

공인전자문서센터 이·수관 기술규격

**Technical Standard for Documents
Transfer between ARCs**

v3.00

2014년 1월

목 차

| | |
|----------------------------------|----------|
| 1. 규격의 개요 | 1 |
| 1.1 목적 | 1 |
| 1.2 적용 대상 및 범위 | 1 |
| 1.3 참고 자료 | 1 |
| 1.4 규격 어휘 | 2 |
| 2. 용어 정의 | 4 |
| 2.1 용어 | 4 |
| 2.2 약어 | 5 |
| 3. 전자문서 이 · 수관 | 6 |
| 3.1 개요 | 6 |
| 3.1.1 이관 대상 정보 | 6 |
| 3.1.2 사전 준비 작업 | 7 |
| 3.1.3 전자문서이관 절차 | 8 |
| 3.1.3.1 전자문서이관절차 흐름도 | 9 |
| 3.1.4 이 · 수관 방안 | 11 |
| 3.1.4.1 온라인/오프라인 이 · 수관 방안 | 12 |
| 3.2 이 · 수관 정보구조 | 14 |
| 3.2.1 개요 | 14 |
| 3.2.2 메시지 패키징 | 14 |
| 3.2.2.1 온라인 메시지 패키징 | 14 |
| 3.2.2.2 오프라인 메시지 패키징 | 15 |
| 3.2.2.3 SOAP 패키징 | 16 |
| 3.2.3 이 · 수관 요청메시지 | 22 |
| 3.2.3.1 기본 정보 | 22 |
| 3.2.3.2 스키마 구조 | 22 |
| 3.2.3.3 메시지 구조 | 22 |
| 3.2.3.4 필드 설명 | 23 |
| 3.2.3.5 Slot 구조 | 24 |
| 3.2.4 이 · 수관 응답메시지 | 25 |
| 3.2.4.1 기본 정보 | 25 |
| 3.2.4.2 스키마 구조 | 25 |
| 3.2.4.3 메시지구조 | 26 |
| 3.2.4.4 필드 설명 | 27 |
| 3.2.4.5 Slot 구조 | 28 |
| 3.2.5 이관 정보 패키지 | 29 |
| 3.2.5.1 이 · 수관 정보 기본구조 | 29 |
| 3.2.6 전자서명의 범위 | 46 |

| | |
|--------------------------------------|----|
| 3.2.6.1 이 · 수관 메시지 전자서명 | 46 |
| 3.2.6.2 패키지 전자서명 | 47 |
| 3.3 온라인 이 · 수관 단계별 처리 방안 | 48 |
| 3.3.1 개요 | 48 |
| 3.3.2 통신 프로토콜 및 메시지 처리 흐름 | 48 |
| 3.3.2.1 처리절차 | 48 |
| 3.3.2.2 프로토콜 정의 | 48 |
| 3.3.3 오류 처리 방안 | 49 |
| 3.3.4 온라인 보안 처리 방안 | 49 |
| 3.4 오프라인 이 · 수관 단계별 처리 방안 | 50 |
| 3.4.1 개요 | 50 |
| 3.4.2 오프라인 처리 단계 | 50 |
| 3.4.2.1 이관 공인전자문서센터의 사전 준비 작업 | 50 |
| 3.4.2.2 이관 공인전자문서센터의 Export 절차 | 54 |
| 3.4.2.3 이관데이터 전달 방안 | 57 |
| 3.4.2.4 수관 공인전자문서센터의 Import 절차 | 57 |
| 3.4.3 오프라인 보안 처리 방안 | 58 |

1. 규격의 개요

1.1 목적

공인전자문서센터는 고객이 보관한 전자문서에 대해서 안정적이고 신뢰성 있게 보관하고, 보관된 전자문서를 서비스하도록 법적으로 “공인”된 서비스 사업자이다. 따라서 사용자의 요구 및 공인전자문서센터의 인증취소나 영업폐지와 같은 사정으로 인해 전자문서보관을 지속할 수 없는 상황이 발생하였을 때, 타 공인전자문서센터 시스템으로 보관중인 전자문서를 안전하고 신속하게 이관하여 고객(이용자)에게 서비스할 수 있어야 한다.

공인전자문서센터는 각 사업자별로 고객에게 최적의 서비스를 제공하기 위해 고유의 시스템 아키텍처 및 정보모델을 보유하고 있다. 이처럼 서로 다른 정보 구조를 가진 공인전자문서센터 간에 원활하게 전자문서를 이·수관하기 위해서는 이에 필요한 수행방안, 수행절차, 전달되는 정보 및 자료의 범위, 구조 등에 표준안을 제시하여야 한다.

“공인전자문서센터 이·수관 기술규격”(이하 본 규격)은 공인전자문서센터 서비스 사업자가 원활하게 전자문서를 이관하거나 수관 받을 수 있도록 하기 위한 기준안을 제시하고자 작성되었다.

1.2 적용 대상 및 범위

모든 공인전자문서센터는 본 규격을 준수하여 보관중인 전자문서를 타 공인전자문서센터로 이관할 수 있어야 하며, 타 공인전자문서센터가 이관 요청하는 전자문서를 수관할 수 있어야 한다.

1.3 참고 자료

- ☐ ISO 14721; Space data and information transfer systems - Open Archival Information System - Reference model, 2003
- ☐ ISO/TS 23081-1; Information and documentation - Records management processes - Metadata for records, 2004
- ☐ ISO 15489-1; Information & documentation-Records management, 2001
- ☐ Requirements for Electronic Records Management System-Metadata Standard, 영국 PRO 메타데이터 표준, 2004

- ☐ RMSCA; Recordkeeping Metadata Standards for Commonwealth Agencies, 호주 국립기록관(NAA) 전자기록관리를 위한 메타데이터
- ☐ 대통령비서실 기록관리시스템 구축 메타데이터 정의서 및 설명서, 2006
- ☐ 기록관리시스템혁신 ISP사업, 국가기록원, 2005
- ☐ NIPA-TS-INTERFACE; 이용자시스템과 공인전자문서센터 간 연계 인터페이스 기술규격 v2.10, 정보통신산업진흥원, 2013
- ☐ NIPA-TS-PACKAGE; 전자문서 정보패키지 기술규격 v3.00, 정보통신산업진흥원, 2013
- ☐ NIPA-TS-CERTIFICATE; 전자문서 증명서 포맷 및 운용절차 기술규격 v3.00, 정보통신산업진흥원, 2013

1.4 규격 어휘

본 지침에서 제시하고 있는 규칙 적용과 관련하여 다음과 같은 유형의 문장 어구를 사용하고 있다. 한글만으로 표현이 충분하지 않은 경우에는 영문을 병기하였다.

- ☐ 필수 요소 : 이 지침에서 제시하는 규칙을 절대적으로 따라야 할 때 사용한다. 지침에 부합하기 위해서는 이것을 엄밀하게 따라야 하며, 이것을 벗어나는 것을 인정하지 않는다. (영문 : Must, Must Not)
 - ~ 한다.
 - ~ 하여야 한다.
 - ~ 안된다.
 - ~ 않는다.
- ☐ 권고(선택) 요소 : 이 지침에서 제시하는 규칙을 따르는 것을 권고할 때 사용한다. 이는 이 밖의 것도 좋지만 이것이 특히 적당하다는 것을 나타낼 때 사용한다. (영문 : Should)
 - ~ 하도록 한다.
- ☐ 완곡한 금지 요소 : 지침의 입장에서 바람직하지 않지만, 반드시 금지하지 않는다. (영문 : Should Not)

- ~ 하지 않도록 한다.

☐ 허용 요소 : 지침의 입장에서 허락한다는 것을 나타낸다. (영문 : May)

- ~ 할 수 있다.

2. 용어 정의

2.1 용어

- 1) “이관”이란 공인전자문서센터가 자체적으로 보관하고 있는 전자문서를 다양한 필요성에 의해 보관, 활용, 관리서비스를 중지하고 타 공인전자문서센터로 등록, 활용, 관리를 의뢰하기 위해 전자문서, 최초등록증명서와 관리정보를 전달하는 것을 말한다.
- 2) “수관”이란 타 공인전자문서센터가 보관하고 있던 전자문서를 이관 의뢰하는 경우 이를 전달 받아서 고객에게 등록, 활용, 관리서비스를 제공하기 위해 공인전자문서센터의 정보구조에 맞게 전자문서 및 관리정보를 등록하는 것을 말한다.
- 3) “이관 공인전자문서센터”란 보관하고 있던 전자문서를 타 공인전자문서센터로 “이관”의뢰하는 공인전자문서센터를 말한다.
- 4) “수관 공인전자문서센터”란 “이관 공인전자문서센터”의 이관의뢰를 받아서 전자문서를 “수관”하는 공인전자문서센터를 말한다.
- 5) “이관 모듈”이란 “이관 공인전자문서센터”가 이관대상인 전자문서 정보를 공인전자문서센터 시스템에서 추출(export)하여 수관 공인전자문서센터로 전달하는 작업을 하는 프로그램을 말하며, 온라인과 오프라인 방식의 이관을 모두 지원한다.
- 6) “수관 모듈”이란 “수관 공인전자문서센터”가 이관 공인전자문서센터로부터 이관 요청 정보를 수신한 후, 이를 해석하여 수관 공인전자문서센터의 공인전자문서센터시스템에 저장하는 작업을 하는 프로그램을 말하며, 온라인과 오프라인 방식의 이관을 모두 지원한다.
- 7) 이관 정보패키지(Transfer Information Package, 이하 TIP)란 공인전자문서센터가 보관하고 있는 전자문서를 타 공인전자문서센터로 이관하기 위해 이관대상이 되는 정보를 전자문서단위로 구조화한 정보패키지를 말한다. TIP는 패키지헤더, XML영역, 전자문서첨부파일, 최초등록증명서로 구성된다.
- 8) “스키마”란 일반적으로 데이터나 정보의 구조를 말하며, 본 규격에서는 특별히 XML로 데이터를 정의하기 위한 구조를 의미한다.
- 9) “보존 정보패키지”(이하 AIP), “배부 정보패키지”(이하 DIP)의 정의는 “전자문서 정보패키지 기술규격 v3.00”(이하 패키지 규격)의 정의를 따른다.
- 10) “증명서”란 공인전자문서센터가 이용자에게 전자문서등록, 전자문서발급, 전자문서이관, 전자문서폐기의 사실에 대한 증명, 발급된 전자문서의 내용이 원본문서와 동일함에 대한 증명, 시점확인 증명 등을 위해 발급하는 보증서를 말하며, 각 증명서의 정의는 “전자문서 증명서 포맷 및 운용절차 기술규격 v3.00”(이하 증명서

규격)의 정의를 따른다.

