From>
      <eb:To>
        <eb:PartyId eb:type="ok-customs.dtm1">XX102344456778</eb:PartyId>
        <eb:Role>http://www.ok-customs.go.kr/ebMSH#receiver</eb:Role>
      </eb:To>

<eb:ConversationId>a5e51512-0c94-4491-8f91-6bdae4914222</eb:ConversationId>
      <eb:Service eb:type="anyURI">urn:Ok-Customs-Service</eb:Service>
      <eb:Action>KCSMetaAction</eb:Action>
    </eb:MessageHeader>
  </SOAP:Header>
  <SOAP:Body
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.x
sd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-hea
der-2_0.xsd
http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
```

```
    <eb:Manifest eb:id="Manifest" eb:version="2.0">
      <eb:Reference eb:id="Reference-1" xlink:href="cid:payload-1"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">meta.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-2" xlink:href="cid:payload-2"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">sample1.xml</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-3" xlink:href="cid:payload-3"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">a.hwp</eb:Description>
      </eb:Reference>
      <eb:Reference eb:id="Reference-4" xlink:href="cid:payload-4"
xlink:type="simple">
        <eb:Description xml:lang="ko-kr">b.hwp</eb:Description>
      </eb:Reference>
    </eb:Manifest>
  </SOAP:Body>
</SOAP:Envelope>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-1>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<kcs:DocumentMetaData>
  <kcs:PayloadInfomation>
    <kcs:Document>
      <kcs:MessageID>20141124092452123000001</kcs:MessageID>
      <kcs:ContentID>payload-2</kcs:ContentID>
      <kcs:ID>10526131532549</kcs:ID>
      <kcs:TypeCode>GOVCBRBR1</kcs:TypeCode>
      <kcs:FilePath>C:₩KCSIPTModule₩sample1.xml</kcs:FilePath>
    </kcs:Document>
    <kcs:RoutingAttachedDocument>

<kcs:AttachedDocumentID>201411240924521230000001001</kcs:AttachedDocumentID>
   <kcs:ContentID>payload-3</kcs:ContentID>
      <kcs:FilePath>C:₩KCSIPTModule₩a.hwp</kcs:FilePath>
      <kcs:FileType>2</kcs:FileType>
      <kcs:FileName>a.hwp</kcs:FileName>
      <kcs:SubReferenceID>B</kcs:SubReferenceID>
```

```
    </kcs:RoutingAttachedDocument>
    <kcs:RoutingAttachedDocument>

<kcs:AttachedDocumentID>20141124092452123000001002</kcs:AttachedDocumentID>
   <kcs:ContentID>payload-4</kcs:ContentID>
      <kcs:FilePath>C:₩KCSIPTModule₩b.hwp</kcs:FilePath>
      <kcs:FileType>2</kcs:FileType>
      <kcs:FileName>b.hwp</kcs:FileName>
      <kcs:SubReferenceID>C</kcs:SubReferenceID>
    </kcs:RoutingAttachedDocument>
  </kcs:PayloadInfomation>
</kcs:DocumentMetaData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-2>
Content-Type: text/xml; charset="UTF-8"
<?xml version="1.0" encoding="UTF-8"?>
<xenc:EncryptedData>…</xenc:EncryptedData>

------=_Part_18_16197505.5407221023761
Content-ID:<payload-3>
Content-Type: application/hwp
Content-Transfer-Encoding: base64
…Base64 encoding HWP file

------=_Part_18_16197505.5407221023761
Content-ID:<payload-4>
Content-Type: application/hwp
Content-Transfer-Encoding: base64
…Base64 encoding HWP file

------=_Part_18_16197505.5407221023761--
```

부록 4. 환경정보 다운로드 방법

1. 국가관세종합정보망 암호화 인증서 다운로드

전자문서를 암호화하여 문서유통서버로 전송하기 위하여 국가관세종합정보망의 암호화 인증서를 다음의 URL에서 다운로드한다.

▶ ebMS 서버방식의 경우
http://gsg.customs.go.kr:8110/mediate/gsg/usw/getResponse/message?code=X509

▶ 사용자 S/W방식의 경우
https://gsg.customs.go.kr:38120/mediate/gsg/usw/getResponse/message?code=X509

인증서 다운로드는 1일 1회 최초 전자문서를 송수신시 암호화 인증서 다운로드 작업을 실시하도록 한다.

부록 5. Document Meta XML 항목정의서

1. Document Meta XML 항목정의서

순번	Class/Element Name	서식 항목명	항목설명
1	DocumentMetaData	DocumentMetaData	전자문서메타정보
2	PayloadInformation		페이로드 정보
3	Document		전자문서정보
4	MessageID	메시지ID	발신자(=송신자)생성한 유일한 문서번호
5	ContentID	컨텐트ID	전자문서 페이로드의 Content-ID
6	ID	제출번호	제출번호
7	TypeCode	전자문서코드	문서타입+문서코드(예: GOVCBR929)
8	FilePath	파일경로	전자문서(XML) 파일의 로컬 경로
9	ElectronicLibrary		전자서고 첨부파일 정보
10	SubTypeCode	분류코드	문서분류체계의 소분류코드, 예) XXX001 (수입신고)
11	AttachedDocument		첨부파일정보
12	AttachedDocumentID	첨부파일ID	발신자(=송신자)생성한 유일한 첨부파일 문서번호
13	ContentID	컨텐트ID	첨부서류 페이로드의 Content-ID
14	FilePath	파일경로	전자문서가 있을 경우 전자문서 파일의 로컬 경로
15	ID	서고문서관리번호	전자서고에 기 제출되어 보관중인 문서 고유번호 - 원본파일단위 유니크 관리번호 - 참조제출 또는 기존 보관문서 삭제처리 시에 입력
16	Name	서고문서파일명	실물제출시 첨부파일명, 예) a.pdf
17	ReferenceID	서고업무참조번호	업무키#1, 예) 10526131532549 (수입신고번호)
18	TypeCode	파일형식코드	1:개별, 2:묶음
19	UseTypeCode	문서작업구분코드	1:추가, 2:삭제
20	SubReference		업무키#2
21	SubReferenceID	확장서고업무참조번호	란번호 등, 예) 001
22	FileInformation		파일정보
23	TypeCode	서고문서종류코드	문서분류체계의 문서종류코드, 예) XXX001001(XXX신고의 Invoice)
24	Name	기타문서제목	서고문서종류코드가 "기타"인 경우, 사용자가 입력한 문서제목
25	StartPageNumeric	시작페이지값	묶음파일의 문서종류별 시작페이지
26	RoutingAttachedDocument		요건기관 첨부파일 정보
27	AttachedDocumentID	첨부파일ID	
28	ContentID	컨텐트ID	전자문서와 관련된 첨부서류가 페이로드에 있을 경우 첨부서류 페이로드의 Content-ID
29	FilePath	파일경로	파일의 로컬 경로
30	FileName	파일명	첨부파일명
31	FileType	파일유형	1 : 서식 공통사항 첨부파일, 2 : 서식 품목별 첨부파일
32	SubReferenceID	확장참조번호	파일유형이 2(품목별 첨부파일)인 경우 해당 파일의 관련 품목식별부호를 기재

사용 예