11) “증적”의 정의는 증명서 규격의 정의를 따른다.

2.2 약어

1. XML : eXtensible Markup Language, 확장성 마크업 언어
2. SOAP : Simple Object Access Protocol
3. GMT : Greenwich Mean Time, 그리니치 표준시
4. DN : Distinguished Name, 식별명칭
5. TIP : Transfer Information Package, 이관 정보패키지
6. AIP : Archival Information Package, 보존 정보패키지
7. DIP : Dissemination Information Package, 배부 정보패키지

3. 전자문서 이·수관

3.1 개요

공인전자문서센터는 다양한 사유로 인하여, 보관중인 전자문서를 타 공인전자문서센터로 이관하거나 타 공인전자문서센터에서 보관 중이던 전자문서를 수관 받게 될 수 있다. 이·수관 작업은 공인전자문서센터에 기 등록되어 보관 중이던 전자문서를 타 공인전자문서센터로 옮기는 작업이기 때문에, 이용자가 전자문서를 공인전자문서센터에 신규등록하는 과정과는 달리, 최초등록시점 및 보관사실 증명, 동일 식별자 처리, 이용자 정보와의 매핑, 관리정보 등록, 무엇보다도 대량의 전자문서에 대한 처리 등 고려해야할 사항이 많다.

모든 공인전자문서센터의 문서보관설비의 구현방식이 동일하지 않을 수 있기 때문에, 본 규격에서는 이·수관 대상, 이·수관 절차, 송·수신 프로토콜, 패키지 포맷, 보안 요건 등, 모든 공인전자문서센터 시스템에 적용 가능한 이·수관 공통사항에 대하여 규정하고 있으며, 데이터 export와 import 절차 등 문서보관설비 구현방식과 관련된 부분은 이관 공인전자문서센터와 수관 공인전자문서센터의 협의 하에 적절한 방식으로 수행할 것을 제안하고 있다.

3.1.1 이관 대상 정보

이관대상이 되는 데이터는 각 이용자별로 보관 의뢰한 전자문서, 최초등록증명서 및 관리를 위한 각종 관리정보가 된다.

- 전자문서 : 이용자가 등록한 전자문서 원본으로서 TIP 형태로 변환되어 이·수관 됨. 필수 이·수관 대상 정보임
- 최초등록증명서 : 이용자가 공인전자문서센터에 전자문서를 등록 의뢰하는 최초 시점에 정상적으로 등록되었음을 증명하기 위해 증명서 규격에 정의된 포맷으로 발행하였던 구조체 정보임. 수관 공인전자문서센터는 TIP에 첨부된 최초등록증명서에 대한 검증을 수행한 후, 증명대상 필드의 정보를 그대로 유지하여 최초등록증명서를 재발급하여야 함. 수관 공인전자문서센터에서 타 공인전자문서센터로 전자문서에 대한 이·수관이 다시 발생하게 되면 수관 공인전자문서센터에서 재발급했던 최초등록증명서만 이·수관 대상으로서 이관됨. 공인전자문서센터와 이용자가 합의한 경우 전자문서 등록 시에 최초등록증명서가 발급되지 않는 경우도 있기 때문에, 이관 공인전자문서센터는 이관대상 전자문서에 대한 최초등록증명서가 발급되었는지 확인하여, 발급되지 않은 상태라면 발급을 수행하여야 함. 또한, 최초등록증명서가 발급된 상태이나 이관시점에 최초등록증명서에 첨부된 전자서명의 유효기간이 만료되었다면 이관 공인전자문서센터는 반드시 유효한 인증서를 이용하여 최초등록증명서를 갱신한 후 이관하여야 함. 필수 이·수관 대상 정보임

- 이용자 정보 : 양 공인전자문서센터간 협의 하에 전자문서 이·수관 전에 미리 이관 또는 등록되어야 함. 선택적 이·수관 대상 정보임
- 관리정보 : 선택적 이·수관 대상 정보임
 - 전자문서에 대한 기본속성 정보 : 패키지 번호, 등록일자, 등록자, 소유자
 - 전자문서에 대한 확장속성 정보 : 이관 공인전자문서센터 및 관리되는 전자문서유형에 따라 추가적으로 정의됨
 - 전자문서에 대한 보안(접근권한) 정보
 - 그 외 기타 정보
 - 연관관계 정보 : 전자문서와 분류체계 간 연관정보, 전자문서 및 속성정보와 연관정보, 증명서 자료와의 연관정보

3.1.2 사전 준비 작업

공인전자문서센터가 전자문서를 원활하게 이·수관하기 위해서는 다음과 같은 사전 준비 작업을 수행하도록 한다.

- 이관 대상 및 범위를 기준으로 이·수관 공인전자문서센터 간 협의
 - 이관 공인전자문서센터는 이관대상 및 범위를 확정하여 수관 공인전자문서센터와 업무협의를 통해 이관요청에 대한 수용여부를 결정함
 - 이관 대상 및 범위가 확정되면 양 공인전자문서센터는 이에 대한 협약서를 작성함.
- 이관 방식 및 이관 일정에 대한 협의
 - 이관데이터의 용량, 요구 일정, 이·수관 공인전자문서센터의 시스템 요건 등에 따라 이관을 위한 구체적 방안에 대한 협의
 - 이관데이터의 용량 및 처리기간 등을 주요 기준으로 오프라인 방식 또는 온라인 방식을 결정
 - 이·수관 방식에 대한 최종 결정은 이관데이터의 용량이나 처리기간 뿐만 아니라, 이·수관 공인전자문서센터가 합의한 일정 및 공인전자문서센터의 시스템 환경 등에 따라 양 공인전자문서센터가 최종 결정을 하도록 함
 - 이·수관 대상 정보 및 정보구조에 대한 합의 필요
 - 이관이 필요한 이용자 정보구조
 - 이용자 별 분류체계에 대한 수용 여부 및 수용 시 이관 방안
 - 전자문서에 대한 이용자 접근권한 수준에 대한 합의

- 이관대상 전자문서의 추가 확장속성정보 현황 및 수관 공인전자문서센터의 수용방안
- 이관 공인전자문서센터가 관리하고 있던 추가정보의 유형 및 이관 여부(예: 전자문서 간 연관관계 정보 등)에 대한 합의
- 이관 공인전자문서센터가 관리하지 않는 정보 중, 수관 공인전자문서센터가 관리를 위해 반드시 필요로 하는 부가 정보가 있을 경우, 이에 대한 획득 방안
- 이용자와 수관 공인전자문서센터 간 이용계약 체결 및 등록, 선택적 준비 작업임
 - 수관 공인전자문서센터는 이관되는 이용자에 대한 정보를 바탕으로 각 이용자 단위로 이용계약을 체결하고 등록한다.
- 이관 공인전자문서센터의 이용자 정보와 수관 공인전자문서센터의 이용자 정보 간 맵핑정보 준비
 - 수관 공인전자문서센터는 이관 공인전자문서센터의 이용자 A가 보유한 이관대상 전자문서를 수관 공인전자문서센터의 어느 이용자 정보에 이관을 할 것인지에 대해 맵핑한 정보를 준비한다.
- 공인전자문서센터 간에 관리방식이 상이(相異)한 데이터에 대하여 협의된 처리 방안에 따라 처리 모듈 준비

3.1.3 전자문서이관 절차

전자문서의 이·수관은 ① 이용자 요청에 의한 이관, ② 이관 공인전자문서센터 영업정지로 인한 이관 등이 있을 수 있는데, 각 이관 유형에 따라 이·수관 절차에 있어서 다소 차이가 있다.

① 이용자 요청에 의한 이관

사용자 요청에 의한 이관인 경우에는 사용자가 수관 공인전자문서센터를 지정하고 이관 공인전자문서센터에게 전자문서의 이관을 요청하는 경우이므로, 이용자가 이관을 요청하는 절차가 먼저 선행되어야 한다. 이용자의 이관요청을 받은 이관 공인전자문서센터는 대상이 되는 수관 공인전자문서센터와 이관대상 범위 및 방식, 일자에 대해서 합의를 한 후, 합의된 내용을 이용자에게 통보하여 이관에 대한 최종 확인을 한다.

이용자의 최종확인을 받은 후에 이관 공인전자문서센터와 수관 공인전자문서센터는 이관을 위한 실제 프로세스를 진행하도록 한다.

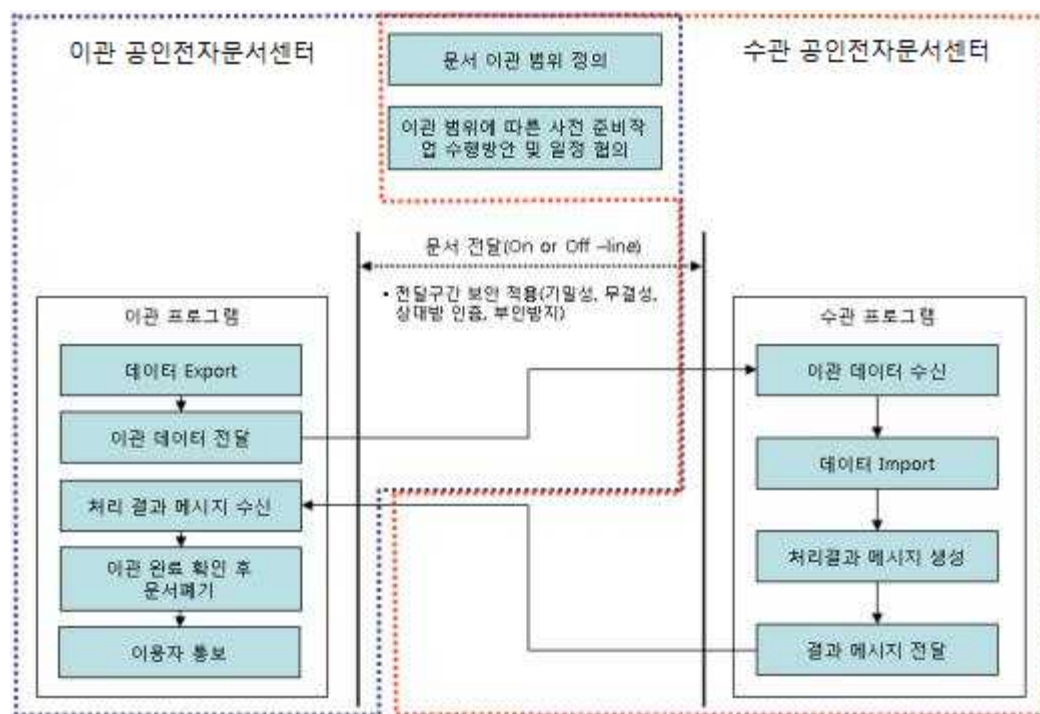
② 이관 공인전자문서센터 영업정지로 인한 이관

이관 공인전자문서센터의 영업정지로 인해 이용자의 의도와 관계없이 불가피하게

이관이 되어야 하는 경우에, 이관 공인전자문서센터는 이관대상 전자문서 및 범위를 파악한 후 이를 기초로 수관 공인전자문서센터와 만나서 전자문서 수관 여부를 협상하도록 한다. 기본적으로 이·수관에 대한 합의가 이루어지면, 이관 공인전자문서센터는 각 이용자에게 이관에 대한 진행상황을 통지한다. 이관 공인전자문서센터와 수관 공인전자문서센터는 이관범위 및 방식, 일자에 대해서 추가적인 협상을 한 후, 합의된 내용을 다시 이용자에게 통보하여 최종 확인을 받고, 이관을 위한 실제 프로세스를 진행하도록 한다.

이·수관에 대한 초기 기본적인 합의과정이 완료되면, 전자문서 이·수관을 위한 실제 처리 프로세스는 다음과 같이 진행이 된다.

3.1.3.1 전자문서이관절차 흐름도



(1) 전자문서 이관의 범위를 정의한다.

- 사전 준비 정보
 - 이관대상이 되는 이용자 정보 및 전자문서의 범위를 조사
 - 이·수관 공인전자문서센터 및 사용자와의 합의에 의해 이관 공인전자문서센터가 제공하던 부가서비스 정보에 대한 이관여부를 결정
- 이관대상 데이터
 - 전자문서 원본, 최초등록증명서

- 전자문서에 대한 속성정보(기본속성 및 확장속성)
 - 전자문서에 대한 보안(접근권한) 정보
 - 기타 부가정보(선택사항)
 - 연관관계 정보: 전자문서와 분류체계간 연관정보, 전자문서 및 속성정보와 연관정보, 전자문서 및 증명서 자료와의 연관정보
 - 부가 서비스 정보: 공인전자문서센터 특성에 따라 이용자에게 제공하던 부가 서비스 정보들
- (2) 이·수관 공인전자문서센터는 이관일정 및 방식을 합의하고 사전정보 이·수관 또는 등록에 대한 준비작업을 수행한다.
- 앞서 합의된 이관범위에 따라 양 공인전자문서센터는 이관 처리일정 및 방식을 논의하고 이에 대해 합의를 함
 - 수관 공인전자문서센터는 이관대상 이용자와 전자문서의 이관 이전에 미리 수관 공인전자문서센터와 이용계약 체결하도록 함
 - 이관 공인전자문서센터로부터 수관 공인전자문서센터에 이용자 정보를 이관 또는 등록
 - 이관 공인전자문서센터의 이용자 정보와 수관 공인전자문서센터의 이용자 정보 간에는 미리 전자문서 이·수관을 위한 맵핑정보를 정의하여야 함
 - 수관 공인전자문서센터에 이용자 단위의 분류체계 정보를 등록(수관 공인전자문서센터의 기존 분류체계에 재 분류하고자 하는 경우에는 이 과정이 생략될 수 있음)
 - 수관 공인전자문서센터는 이관 공인전자문서센터의 이용자의 분류체계와 수관 공인전자문서센터에서 수관이용자가 사용할 수 있는 분류체계 간에 이용자 단위로 맵핑정보를 정의하여야 함
 - 이·수관 공인전자문서센터 간 합의된 이관정보범위 및 방식에 따라 기존에 보유한 이·수관 모듈을 커스터마이징 함
- (3) 전자문서이관 정보 export
- 이관대상 전자문서를 정의하고 이를 검색한다.
 - 이관대상 전자문서, 증명서 및 관리정보 등을 본 규격의 “3.2 이·수관 정보 구조”에서 명시한 포맷에 맞게 export 함
 - 고객 요청에 의하여 암호화하여 보관 중인 전자문서는 반드시 복호화 작업을 수행하여야 함
 - 이관 시점에 최초등록증명서의 전자서명이 만료되었다면, 이관 공인전자문서센터는 반드시 유효한 인증서를 사용하여 최초등록증명서를 갱신하여야

함

(4) 이관데이터 전달

- export한 이관요청메시지를 온라인 또는 오프라인의 방법을 통해 보안이 적용되는 방식으로 수관 공인전자문서센터에 전달함

(5) 전자문서 정보 Import

- 수관 공인전자문서센터는 이관 공인전자문서센터로부터 이관요청메시지를 받아서 이를 해석한 후 수관 공인전자문서센터 구조에 맞게 등록하고 등록증적을 생성
- 고객 요청에 의하여 암호화할 필요가 있는 전자문서는 암호화 작업을 수행하여 등록
- 수관 공인전자문서센터는 수관받은 최초등록증명서의 증명대상 정보를 유지하여 재발급 (최초등록증명서 재발급에 대한 상세 설명은 증명서 규격의 "부록 4. 전자문서 수관 시의 최초등록증명서 재발급" 절을 참조)

(6) 전자문서폐기

- 이관과정에서 오류가 발생된 전자문서에 대해서는 원인을 파악한 후 문제점을 수정, 보완하여 (3) ~ (6) 과정을 다시 수행함
- 전자문서에 대한 이관이 완료된 후 이관 공인전자문서센터는 이관전자문서가 정확히 이관되었는지를 확인하고 이관증적을 생성한 후 대상 전자문서를 폐기함

(7) 이용자 통보

- 폐기작업까지 이관 프로세스가 완료되면 이관 공인전자문서센터는 이용자에게 이관사실을 통보
- 이관 공인전자문서센터는 이용자 요청시 이용자에게 이관증명서를 발급함
- 수관 공인전자문서센터는 이용자 요청시 이용자에게 등록증명서를 발급함
- 수관 공인전자문서센터는 이용자에게 최초등록증명서 다운로드 서비스 제공

3.1.4 이·수관 방안

이관 공인전자문서센터와 수관 공인전자문서센터는 전자문서의 양과 처리기간 등을 고려하여 양 공인전자문서센터 간 협의에 의해 오프라인 또는 온라인 처리 여부를 결정한다.

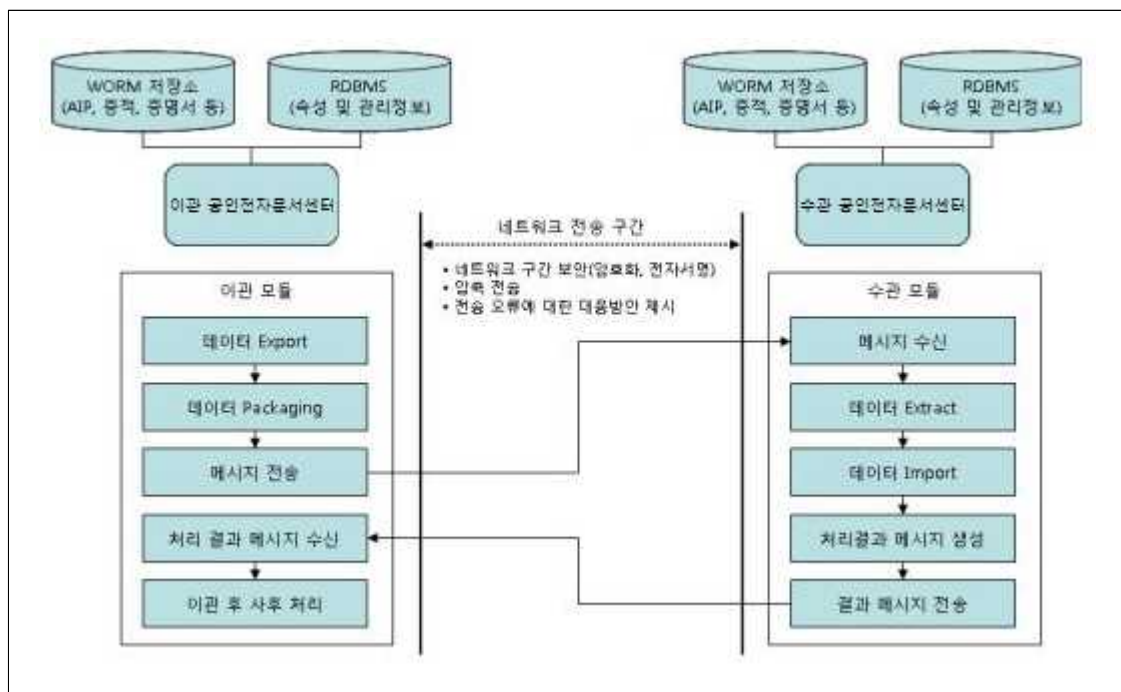
3.1.4.1 온라인/오프라인 이·수관 방안

온라인과 오프라인의 이·수관은 데이터를 전달하는 방식 및 이를 위한 이·수관 메시지 구조에 있어서 약간의 차이가 있을 뿐 전체적인 처리 흐름은 거의 동일하다.