```
<?xml version="1.0" encoding="UTF-8"?>
<kcs:DocumentMetaData
    xmlns:kcs="urn:kr:gov:kcs:data:standard:KCS_DocumentMetaDataSchemaModule:1:0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:kr:gov:kcs:data:standard:KCS_DocumentMetaDataSchemaModule:1:0
../../schema4G/kcs/data/standard/KCS_DocumentMetaDataSchemaModule_1.0_standard.xsd">
    <!--1..999 반복-->
  <kcs:PayloadInformation>
```

```
<!--전자문서정보 : 0..1 -->
<kcs:Document>
    <!--메시지ID-->
    <kcs:MessageID>00000000000</kcs:MessageID>
    <!--컨텐트ID-->
    <kcs:ContentID>payload-2</kcs:ContentID>
    <!--제출번호-->
    <kcs:ID>10526131532549</kcs:ID>
    <!--전자문서코드-->
    <kcs:TypeCode>GOVCBR929</kcs:TypeCode>
    <!--파일경로-->
    <kcs:FilePath>C:WKCSIPTModuleWabc.xml</kcs:FilePath>
</kcs:Document>

<!--전자서고 첨부파일 정보 : 0..1 -->
<kcs:ElectronicLibrary>
    <!--분류코드-->
    <kcs:SubTypeCode>XXX001</kcs:SubTypeCode>

    <!--0..999 반복-->
    <kcs:AttachedDocument>
        <!--첨부파일ID-->
        <kcs:AttachedDocumentID>00000000000</kcs:AttachedDocumentID>
        <!--컨텐트ID-->
        <kcs:ContentID>payload-3</kcs:ContentID>
        <!--파일경로-->
        <kcs:FilePath>C:WKCSIPTModuleWa.pdf</kcs:FilePath>
        <!--서고문서관리번호-->
        <kcs:ID>13090000000001</kcs:ID>
        <!--서고문서파일명-->
        <kcs:Name>a.pdf</kcs:Name>
        <!--서고업무참조번호-->
        <kcs:ReferenceID>10526131532549</kcs:ReferenceID>
        <!--파일형식코드(1:개별, 2:묶음, 3:압축)-->
        <kcs:TypeCode>1</kcs:TypeCode>
        <!--문서작업구분코드(1:추가, 2:삭제)-->
        <kcs:UseTypeCode>1</kcs:UseTypeCode>

        <!--0..999 반복-->
        <kcs:SubReference>
            <!--확장서고업무참조번호-->
            <kcs:SubReferenceID>1</kcs:SubReferenceID>
```

```
                </kcs:SubReference>

                <!--0..999 반복-->
                <kcs:FileInformation>
                    <!--서고문서종류코드-->
                    <kcs:TypeCode>XXX001001</kcs:TypeCode>
                    <!--기타문서제목-->
                    <kcs:Name>기타문서제목</kcs:Name>
                    <!--시작페이지값-->
                    <kcs:StartPageNumeric>1</kcs:StartPageNumeric>
                </kcs:FileInformation>

            </kcs:AttachedDocument>
        </kcs:ElectronicLibrary>

        <!--요건기관 첨부파일 정보 : 0..999 반복-->
        <kcs:RoutingAttachedDocument>
            <!--첨부파일ID-->
            <kcs:AttachedDocumentID>00000000000</kcs:AttachedDocumentID>
            <!--컨텐트ID-->
            <kcs:ContentID>payload-4</kcs:ContentID>
            <!--파일경로-->
            <kcs:FilePath>C:₩KCSIPTModuleWa.pdf</kcs:FilePath>
            <!--파일유형(1 : 서식 공통사항 첨부파일, 2 : 서식 품목별 첨부파일)-->
            <kcs:FileType>1</kcs:FileType>

            <!--0..999 반복-->
            <kcs:SubReference>
                <!--확장참조번호-->
                <kcs:SubReferenceID>0000000</kcs:SubReferenceID>
                <!--파일구분(A : BL첨부파일, B : Invoice, C : Packing List,
                            D : 안전인증서, E : 제품설명서, F : 기타)-->
                <kcs:UseTypeCode>A</kcs:UseTypeCode>
            </kcs:SubReference>