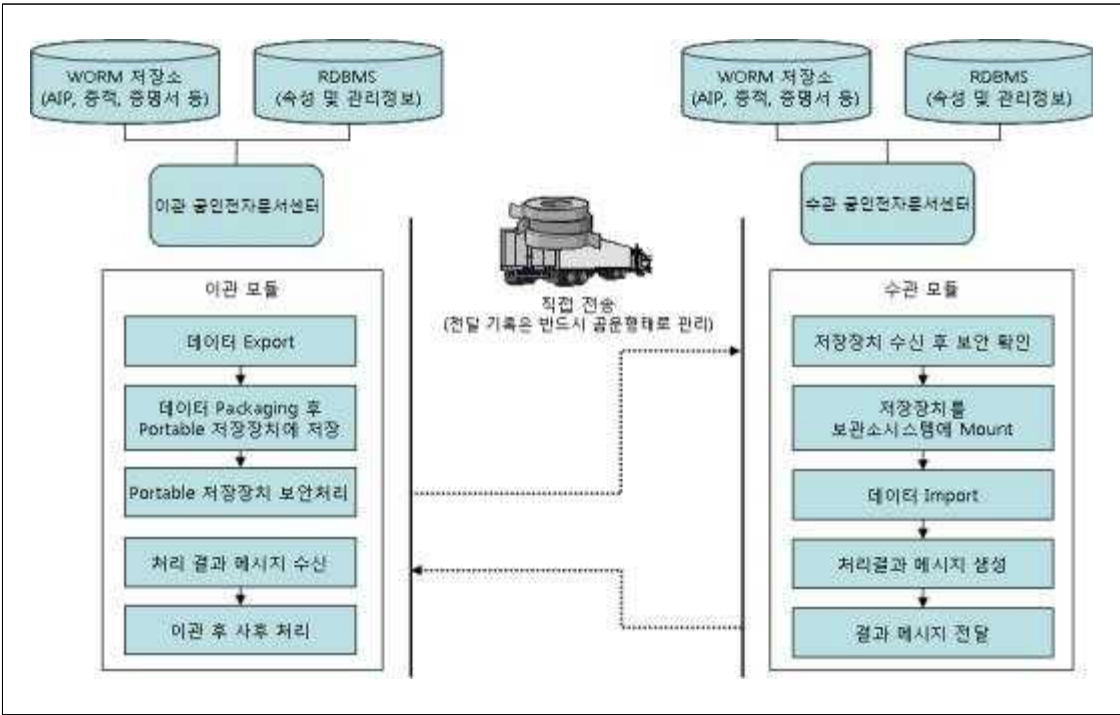
전달되는 메시지 구조에 있어서, 온라인 방식은 이관대상이 되는 복수의 TIP를 SOAP Attachment 규약에 따라 하나의 메시지 내에 embedding을 하는 구조를 택한 반면에 오프라인 방식인 경우에는 Portable 저장장치에 TIP를 독립적으로 저장하고 Request Message에서 이에 대한 위치정보를 보유하는 referencing 구조를 택하고 있다. (자세한 정보구조는 “3.2 이·수관 정보구조” 참조)

이러한 메시지 구조 외에 가장 큰 차이점은 export 한 데이터를 전달하는 방식의 차이로 할 수 있다. 오프라인 방식의 이관은 Portable 저장장치에 이관하고자 하는 이관 메시지를 저장하여 입출력 장치가 봉인된 상태에서 차량 등의 방법을 통해 직접 전달하게 되고, 온라인 방식은 SOAP 통신을 이용하여 이·수관 공인전자문서센터 시스템 간 직접연계를 하여 전달하게 된다.

(1) 온라인 이·수관 프로세스 흐름도



(2) 오프라인 이·수관 프로세스 흐름도



3.2 이·수관 정보구조

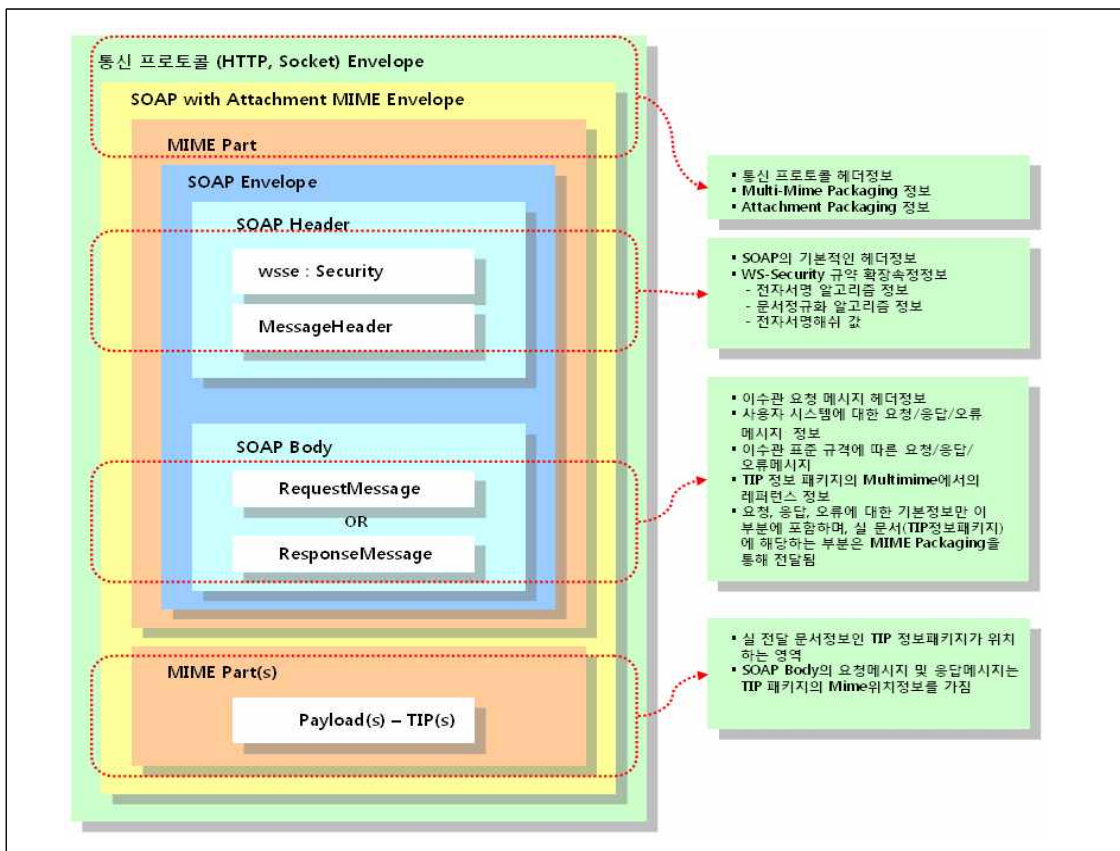
3.2.1 개요

공인전자문서센터 간 전자문서의 이·수관을 위해 사용하는 메시지는 요청메시지(RequestMessage)와 응답메시지(ResponseMessage)의 두 가지 유형으로 구성된다. 각각의 메시지는 이·수관 시스템이 해석하여 처리할 수 있도록 하기 위해서, 이관 공인전자문서센터는 본 규격에서 정의하는 요청 표준에 따라 요청메시지를 생성하여 수관 공인전자문서센터에 보내야 하며, 수관 공인전자문서센터는 본 규격에서 정의하는 응답 표준에 따라 응답메시지를 생성하여 이관 공인전자문서센터에 전달해야 한다.

3.2.2 메시지 패키징

전자문서의 이·수관 유형에는 온라인/오프라인 방법이 있다. 메시지 패키징은 이·수관 유형에 따라 패키징 방법에 약간의 차이가 있다.

3.2.2.1 온라인 메시지 패키징



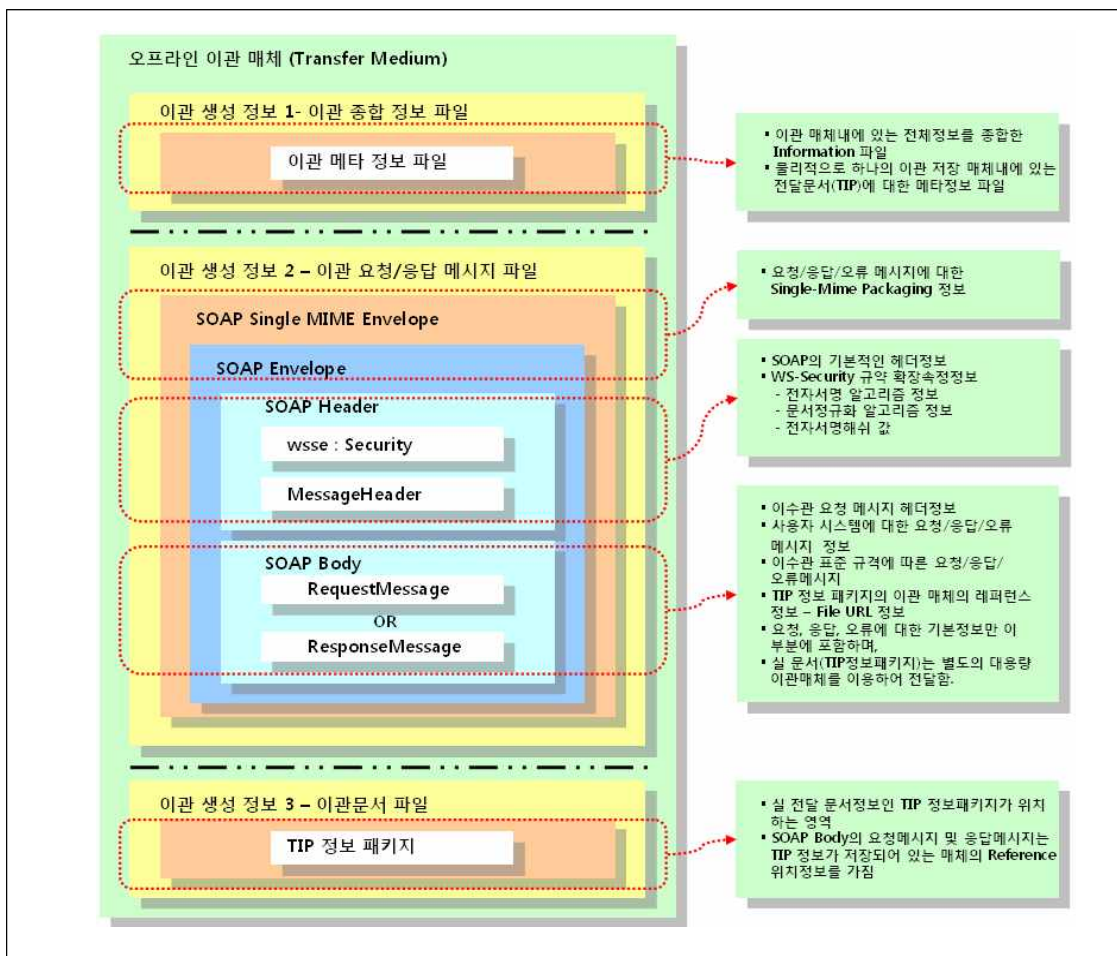
온라인 이·수관 방법은 이관 공인전자문서센터에서 이관대상이 되는 전자문서를