        </kcs:RoutingAttachedDocument>
    </kcs:PayloadInformation>
</kcs:DocumentMetaData>
```

2. 첨부서류 관련 항목

2.1 신고인 작성 가이드

2.1.1 ※첨부파일 동시 전송가능 서식은 관세청 정책에 따라 결정되며 별도 공지한다. 동시전송 허용된 서식만 첨부서류 동시전송 기능을 적용해야한다.

2.1.2 항목 설명

항목명	TYPE	SIZE	조건	반복		항목설명	Sample Value
전자서고			C			전자서고 첨부파일 정보	
분류코드	an	6	M			업무단위 식별코드	
첨부파일			C	999		첨부파일정보 Section - 첨부파일 각각에 대한 메타정보	
서고문서관리번호	an	15	C			전자서고에 기 제출되어 보관중인 첨부파일의 고유 ID 로 해당 첨부파일을 다른 신고서에 첨부하여 제출하고자 할 경우 해당 파일의 고유 ID 만을 기입하면 실물파일 제출과 동일하게 처리 - 참조제출	
서고문서파일명	an..	300	C			실물제출 시 첨부파일명 * 확장자 포함	a.pdf
서고업무참조번호	an..	500	M			First Level 업무키(PK) 예) 수입신고번호, 수출신고번호	
파일형식코드	a	1	C			해당 파일이 하나의 문서종류로 구성되었는지, 복수의 문서종류로 구성되었는지 여부 - 1: 하나의 문서종류(개별) - 2: 복수의 문서종류(묶음) * 묶음파일은 압축파일이 아님 * 묶음파일은 수입신고의 B/L, Invoice, Packing List 에만 제한적으로 허용 됨	1
문서작업구분코드	a	1	M			전자서고 작업요청 구분자 - 1: 등록(참조제출 또는 실물제출) * 문서작업구분코드는 '1'로 고정	1
확장참조번호			C	999		확장키 Section	
확장서고업무참조번호	an..	50	C			해당 첨부파일이 First Level 업무키 외에 부가적인 Secondary Level 키에 매핑 되는 경우 기입 예) 수입신고의 란, 모델규격번호	001
파일정보			C	999		문서종류 Section	
서고문서종류코드	an	9	C			해당파일의 문서종류코드	
기타문서제목	an..	150	C			사용자가 부가적인 문서제목을 입력하는 경우 기입 예) 문서종류가 "기타"인 경우 등	
시작페이지값	a..	22	C			파일형식코드가 "묶음"인 경우 해당 문서종류가 시작되는 페이지	

• 분류코드 및 서고문서종류코드

분류코드 및 서고문서종류코드는 전자서고에 신고업무 등을 통하여 제출되는 문서를 구분하고 관리하기 위한 코드체계로써 추후 관세청에서 제공하는 해당 코드

집을 참조하여 해당하는 코드를 사용하여야 합니다.

분류코드와 서고문서종류코드는 상호 계층적 구조를 이루고 있습니다.
먼저 분류코드는 시스템구분(3자리)+업무구분(일련번호 3자리)로 구성되어 있으며, 서고문서종류코드는 분류코드(6자리)+문서구분(일련번호 3자리)로 구성되어 있습니다.

시스템구분은 각각의 업무시스템을 구분하기 위한 약어이며, 업무구분은 각 시스템 별로 처리되는 다양한 업무단위를 구분하기 위한 일련번호 입니다.

서고문서종류코드는 하나의 분류코드(업무) 단위에 첨부될 수 있는 다양한 문서종류를 식별하기 위한 코드체계 입니다.
수입신고와 관련된 첨부서류에는 INVOICE, B/L, Packing List, 원산지증명서, 수입요건구비서류 등 여러 종류가 있습니다. 이러한 각각의 문서를 구분하기 위하여 분류코드에 일련번호 3자리를 추가하여 각각의 문서종류를 구분하고 있습니다.

• 첨부파일
첨부파일 섹션은 하나의 신고서에 첨부되는 파일 각각에 대한 메타정보를 표기하는 영역으로 첨부되는 파일의 개수 만큼 중복 기재되어야 합니다.

• 서고문서관리번호
서고문서관리번호는 전자서고에 등록된 문서 각각에 대하여 고유하게 발번되는 Document ID입니다.
첨부서류 제출 시, 해당 첨부서류가 과거 다른 신고서를 제출하면서 이미 전자서고에 등록된 경우에는 해당 문서의 서고문서관리번호 만을 기재하여 제출하면, 실물파일을 제출한 것과 동일하게 처리됩니다. 이러한 제출방식을 “참조제출”이란 용어로 정의하며 기 제출한 문서를 재활용하기 위한 처리방식이라 할 수 있습니다.

“참조제출”과 대비한 개념으로 실물파일을 제출하는 경우를 “실물제출”이란 용어로 정의합니다.

기 제출문서의 서고문서관리번호는 국가관세종합정보망의 전자서고 보관문서조회 화면을 통하여 확인할 수 있습니다.

• 서고문서파일명

서고문서관리번호에 의한 “참조제출”이 아닌 실물파일을 제출하는 경우, 즉 “실물제출”인경우에 해당파일의 파일명(확장자 포함)을 기입하는 항목입니다.

• 서고업무참조번호

해당 신고건의 PK값을 입력하는 항목입니다.
수입신고의 경우에는 “수입신고번호”, 수입신고정정신청의 경우 “수입신고 정정신청번호”, 수출신고의 경우 “수출신고번호” 등이 됩니다.
즉, 위에서 선택한 분류코드별로 PK역할을 하는 신고/신청번호 값을 기입하면 됩니다.

입력시에는 하이픈 등을 제거한 상태로 입력하여야 하며, 여러 항목으로 구성된 경우에는 각 항목을 Concatenation으로, 항목 중 숫자필드의 경우에는 자리수 만큼 ‘0’으로 채운 후 작성되어야 합니다.

예) 수입신고 : 세관부호(VC, 3)+년도(VC, 2)+신고인부호(VC, 5)
➡ XXX-YY-ZZZZZ (X) → XXXYYZZZZZ (O)
수입신고정정신청 : 수입신고번호(VC, 15)+정정신청일자(VC, 8)+정정신청차수(NN, 3)
➡ XXXXXXXXXXXXXXXYYYYYYYY001

• 파일형식코드

파일형식코드는 뒤에서 설명할 “서고문서종류코드”와 관련된 항목으로 대상파일이 하나의 문서종류로 구성된 경우에는 “개별파일” 즉 “1”로, 대상파일이 복수의 문서종류로 구성된 경우에는 “묶음파일” 즉 “2”로 표기하여야 합니다.

일반적인 경우 하나의 파일이 하나의 문서종류로 구성되지만, 수입신고의 경우 주로 첨부 되는 B/L, INVOICE, Packing List에 대해서는 신고업무의 편의를 위하여 개별파일이 아닌 하나의 파일 즉 묶음파일로 제출할 수 있도록 허용합니다.

다시 말해, “묶음파일”은 수입신고의 B/L, INVOICE, Packing List 첨부서류에만 제한적으로 허용되는 파일형식으로 여기서 말하는 묶음파일은 압축파일이 아닌 하나의 일반적인 파일을 말합니다.

“묶음파일”을 파일형식으로 지정한 경우에는 하나의 파일을 구성하는 각각의 문서종류별 시작페이지를 뒤에서 설명할 “시작페이지값” 항목에 기재하여야 합니다.

물론 수입신고의 B/L, INVOICE, Packing List의 경우에도 각각을 개별파일로 제

출할 수 있으며, 그 외의 첨부서류 및 업무의 경우에는 “개별파일”이 기본적인 파일형식이 됩니다.

• 문서작업구분코드

문서작업구분코드는 해당 파일의 제출처리가 문서를 신규 제출하기 위한 것인지, 아니면 기 제출한 문서의 삭제처리를 위한 것인지를 구분하는 항목입니다.

전자문서를 통한 첨부서류의 제출 시 문서작업구분코드는 “등록” 즉 “1”로 고정됩니다.

• 확장서고업무참조번호

확장서고업무참조번호는 하나의 첨부파일이 “서고업무참조번호” 즉 PK외에 부가적인 Secondary Key Level에 매핑될 경우 표기하는 항목입니다.

수입신고의 경우 첨부되는 각각의 첨부서류는 수입신고번호 외에 복수개의 란번호 또는 모델규격번호에 부가적으로 매핑될 수 있는데, 이와 같이 하나의 파일이 매핑되는 관련 란번호 또는 모델규격번호와 같은 항목들을 “확장서고업무참조번호”라 명명합니다.

수입신고업무와 같이 업무별로 “확장서고업무참조번호”가 존재하는 업무의 경우에는 대상파일이 매핑되는 Secondary Key 값들을 그 건수만큼 본 항목에 반복기재하면 됩니다.

• 파일정보

파일정보 섹션은 해당 파일의 문서종류를 지정하는 영역입니다.
앞의 “파일형식코드” 항목이 “1” 즉 “개별파일”인 경우에는 해당파일의 문서종류코드를 한 건 기입하면 되고, “파일형식코드” 항목이 “2” 즉 “묶음파일”인 경우에는 해당파일을 구성하는 각각의 문서종류코드 및 시작페이지를 반복 기재하여야 합니다.

• 서고문서종류코드

해당파일의 문서종류코드를 배포되는 코드집을 참조하여 기재합니다.

• 기타문서제목

해당파일의 문서종류가 “기타” 종류인 경우 사용자가 추가로 입력한 문서제목을

기재하기 위한 항목입니다.

첨부서류 제출화면에서 기타문서의 제목을 추가로 입력할 수 있는 화면의 구성은 각 업무종류에 따라 선택적으로 적용 가능합니다.

• 시작페이지값

"파일형식코드"가 "2", 즉 "묶음파일"인 경우 해당파일을 구성하는 각각의 문서종류별 시작페이지를 기입하는 항목입니다.

입력된 시작페이지는 해당 신고서 처리 시, 해당 문서종류를 찾아가기 위한 Index 역할을 합니다.
앞에서 언급한 것처럼 "묶음파일"은 수입신고의 B/L, INVOICE, Packing List 첨부서류에만 제한적으로 허용되는 파일형식 입니다.

예를 들어 하나의 파일이 B/L, INVOICE, Packing List로 구성되어 있고, B/L이 1Page부터, INVOICE가 3Page부터, Packing List 10Page부터 시작된다고 할 때 시작페이지값은 문서 종류별로 각각 1, 3, 10으로 기재 되어야 합니다.

2.2 첨부파일 제출 유형에 따른 항목작성 방법

2.2.1 실물제출

목명	TYPE	SIZE	조건	반복		작성여부	비고
전자서고			C				
분류코드	an	6	M			O	코드집 참조
첨부파일			C				
서고문서관리번호	an	15	C			X	
서고문서파일명	an..	300	C			O	파일명
서고업무참조번호	an..	500	M			O	업무키
파일형식코드	a	1	C			1 or 2	1:개별파일, 2:묶음파일
문서작업구분코드	a	1	M			1	1:등록(고정 값)
확장참조번호			C	999	999		
확장서고업무참조번호	an..	50	C			O	확장키가 있을 경우 작성
파일정보			C				
서고문서종류코드	an	9	C		999	O	코드집 참조
기타문서제목	an..	150	C			O	Optional 항목
시작페이지값	a..	22	C			O	파일형식코드 "2"인 경우 작성

2.2.2 참조제출

항목명	TYPE	SIZE	조건	반복		작성여부	비고
전자서고			C				

분류코드	an	6	M			O	코드집 참조
첨부파일			C				
서고문서관리번호	an	15	C			O	
서고문서파일명	an..	300	C			X	원본파일명
서고업무참조번호	an..	500	M			O	업무키
파일형식코드	a	1	C			1 or 2	1:개별파일, 2:묶음파일
문서작업구분코드	a	1	M			1	1:등록(고정 값)
확장참조번호			C	999	999		
확장서고업무참조번호	an..	50	C			O	확장키가 있을 경우 작성
파일정보			C				
서고문서종류코드	an	9	C		999	O	코드집 참조
기타문서제목	an..	150	C			O	Optional 항목
시작페이지값	a..	22	C			O	파일형식코드 "2"인 경우 작성

부록 6. 사용자 S/W 개발 가이드

1. 요청 및 응답

사용자 S/W를 이용한 연계 방식은 서버 대 서버 방식과 다른 클라이언트 대 서버 방식으로 클라이언트에서 요청을 하면 서버에서 응답을 주는 구조이며, SSL을 이용하여 서버와 통신을 한다. 따라서 문서 송신 요청은 첨부가 있는 구조(Mulipart)로 본 지침서의 내용에 준수하여 통신 하고, 문서/목록 수신 요청은 첨부가 없는 구조(Simplepart)에 준수하여 통신 한다. 보안 적용은 4장을 참고하여 보안 표준을 준수하되 암/복호화 부분은 SSL통신으로 대체한다. 첨부 유무에 따라서 변경되는 부분을 다음과 같이 기술한다.

① HTTP 헤더 정보 설정 방법

구분	HTTP 헤더 정보(Content-Type)	비고
Multipart	Content-Type:Multipart/Related	첨부 존재
Simplepart	Content-Type:text/xml	첨부 없음

(* Multipart는 5.2 HTTP 헤더 구조 참조)

다음은 Simplepart을 사용한 예이다.

```
POST /service/ebXMLHandler HTTP/1.1
Host: localhost
SOAPAction: "ebXML"
Content-type: text/xml;charset=UTF-8
Authorization: Basic 4czqHGdsS4pfHF3BEeo4VF7pLY=:KoYMzj7dLTaQSDRFGHHUIKKJJ...NMHJK
Accept : text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection : keep-alive
Content-Length : 85571
locale : ko_KR
```

② 사용자 S/W 통신 종류별 SOAP 메시지 설정 방법

구분		패키지 형태	SOAP Header (eb:Action)	SOAP Header (기타)	Data(http body)
신청서	요청	Multipart	KCSMetaAction / KCSSingleAction	5.3 MIME 구조 참조	N/A
	응답	N/A	N/A	N/A	N/A
통보서 목록	요청	Simplepart	KCSListReqAction	문서함 ID	N/A
	응답	Text	N/A	N/A	통보서 목록
통보서	요청	Simplepart	KCSFileReqAction	문서함 ID, 전자문서 메시지ID	N/A
	응답	Text	N/A	N/A	통보서 XML
요건 확인서 목록	요청	Simplepart	KCSRListReqAction	문서함 ID	N/A
	응답	Text	N/A	N/A	요건 확인서 목록
요건 확인서	요청	Simplepart	KCSRFileReqAction	문서함 ID, 전자문서 메시지ID	N/A
	응답	Text	N/A	N/A	요건 확인서 XML

[각 태그의 경로]

- eb:Action : SOAP/Header/MessageHeader/Action
- 문서함ID : SOAP/Header/MessageHeader/From/PartyId
- 전자문서메시지ID : SOAP/Header/MessageHeader/ConversationId

1.1 첨부가 없는 방식의 구조(Simplepart)

HTTP 전송 프로토콜을 이용하여 SOAP 메시지를 전송하는 방식이다.

Simplepart의 구조와 예제는 다음과 같다.

구조)