이·수관 규격에 따라서 요청메시지를 생성한 후 통신 프로토콜(http, socket)을 이용하여 온라인 상에서 자동으로 전자문서를 전달하고, 수관 공인전자문서센터는 요청메시지를 처리한 후 응답메시지를 같은 방법으로 생성하여 이관 공인전자문서센터로 전달하는 유형이다.

온라인 이·수관 메시지 패키지 구성은 헤더정보 및 바디정보를 SOAP Envelope를 이용하여 패키징을 한 후, 첨부문서인 TIP를 SOAP Attachment 방식으로 패키징하고, 최종적으로 전체 메시지 정보를 온라인 전송프로토콜 패키징 방식을 사용한다. 즉 각종 헤더정보, 메타정보 및 TIP정보가 하나의 메시지에 포함되는 패키지로 구성되어 송수신하는 방식이다.

3.2.2.2 오프라인 메시지 패키징

오프라인 이·수관 방법은 이관 매체 (Storage, DVD/CD 등)에 이관정보를 담아서 송수신하는 방법이다. 이관 공인전자문서센터는 3가지 이관 전자문서정보인 ①이관 종합정보 파일, ②이관 요청메시지, ③이관문서 파일을 생성하고, 이렇게 생성된 메시지를 이관 매체에 담아서 수관 공인전자문서센터에 전달한다. 수관 공인전자문서센터는 오프라인으로 전달된 이관 매체에 저장된 이관정보로부터 전자문서를 추출하여 공



인전자문서센터 저장소에 등록한다.

3.2.2.3 SOAP 패키징

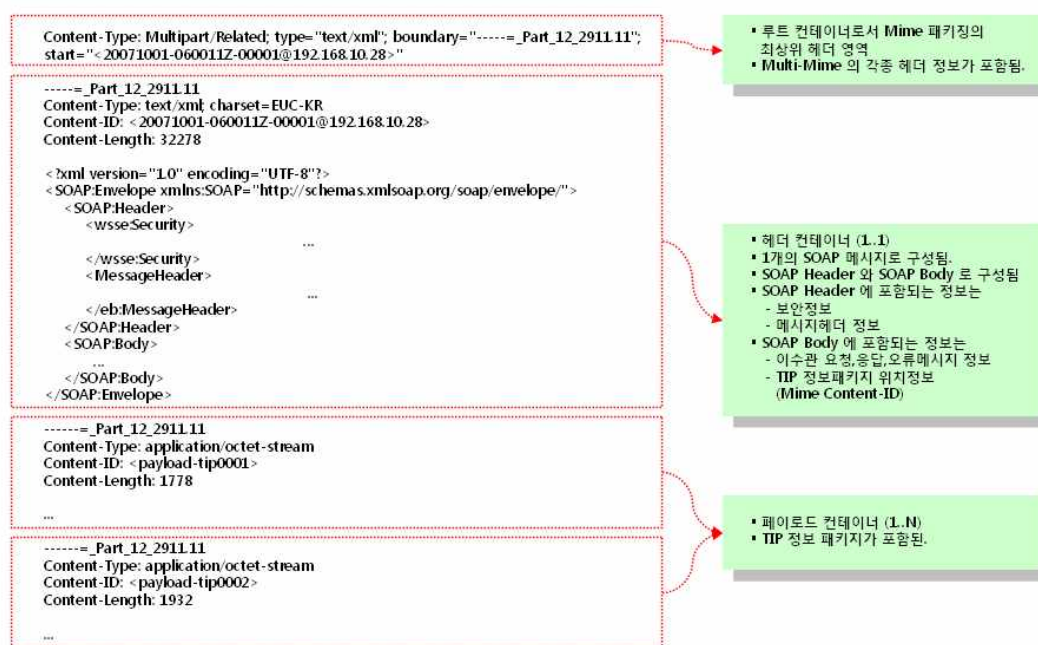
이·수관 요청 및 응답메시지는 기본적으로 SOAP 패키징으로 Enveloping된 후, 메시지의 전달 방식이 온라인 혹은 오프라인 인지에 따라 SOAP으로 패키징 된 정보의 MIME 유형을 Multi-MIME (온라인) 혹은 Single-MIME (오프라인) 을 사용한다.

이·수관 메시지의 패키징은 다음의 명세를 따른다.

- Simple Object Access Protocol (SOAP) 1.1 [SOAP]
- SOAP Messages with Attachments [SOAPAttach]

3.2.2.3.1 SOAP with Multi-MIME

온라인 이·수관 메시지를 패키징하는 방법으로서, 메시지 내의 Content-Type MIME 헤더는 반드시 SOAP 메시지를 포함하는 MIME 본체 부분의 MIME 미디어 유형과 동일한 타입 속성을 가지고 있어야 한다. [SOAP] 명세에 따르면 SOAP 메시지의 MIME 미디어 유형은 "Multipart/Related" "text/xml" 값을 가져야 한다.



메시지 패키지의 최상위 부분을 루트 컨테이너라 하는데, Content-Type MIME 헤더를 가진다. 루트 컨테이너의 Content-Type MIME 헤더에는 "Multipart/Related" 및 boundary, start는 항상 존재한다.

메시지의 본체 부분을 헤더 컨테이너라고 한다. 헤더 컨테이너의 Mime 헤더 영역

에는 Content-Type 과 Content-Length 가 필수적으로 포함된다. MIME Content-Type 헤더는 SOAP 명세에 준하여 "text/xml" 값을 가져야 한다. Content-Type 헤더는 "charset" 속성을 포함할 수도 있다. Mime Content-Length 헤더는 헤더 컨테이너 내에 포함되는 SOAP Envelope 메시지의 바이트단위의 크기 정보를 가진다.

헤더 컨테이너는 MIME의 본체 부분으로 하나의 SOAP 메시지가 포함된다.

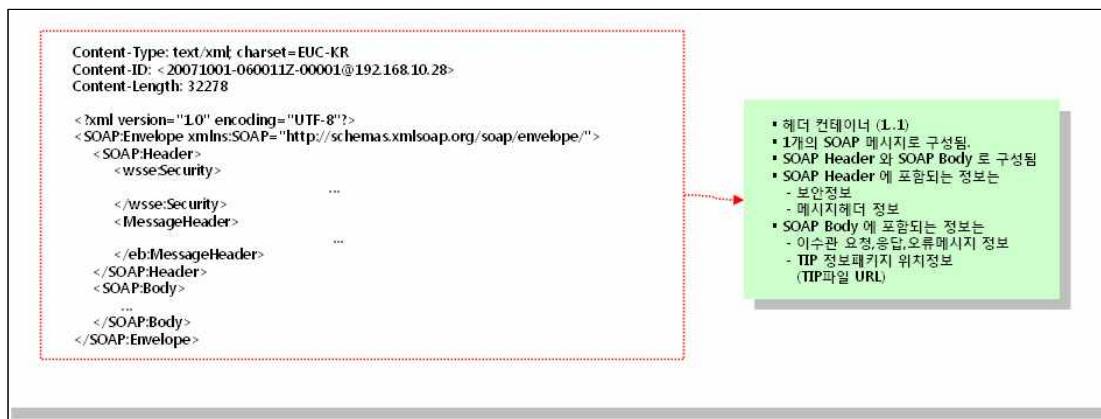
SOAP 메시지는 SOAP Header 와 SOAP Body 로 구분된다. SOAP Header 영역에는 이·수관 메시지에 대한 보안헤더(Security Header)와 메시지헤더(Message Header)가 포함되고, SOAP Body 영역에는 요청메시지(RequestMessage)와 응답메시지(ResponseMessage)가 포함된다.

메시지의 첨부 부분을 페이로드 컨테이너라고 한다. 페이로드 컨테이너는 [SOAPAttach] 명세에 따라 패키징되며, 이·수관 메시지 내에는 반드시 1개 이상의 페이로드가 포함된다. 페이로드 컨테이너에는 TIP가 포함된다. 각 페이로드 컨테이너의 TIP는 SOAP Body내의 TIPInfo에 의해 참조되어야 한다. 참고로 TIPInfo는 페이로드 컨테이너의 Content-ID 정보를 가진다.

페이로드 컨테이너의 Mime 헤더 영역에는 Content-Type 과 Content-Length 가 필수적으로 포함된다. MIME Content-Type 헤더는 SOAP 명세에 준하여 페이로드의 문서유형(Media Types : RFC 2046 에 정의된 Media Type)에 따른 값을(ex. "text/xml", "application/octet-stream" ...) 가져야 한다. Content-Type 헤더는 "charset" 속성을 포함할 수도 있다. Mime Content-Length 헤더는 페이로드 컨테이너안에 포함되는 TIP의 바이트단위의 크기 정보를 가진다.