```
HTTP Header  +  SOAP Envelope ( SOAP Header + SOAP Body )
```

예제)

HTTP 헤더

```
POST /service/ebXMLHandler HTTP/1.1
Host: localhost
SOAPAction: "ebXML"
Content-type: application/soap+xml;charset=UTF-8
Authorization: Basic 4czqHGdsS4pfHF3BEeo4VF7pLY=:KoYMzj7dLTaQSDRFGHHUIKKJJ...NMHJK
Accept : text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection : keep-alive
Content-Length : 85571
locale : ko_KR
```

SOAP Envelope

```
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
```

SOAP 헤더

```
<SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_
0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader" eb:version="2.0">
  ..........(중략).............
  </eb:MessageHeader>
<eb:SyncReply SOAP:mustUnderstand="1" eb:version="2.0"
SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
</SOAP:Header>
```

SOAP 바디

```
<SOAP:Body>
..........(중략).............
</SOAP:Body>
</SOAP:Envelope>
```

1.2 신청서 요청 및 응답

1.2.1 신청서 요청

5.3장 MIME 구조 참조하며, 전자문서 암호화는 생략하고 채널 암호화인 SSL 통신으로 대체한다.

1.2.2 신청서 요청에 대한 응답

정상/오류 코드 값이 리턴이 된다. (부록7. 오류코드 참조)

1.3 통보서 목록 요청 및 응답

1.3.1 통보서 목록 요청

메시지에 eb:Action, 문서함ID를 입력하여 ebMS로 요청한다.
다음은 메시지 예제이다.

```
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
<SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_
0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader" eb:version="2.0">
    <eb:From>
      <eb:PartyId eb:type="ok-customs.dtm1">XX12345678901234</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
    </eb:From>
    <eb:To>
      <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#seller</eb:Role>
    </eb:To>
    <eb:CPAId>KCSIPTJXA0001</eb:CPAId>
    <eb:ConversationId></eb:ConversationId>
    <eb:Service eb:type="anyURI">urn:Ok-Customs-Service:order</eb:Service>
    <eb:Action>KCSListReqAction</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20150113104106603125</eb:MessageId>
      <eb:Timestamp>2015-01-13T10:41:15.165Z</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
<eb:SyncReply SOAP:mustUnderstand="1" eb:version="2.0"
SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
</SOAP:Header>
<SOAP:Body>
..........(중략).............
</SOAP:Body>
</SOAP:Envelope>
```

1.3.2 통보서 목록 요청에 대한 응답

정상/오류 코드(부록7. 오류코드 참조), 통보서 목록들 값이 리턴이 된다. 다음은 리턴 데이터 예제이다. (발신일시+전자문서메시지ID,발신문서코드)

```
20150911123359ELI-19b4c39a-9f79-4517-9f57-cffb6b4b485e,GOVCBRR20
20150911130006ELI-2b4f39b6-c0e6-4b99-943f-5e16aa6cb667,GOVCBRR20
20150911135032ELI-9b135f1e-247b-4ee1-b7ee-4c75285bf189,GOVCBRR20
20150911135359ELI-d2b470a2-5333-4e37-876f-217f4469ccb2,GOVCBRR20
20150911135504ELI-010fd6ad-8c6f-4c3c-bdb9-ec83090d34eb,GOVCBRR20
20150911135513ELI-3e948cc2-5069-410d-bb55-b4a6498733dc,GOVCBRR20
20150911135521ELI-19f6a49f-311f-43e3-869e-dd9e610b97f4,GOVCBRR20
20150915183829ELI-f9bd4d11-3dca-4b20-a8c8-8c249497540a,GOVCBRR20
20150921090045ELI-678f0e35-dc1d-48bf-a7cc-ff920a15cc85,GOVCBRR20
20150921144049ELI-ae569c47-5e8d-432e-9818-247d92094f62,GOVCBRR20
```

1.4 통보서 요청 및 응답

1.4.1 통보서 요청

메시지에 eb:Action, 문서함ID, 전자문서 메시지ID를 입력하여 ebMS로 요청한다.

다음은 메시지 예제이다.

```
<SOAP:Envelope xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xlink="http://www.w3.org/1999/xlink"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/soap/envelope/
http://www.oasis-open.org/committees/ebxml-msg/schema/envelope.xsd">
<SOAP:Header
xmlns:eb="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd"
xsi:schemaLocation="http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_
0.xsd http://www.oasis-open.org/committees/ebxml-msg/schema/msg-header-2_0.xsd">
  <eb:MessageHeader SOAP:mustUnderstand="1" eb:id="MessageHeader" eb:version="2.0">
    <eb:From>
      <eb:PartyId eb:type="ok-customs.dtm1">XX12345678901234</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#sender</eb:Role>
    </eb:From>
    <eb:To>
      <eb:PartyId eb:type="ok-customs.dtm1">OK-CUSTOMS</eb:PartyId>
      <eb:Role>http://www.ok-customs.go.kr/ebMSH#seller</eb:Role>
    </eb:To>
    <eb:CPAId>KCSIPTJXA0001</eb:CPAId>
    <eb:ConversationId>발신일시+전자문서메시지ID</eb:ConversationId>
    <eb:Service eb:type="anyURI">urn:Ok-Customs-Service:order</eb:Service>
    <eb:Action>KCSListReqAction</eb:Action>
    <eb:MessageData>
      <eb:MessageId>20150113104106603125</eb:MessageId>
      <eb:Timestamp>2015-01-13T10:41:15.165Z</eb:Timestamp>
    </eb:MessageData>
  </eb:MessageHeader>
<eb:SyncReply SOAP:mustUnderstand="1" eb:version="2.0"
SOAP:actor="http://schemas.xmlsoap.org/soap/actor/next"/>
</SOAP:Header>
<SOAP:Body>
.....(중략).....
</SOAP:Body>
</SOAP:Envelope>
```

1.4.2 통보서 요청에 대한 응답

정상/오류 코드(부록7. 오류코드 참조), 전자서명된 통보서 XML 값이 리턴이 된다. 전자서명 알고리즘은 4장.보안표준을 참고한다.

다음은 리턴 데이터 예제이다.(통보서XML + 전자서명)

```
<wco:Response
xmlns:kcs="urn:kr:gov:kcs:data:standard:KCS_ResponseOfBEV_R20SchemaModule:1:0"
xmlns:wco="urn:kr:gov:kcs:data:standard:KCS_ResponseOfBEV_R20SchemaModule:1:0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:kr:gov:kcs:data:stan
dard:KCS_ResponseOfBEV_R20SchemaModule:1:0
./schema4G/kcs/data/standard/KCS_ResponseOfBEV_R20SchemaModule_1.0_standard.xsd">
    <wco:IssueDateTime>20150914155308</wco:IssueDateTime>
    <wco:TypeCode>GOVCBRR20</wco:TypeCode>
    <wco:Declaration>
        <wco:AcceptanceDateTime>20150914155308</wco:AcceptanceDateTime>
        <wco:DeclarationOfficeID>01020</wco:DeclarationOfficeID>
        <wco:ID>4321013123456</wco:ID>
        <wco:TypeCode>GOVCBRD63</wco:TypeCode>
        <wco:VersionID>1</wco:VersionID>
    </wco:Declaration>
    <wco:Error>
        <kcs:Description>오류내역</kcs:Description>
        <wco:Pointer>
            <wco:DocumentSectionCode>1</wco:DocumentSectionCode>
            <wco:SequenceNumeric>3</wco:SequenceNumeric>
            <wco:TagID>오류문서 Key1</wco:TagID>
            <wco:TagID>오류문서 Key2</wco:TagID>
            <wco:TagID>오류문서 Key3</wco:TagID>
        </wco:Pointer>
    </wco:Error>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xsi:schemaLocation="http://www.w3.org/2000/09/xmldsig#
http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd">
.....(중략).....
</ds:Signature></wco:Response>
```

부록7. 오류코드

1. 오류코드 구조

HTTP 헤더에 오류 관련 정보를 넣어서 신고인에게 전송 한다.

1.1 HTTP 헤더 정보

항목명(Name)	항목값(Value)	비고
CustomsErrCode	C401	
CustomsErrDesc	Identification Error	

다음은 오류코드를 사용한 예이다.