3.2.2.3.2 SOAP with Single-MIME

오프라인 이·수관 메시지를 패키징하는 방법으로서, 온라인 메시지의 패키징 방법에서 루트 컨테이너와 페이로드 컨테이너 영역이 생략된다. 따라서 메시지 패키지는 non-multipart 형태로 패키징 된다.



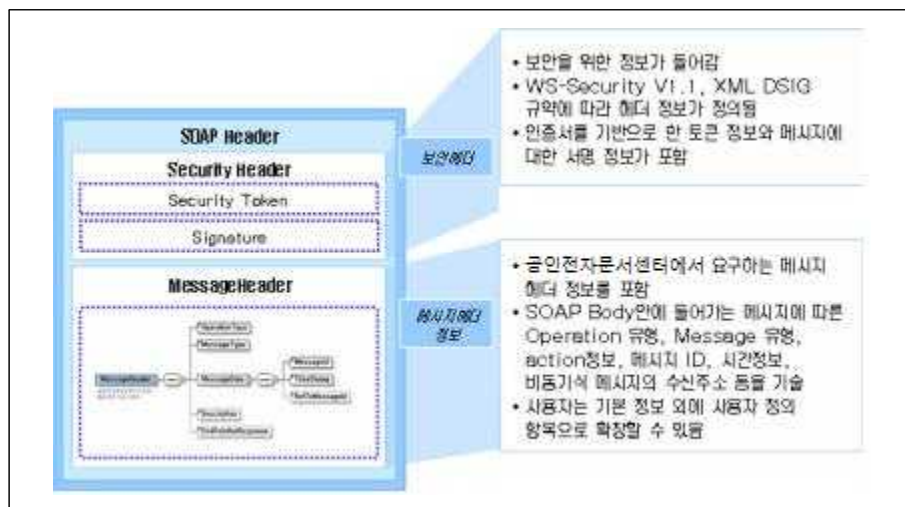
오프라인 메시지는 1개의 헤더 컨테이너 구성되며, 헤더 컨테이너의 Content-Type MIME 은 "text/xml" 미디어 타입을 유형을 가지고, charset 속성을 가진다. 단, 온라인 패키지 요구되는 파라미터들인 start 파라미터, boundary는 존재하지 않는다.

헤더 컨테이너는 MIME의 본체 부분으로 하나의 SOAP 메시지가 포함된다. 포함되는 정보는 온라인에서와 같다.

오프라인 방식에서 이·수관 전달물인 TIP는 이·수관 메시지에 포함되지 않고 별도의 이관 매체에 저장된다. 이렇게 별도의 이관 매체에 저장된 TIP는 SOAP Body내의 TIPInfo 요소에 의해 그 위치정보가 참조된다.

3.2.2.3.3 SOAP Header

SOAP 헤더는 WS-Security V1.1 규약에서 정의하는 <Security>항목과 추가적으로 정의된 <MessageHeader>항목으로 구성된다. 전체 구조는 다음과 같다.



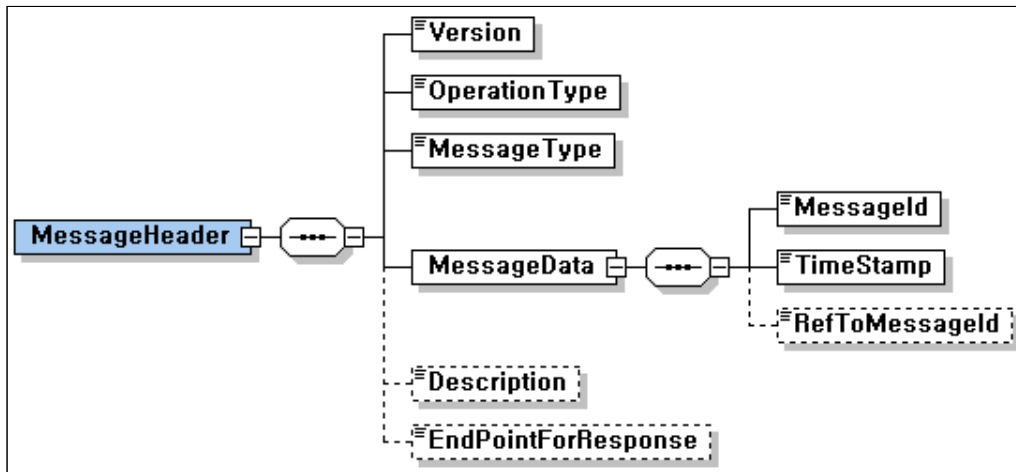
(1) Security 구조

Security항목에 대한 상세 설명은 “이용자시스템과 공인전자문서센터간 연계 인터페이스 기술규격 v2.10”(이하 연계 인터페이스 규격)의 “4.2.5 전송보안” 절을 참조함.

(2) MessageHeader 구조

MessageHeader에는 작업 종류, 요청 · 응답 · 오류 구분, 메시지 식별자, 타임스탬프 등의 요청메시지에 대한 일반적인 정보를 나타내는 필드들이 포함된다. MessageHeader의 구조는 요청메시지(RequestMessage)와 응답메시지(ResponseMessage)에서 동일하게 적용된다.

○ 스키마 구조



○ 메시지 구조

| 메시지 필드명 | | | Type(크기) |
|-------------------------|-------------------------------|--------------------------|-------------------------|
| MessageHeader (1..1) | Version (1..1) | | string (3bytes) |
| | OperationType (1..1) | | char (1byte) |
| | MessageType (1..1) | | char (1byte) |
| | MessageData (1..1) | MessageId (1..1) | string (36bytes) |
| | | TimeStamp (1..1) | string (15bytes) |
| | | RefToMessageId (0..1) | string (36bytes) |
| | Descrtiption (0..1) | | string (500bytes 이내) |
| | EndPointforResponse (0..1) | | string (300bytes 이내) |

○ 필드 설명

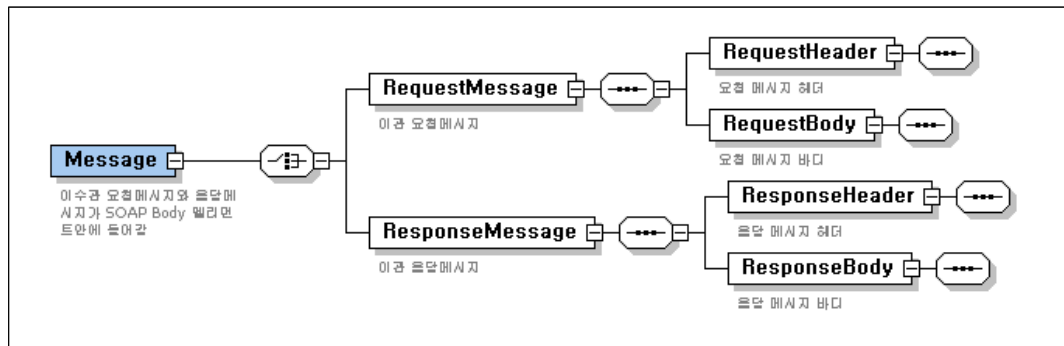
| 필드 명 | 설명 | 생성규칙 | 예 |
|---------|--------------------|--|-------|
| Version | 이 · 수관 메시지 스키마의 버전 | 본 규격을 준용한 이 · 수관 메시지 스키마의 버전은 “1.0”으로 설정 | “1.0” |

| | | | |
|---------------------|---|---|--|
| OperationType | 요청 유형에 대한 구분 값 | 전자문서이수관(t) | 't' |
| MessageType | 전송하는 메시지에 따른 구분 값 | request(1) response(2) | '1' |
| MessageId | message의 ID | 요청 : "req_" + 16bytes random number를 16진수 string으로 변환한 값, 응답 : "res_" + 요청 메시지에 첨부된, 16 진수 string 값으로 변환된 16bytes random number | "req_0aa2c56e 3bce534aefc3b23dec 42fae3" |
| TimeStamp | 메시지가 전송된 GMT 시각 | "yyyymmddhhmiss" +"Z" | "20060918160955Z" |
| RefToMessageId | 응답메시지인 경우 이전 메시지에 대한 ID 값 | | "req_0aa2c56e 3bce534aefc3b23dec 42fae3" |
| Description | 메시지에 대한 부연설명 | | |
| EndPointforResponse | 비 동기식인 경우 응답메시지를 받을 수 있는 IP주소 및 포트 또는 E-mail 등. 송신자와 수신자 간 비동기 전송을 위한 프로토콜의 협의가 필요함 | Null 값을 보내는 경우에는 별도의 응답메시지를 보내지 않고 클라이언트 어플리케이션에서 확인함 | "admin@kisa.kr" "127.0.0.1:9999" |

3.2.2.3.4 SOAP Body

SOAP Body는 이·수관 요청 및 응답메시지를 담을 수 있는 요청메시지(RequestMessage) 또는 응답메시지(ResponseMessage) 항목 중 하나로 구성된다.