```
POST /service/ebXMLHandler HTTP/1.1
Host: localhost
SOAPAction: "ebXML"
Content-type: text/xml;charset=UTF-8
Accept : text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection : keep-alive
Content-Length : 85571
locale : ko_KR
CustomsErrCode : C401
CustomsErrDesc : Identification Error
```

2. 오류코드 목록

오류분류	번호	에러코드	오류코드설명	오류내용 설명 및 조치사항
접근제어	1	C401	신원확인오류로 수신거부 (Identification Error)	신원확인정보(본인확인) 내용이 있는 Http Header에 Authoriztation 항목이 누락되었거나 Authoriztation에 "사용자ID:신원확인정보"를 잘못 기재 되어 있는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서에 본인확인 표준을 참고하시기 바랍니다.
ebXML 오류	2	C402	등록되지 않은 문서함사용 (Unregistered Document Box)	관세청에 등록된 귀사의 문서함이 맞는지 MyCustoms에서 확인 바랍니다.
	3	C410	정의되지 않은 Action이 사용됨 (Undefined Action)	수신된 SOAP 메시지내에 eb:Action 값은 관세청에서 정의한 값만 허용 가능합니다. SOAP:Header 하위에 eb:Action Tag 값을 잘못 기재 되었는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서를 참고하시기 바랍니다.
	4	C411	SOAP 메시지 필수값 오류 (Soap Message Mandatory Value Error)	SOAP:Header의 필수값이 누락 또는 잘못기재 되어 있는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서를 참고하시기 바랍니다.
	5	C412	서식 미첨부 오류	수신된 ebXML 메시지 안에 Payload(신고서 & 첨부파일)

			(Not Attach Payload)	SOAP 메시지만 있습니다. Payload가 누락 되었는지 확인 바랍니다.
	6	C450	수신정지대상 문서함 (Suspended Document Box)	관세청에 등록된 귀사의 문서함에 사용 상태를 MyCustoms에서 확인 바랍니다.
서식오류	7	C501	서식 검증 오류 (XML Schema Verification Error)	수신된 신고서의 서식이 관세청에서 배포한 해당 서식과 불일치 합니다. 관세청에서 배포한 해당 문서의 항목정의서를 참고하시기 바랍니다. (XML 스키마 오류)
	8	C502	문서코드와 서식 불일치 (Document Code And Document format Inconsistency)	관세청에서 정의한 문서코드와 신고서 서식이 불일치 합니다. 신고서식에 맞는 문서코드를 사용하여 SOAP Description을 수정하시기 바랍니다.
	9	C503	등록되지 않은 문서코드 사용 (Unregistered Document Code)	각 업무별 관세청에서 정의한 문서코드를 사용하시기 바랍니다.
	10	C504	요건 서식 검증 오류 (XML Schema Verification Error)	수신된 신고서(통보서)의 서식이 관세청에서 배포한 해당 서식과 불일치 합니다. 관세청에서 배포한 해당 문서의 항목정의서를 참고하시기 바랍니다. (XML 스키마 오류)
전자문서 메타정보 오류	11	C600	전자문서메타정보 XML 스키마 오류 (Document Meta Data XML Schema Verification Error)	수신된 전자문서메타정보 XML 서식이 관세청에서 배포된 해당 서식과 불일치 합니다. 관세청에서 배포한 해당 문서의 항목정의서를 참고하시기 바랍니다. (XML 스키마 오류)
	12	C601	전자문서메타정보 XML 필수값 오류(Document Meta Data XML Mandatory Value Error)	수신된 전자문서메타정보 XML에 필수값이 누락 또는 잘못기재 되어 있는지 확인 바랍니다. 관세청에서 배포한 해당 문서의 항목정의서를 참고하시기 바랍니다.
	13	C602	전자문서메타정보 XML내용과 Payload 구조와 불일치 (Document Meta Data XML Contents And Payload Structure Inconsistency)	수신된 전자문서메타정보 XML의 전자문서와 첨부파일 개수와 실제 ebXML의 Payload 개수와 일치하지 않습니다. 해당 서식의 내용과 ebXML 메시지를 비교해서 다른 부분을 수정하시기 바랍니다.
	14	C603	Payload-1에 메타XML 없음 (Not Payload-1 Document Meta Data XML)	SOAP 헤더의 eb:Action의 값이 "KCSMetaAction"인 경우는 ebXML 메시지 Payload-1에 전자문서메타정보 XML이 위치해야 합니다.
	15	C604	전자문서메타정보 XML 문서코드와 서식 불일치 (Document Meta Data XML Contents And Document Code Inconsistency)	수신된 전자문서메타정보 XML의 전자문서코드와 신고서식의 전자문서코드와 불일치 합니다. 신고서식에 맞는 문서코드를 사용하여 전자문서메타정보 XML를 수정하시기 바랍니다.
전자서명 검증오류	16	C420	SOAP 전자서명 검증 오류 (Soap Message Electronic Signature Verification Error)	XML DISG(XML Digital Signature)에 기술된 전자서명 표준과 관세청에서 지원하는 알고리즘이 사용되었는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서를 참고하시기 바랍니다.
	17	C421	신고서 전자서명 검증 오류 (XML Electronic Signature Verification Error)	XML DISG(XML Digital Signature)에 기술된 전자서명 표준과 관세청에서 지원하는 알고리즘이 사용되었는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서를 참고하시기 바랍니다.
암복호화 오류	18	C430	신고서 복호화 오류 (XML Decryption Error)	W3C의 XML Encryption에 기술된 암호화 표준과 관세청에서 지원하는 알고리즘이 사용되었는지 확인 바랍니다. 자세한 내용은 전자문서 표준연계 지침서를 참고하시기 바랍니다.
통보서요청(사용자	19	C901	수신할 문서 없음 (No Data)	문서함의 발신대기중인 통보서 문서가 없습니다. (사용자S/W : 통보서 리스트 요청)

S/W)	20	C902	수신할 파일 없음 (File Not Found)	문서함의 요청파일을 찾을 수 없습니다. (사용자S/W : 통보서 파일요청)
기타코드	21	C200	정상처리 (Success)	ebXML 메시지가 정상 처리 되었습니다.
	22	C500	서버 시스템 오류 (System Error)	관세청 시스템 내부 오류가 발생하였습니다.

부록8. 시스템 오류통보

1. 시스템 오류 통보서 항목정의서

순번	서식 항목명	항목설명	Sample Value
1	문서형태구분	문서코드를 기재	G0VCBRINF
2	오류통보일시	오류통보일시를 기재	CCYYMMDDHHMMSS
3	신청문서 수신일시	신청문서 수신일시	CCYYMMDDHHMMSS
4	오류발생 메시지ID	발신자(=송신자)생성한 유일한 문서번호	20150601000001
5	오류발생 컨텐트ID	전자문서 페이로드의 Content-ID	payload-2
6	오류발생 제출번호	오류발생 문서의 문서번호(제출번호)를 기재	4321013123456
7	오류발생 문서구분	오류발생 문서의 문서구분코드를 기재	G0VCBR5DA
8	**오류내역**		
9	오류코드	오류응답코드를 기재	C501
10	오류내역	오류상세내역을 기재	서식검증오류

다음은 시스템 오류 통보서를 사용한 예이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<wco:Response
    xmlns:kcs="urn:kr:gov:kcs:data:standard:KCS_ResponseOfGSG_INFSchemaModule:1:0"
    xmlns:wco="urn:kr:gov:kcs:data:standard:KCS_ResponseOfGSG_INFSchemaModule:1:0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:kr:gov:kcs:data:standard:KCS_ResponseOfGSG_INFSchemaModule:1:0
../../schema4G/kcs/data/standard/KCS_ResponseOfGSG_INFSchemaModule_1.0_standard.xsd">
    <!--오류통보일시(CCYYMMDDHHMMSS)-->
    <wco:IssueDateTime>20150603123012</wco:IssueDateTime>
    <!--문서형태구분(G0VCBRINF)-->
    <wco:TypeCode>G0VCBRINF</wco:TypeCode>
    <wco:Declaration>
        <!--신청문서 수신일시(CCYYMMDDHHMMSS)-->
        <wco:AcceptanceDateTime>20150603123012</wco:AcceptanceDateTime>
        <!--오류발생 제출번호-->
        <wco:ID>4321013123456</wco:ID>
        <!--오류발생 문서구분-->
        <wco:TypeCode>G0VCBR5DA</wco:TypeCode>
        <wco:AdditionalInformation>
            <!--오류발생 메시지ID-->
            <kcs:MessageID>20150601000001</kcs:MessageID>
            <!--오류발생 컨텐트ID-->
            <kcs:ContentID>payload-2</kcs:ContentID>
        </wco:AdditionalInformation>
        <wco:Error>
            <!--오류코드-->
            <wco:ValidationCode>C501</wco:ValidationCode>
            <!--오류내역-->
            <kcs:Description>서식검증오류</kcs:Description>
        </wco:Error>
    </wco:Declaration>
</wco:Response>
```

부록 9. 개정 이력표

관리본개정이력표

문서명	표준연계지침서

버 전	날 짜	내 용	작성자
Draft	2014.12.11	최초제정	심용무
	2015.01.16	통보서의 전자서명/암호화 추가 5.5장 사용자 S/W의 통보서 목록 요청 및 통보서 요청 추가	심용무
	2015.03.16	사용자S/W 개발 가이드 추가 (2.2.2장, 부록 6)	심용무
	2015.04.22	SOAP 메시지의 prefix 변경 (env -> SOAP)	심용무
	2015.05.12	첨부서류 사후 제출 관련 내용 수정 - 5.2 HTTP 헤더 구조 (“5.3.3.1 페이로드 구조” 내용 추가) - 부록 5. Document Meta XML 항목정의서 (“2.1 신고인 작성 가이드”내용 추가) - 부록 5. Document Meta XML 항목정의서 (“1.온라인 첨부파일 제출 기능”내용 삭제) (“2.2.2장 사후 제출” 내용 삭제)	심용무
	2015.07.07	- Page 13 사용가능인증서 설명문 일부내용 삭제	심용무
	2015.07.21	- Page 4 지침서 개요 내용 일부 삭제(1.1.4장) - Page 49 7장 사용자 정보 관리정책 내용 추가 (“4세대 오픈전 최종버전 확정 후 배포 예정”)	심용무
	2015.07.27	시스템 오류 처리 관련 내용 수정 - 2.3 시스템 오류 처리 내용 수정 - 부록7. 오류코드 추가 - 부록8. 시스템 오류통보 추가	심용무
	2015.07.28	오류코드를 SOAP 메시지에서 HTTP 헤더로 변경 - 2.2.2 사용자 S/W 연계 처리 절차 (신청서 응답의 전자서명 제거) - 부록 6. 사용자 S/W 개발 가이드 (응답코드 관련 내용 변경)	심용무
	2015.08.31.	- Page 13 인증기관별 사용가능 공인인증서 내용 삭제	심용무

	2015.10.23 2015.12.18	사용자S/W SSL통신 채널 암호화 관련 내용 수정 - Page 6 1.2.2 업무처리 절차 (“신고서 전송” 내용 수정) - Page 9 2.2.2 사용자 S/W 연계 처리 절차 내용 수정 - Page 85 부록 6. 사용자 S/W 개발 가이드 내용 수정 (“1. 요청 및 응답” 내용 수정) 국가관세종합정보망에서 사용 가능한 인증서 내용 수정 - Page 14, 4.1.1 사용 인증서 종류 수정 - Page 76, 1.국가관세종합정보망 암호화 인증서 다운로드내 URL 정보 수정 문서수발신 오류코드 추가 정정 - Page 95, 2.오류코드, C450 추가	