○ 스키마 구조



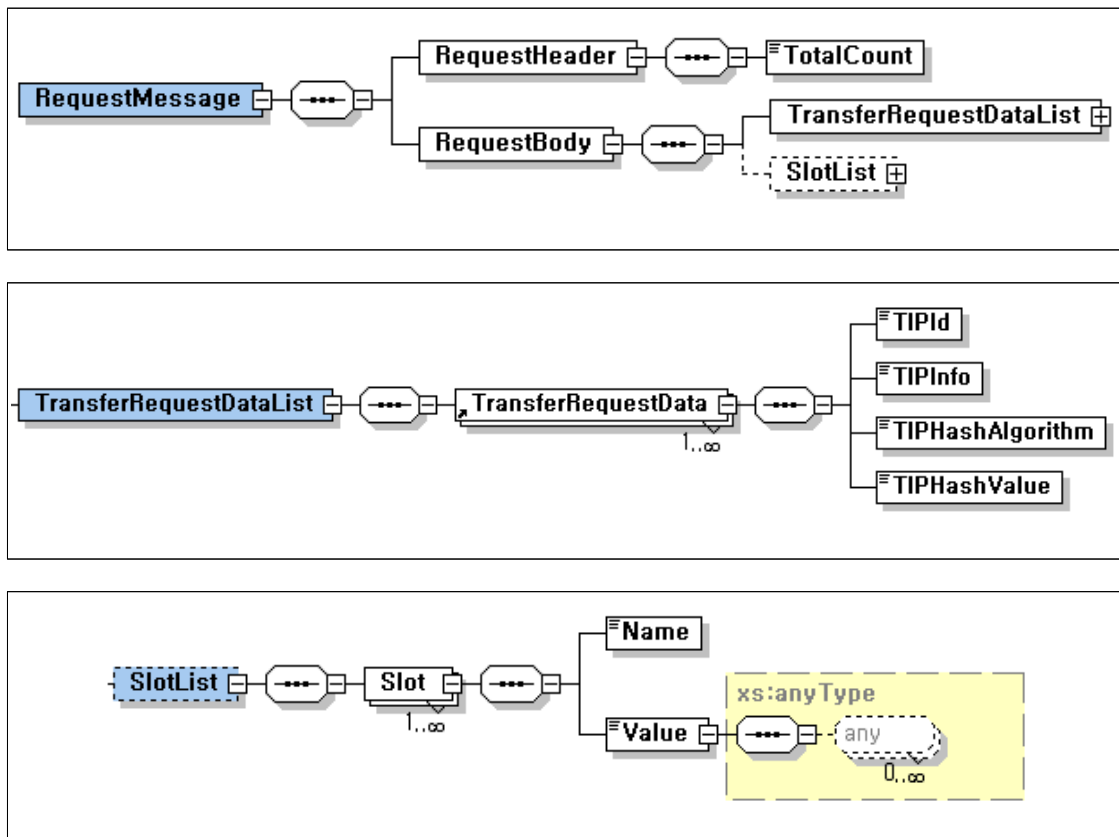
3.2.3 이 · 수관 요청메시지

3.2.3.1 기본 정보

공인전자문서센터에 보관 중인 전자문서를 타 공인전자문서센터에 이관 요청할 때 사용하는 요청메시지를 정의한다.

RequestMessage 항목은 처리 요청 건수를 포함하는 RequestHeader와 실제 이관 요청의 내용물인 TIP의 메타정보가 포함된 RequestBody로 이루어져 있다. 동일 작업에 대하여 복수개의 요청 데이터 처리가 가능하도록 RequestBody는 요청정보가 반복적으로 추가될 수 있는 구조를 지닌 TransferRequestDataList를 포함하며, TransferRequestDataList의 구조는 이 · 수관 요청 서비스에 필요한 정보를 담을 수 있는 TransferRequestData 항목으로 정의 된다.

3.2.3.2 스키마 구조



3.2.3.3 메시지 구조

| 메시지 필드명 | Type(크기) |
|---------|----------|
|---------|----------|

| | | | | | |
|---------------------------|--------------------------|---------------------------------------|-----------------------------------|----------------------------|-------------------------|
| Request Message (1..1) | Request Header (1..1) | TotalCount (1..1) | | | long (4bytes) |
| | Request Body (1..1) | TransferRequest DataList (1..1) | TransferRequest Data (1..∞) | TIPId (1..1) | string (128bytes 이내) |
| | | | | TIPInfo (1..1) | string (256bytes 이내) |
| | | | | TIPHashAlgorithm (1..1) | string (10bytes 이내) |
| | | | | TIPHashValue (1..1) | string (100bytes 이내) |
| | | SlotList (0..1) | Slot (1..∞) | | structure |

3.2.3.4 필드 설명

| 필드 명 | 설명 | 생성규칙 | 예 |
|------------------|--|--|---|
| TotalCount | TransferRequestDataList 하 위 의 TransferRequestData의 수 | | "10" |
| TIPId | TIP정보패키지의 패키지 메타데이터에 있는 패키지 식별자 값 | | "000000001" |
| TIPInfo | 전달메시지 내에서 첨부 된 TIP정보패키지의 위치 정보를 기술 | 온라인 패키징 : 페이로드 컨테이너의 Mime Content-ID 오프라인 패키징 : TIP정 보패키지가 저장되어 있는 매체의 위치정보 | "<payload- tip0001>" "/payload /tip/1210/ T10001.tip" |
| TIPHashAlgorithm | 첨부된 TIP 정보패키지 파일의무결성을 확인하기 위하여사용한 Hash 알고 리즘 | "sha1", "sha256" | |

| | | | |
|--------------|---------------------|---|--------------------------------|
| TIPHashValue | 첨부된 TIP 파일을 Hash한 값 | 첨부된 TIP를 Hash한 값으로서, string변환시 base64encoding적용 | "cFuOuMnGkK0SsS4cCUoxMcIpwNU=" |
|--------------|---------------------|---|--------------------------------|

3.2.3.5 Slot 구조

| 메시지 필드명 | | | Type (크기) | 비고 |
|--------------------|----------------|-----------------|--------------------|--|
| SlotList (0..1) | Slot (1..∞) | Name (1..1) | string (50bytes이내) | Slot을 식별하기 위한 Slot의 이름으로서, 사용하기 위해서 정의되어 있어야 함 |
| | | Value (1..1) | defined by Name | 정의된 형식을 따름 |

3.2.4 이 · 수관 응답메시지

3.2.4.1 기본 정보

MessageHeader의 구조는 요청메시지와 동일하다.

응답메시지는 전체 처리 결과, 전체 처리 건수, 성공한 처리 건수, 실패한 처리 건수 정보를 포함하는 응답메시지헤더(ResponseHeader)와 실제 응답의 내용이 포함된 응답메시지바디(ResponseBody)로 이루어져 있다.

공인전자문서센터가 전자문서를 타 공인전자문서센터에 이관하는 작업은 요청 및 응답 작업 시점과 비동기적으로 이루어지므로, 전자문서 이관 요청에 대한 응답메시지에는 해당 전자문서에 대한 이관 가능 여부의 확인 결과가 포함된다.

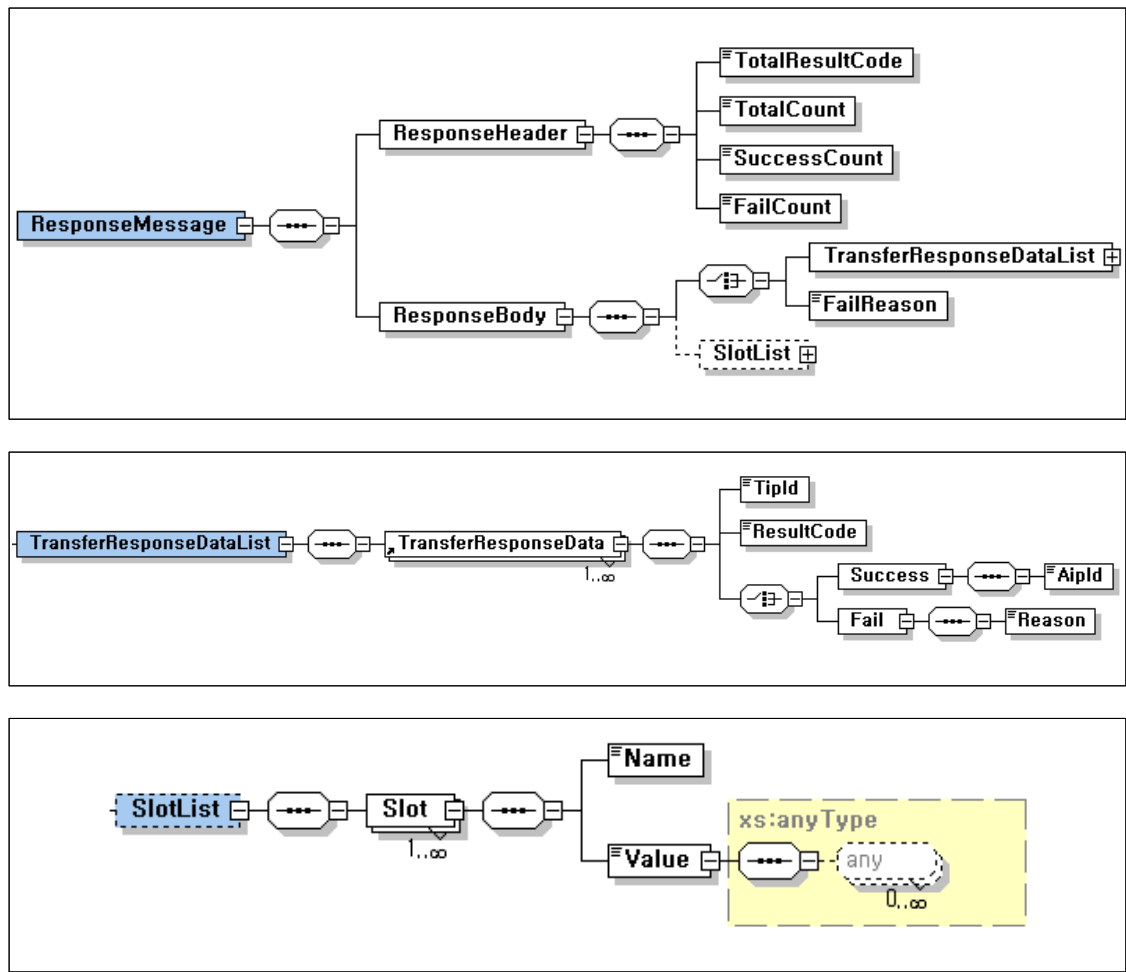
응답메시지바디(ResponseBody)는 전체 처리 결과인 TotalResultCode의 값에 따라 ResponseDataList나 FailReason으로 대체되는 ResponseResult를 포함한다. 이때 복수의 요청 건수에 대한 처리 결과가 부분 성공일 경우나 전체 실패일 경우라도, 전체 처리 결과를 성공으로 처리할지 실패로 처리할지에 대한 결정은 공인전자문서센터의 정책을 따른다. 예를 들어, 공인전자문서센터는 복수의 요청에 대한 처리 결과가 모두 실패이나, 각 요청에 대한 개별적인 실패 사유를 이용자에게 전달하기 위하여 전체 처리 결과를 성공으로 설정할 수 있다.

전체 처리 결과가 성공인 경우, 요청메시지와 마찬가지로 복수개의 요청에 대한 응답이 가능하도록 TransferResponseDataList는 복수개의 TransferResponseData를 포함할 수 있는 구조로 되어 있으며, TransferResponseData의 구조는 연계 유형별 응답메시지 구조에서 각 서비스 유형에 따른 이름과 구조로 재정의 된다.

전체 처리 결과가 실패인 경우, 실패 사유인 FailReason이 ResponseResult를 대신하게 된다.

ResponseBody에서도 RequestBody와 마찬가지로, 확장 필드를 의미하는 Slot이 반복적으로 추가될 수 있는 구조를 지닌 SlotList를 ResponseResult의 다음에 포함할 수 있다.

3.2.4.2 스키마 구조



3.2.4.3 메시지구조

| 메시지 필드명 | | | | | | Type(크기) |
|----------------------------|---------------------------|---------------------------|------------------------------|---------------------------|------------------|-----------------------------|
| Response Message (1..1) | Response Header (1..1) | TotalResultCode (1..1) | | | | char (1byte) |
| | | TotalCount (1..1) | | | | long (4bytes) |
| | | SuccessCount (1..1) | | | | long (4bytes) |
| | | FailCount (1..1) | | | | long (4bytes) |
| | Response Body (1..1) | Response Result (1..1) | Transfer Respons eDataLis | Transfer Response Data | TIPIId (1..1) | string (128bytes 이 내) |

| | | | | | | | | |
|--|--|--------------------|----------------|--------|-------------------------|----------------------|------------------|-----------------------------|
| | | | t (choice1) | (1..∞) | ResultCode (1..1) | | | char (1byte) |
| | | | | | Result (1..1) | Success (choice3) | AipId (1..1) | string (128bytes 이 내) |
| | | | | | | Fail (choice4) | Reason (1..1) | string (500bytes 이 내) |
| | | | | | FailReason (choice2) | | | string (600bytes 이 내) |
| | | SlotList (0..1) | | | Slot (1..∞) | | | structure |

3.2.4.4 필드 설명

| 필드 명 | 설명 | 생성규칙 | 예 |
|-----------------|--|--|---------------------------|
| TotalResultCode | 요청메시지의 이 · 수 관 전체 처리결과에 종합 코드값 | 요청메시지의 수신 결과에 따라 성공('1'), 실패('2') 여부를 기록 | '1', '2' |
| TotalCount | ResponseDataList 하 위 의 TransferDocumentRes ponseData의 수 | | |
| SuccessCount | 처리 성공한 ResponseData의 수 | TotalResultCode의 값이실패 인 경우 0 | 3000 |
| FailCount | 처리 실패한 ResponseData의 수 | TotalResultCode의 값이실패 인 경우 0 | 212 |
| TIPId | TIP정보패키지의 패키 지메타데이터에 있는 패키지 식별자 값 | | "00000000 1" |
| ResultCode | 요청메시지의 이 · 수 관 처리결과에 코드값 | 요청메시지의 수신 결과에 따라 성공('1'), 실패('2') 여부를 기록 | '1', '2' |
| AipId | 요청메시지의 처리 결 과가 성공인 경우 수 | AIP에서 제공하는 패키지 ID를 기술함 | "100.000.0 000.1100.5" |

| | | | |
|-------------------------|-------------------------------------|---|--|
| | 관 공인전자문서센터 의 AIP 패키지 ID | | 943854a-ce 3b-4b68-99 55-cbacfd1 5555f" |
| Reason | 요청메시지의 처리 결 과가 실패인 경우 부 연설명 값 | 요청메시지의 수신 결과가 실패인 경우 발생한 오류 에 대한 부연설명을 기술 함. | |
| FailReason (choice2) | string (500bytes 이내) | 전체 작업에 대한 처리 실 패 사유 | 공 인 전 자 문 서 센 터 시 스템 의 오류 메시 지 형식을 따름 |

3.2.4.5 Slot 구조

| 메시지 필드명 | | | Type (크기) | 비고 |
|--------------------|----------------|-----------------|-------------------------|--|
| SlotList (0..1) | Slot (1..∞) | Name (1..1) | string (50bytes 이 내) | Slot을 식별하기 위한 Slot의 이름으로서, 사용하기 위해서 정의되어 있어야 함 |
| | | Value (1..1) | defined by Name | 정의된 형식을 따름 |

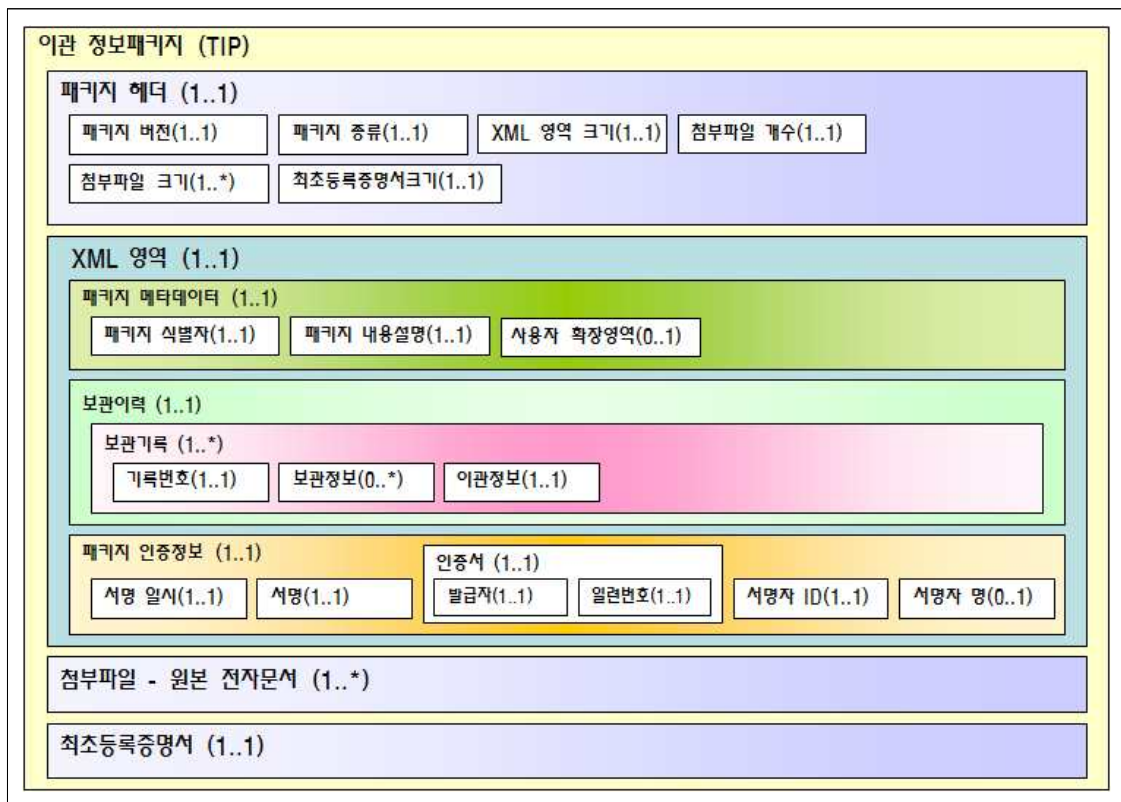
3.2.5 이관 정보 패키지

이·수관을 위한 전자문서 정보패키지는 전자문서의 내용과 전자문서에 대한 메타데이터, 즉 이·수관되는 정보의 신뢰성, 무결성, 가용성을 만족시키기 위해 필요한 전자문서의 생산, 등록, 이력, 내용 등에 관한 정보와 이를 이관 공인전자문서센터 시스템 내에서 수관 공인전자문서센터 시스템으로의 안전하고 지속적인 보존 및 활용 관리를 위한 정보로 구성된다.

3.2.5.1 이·수관 정보 기본구조

TIP는 전자문서를 이관하는 공인전자문서센터에서 생성하여 수관하는 공인전자문서센터로 전달되는 전자문서의 개념 모형을 말한다. 이·수관 정보의 기본구조는 헤더 정보(1..1), XML 영역(1..1), 첨부파일(1..*), 최초등록증명서(1..1)로 구성된다.

3.2.5.1.1 패키지 개념도



3.2.5.1.2 패키지 헤더 정보

패키지 헤더 정보는 정보패키지의 전체 구조를 어플리케이션에게 지시하는 정보로서 아래와 같은 정보로 구성된다.

| 번호 | 메타 데이터 명 | 유 형 | 크기 | 비고 |
|----|----------|-----|----|----|
|----|----------|-----|----|----|

| | | | | |
|---|------------|--------|--------|--------------------------------|
| 1 | 패키지 버전 | string | 3bytes | "3.0" |
| 2 | 패키지 종류 | string | 3bytes | "TIP" |
| 3 | XML 영역 크기 | Long | 4bytes | |
| 4 | 첨부파일 개수 | Short | 2bytes | |
| 5 | 첨부파일 크기 | Double | 8bytes | 배열의 형태를 가지며, 크기는 첨부파일의 개수로 결정함 |
| 6 | 최초등록증명서 크기 | Long | 4bytes | |

패키지 헤더 정보는 XML 형식으로 기재되지 않고, 각 메타 데이터의 정의된 형식으로 단순 연결하여 기술된다.

위의 메타데이터를 간단히 설명하면,

- ☐ 패키지 버전은 정보패키지의 버전을 기술하는 것으로, 본 규격 버전에서의 패키지 버전은 3.0으로 설정하고, 소숫점 한자리까지만 사용하는 것으로 한다. (예 : "3.0")
- ☐ 패키지 종류는 "TIP"를 설정한다.
- ☐ XML 영역 크기는 TIP에 대한 메타데이터를 포함하고 있는 XML 영역의 크기를 할당한다.
- ☐ 첨부파일 개수는 이 · 수관 정보패키지에 삽입되어 있는 첨부파일의 전체 개수로서 TIP에 첨부되는 전자문서의 총 개수를 할당한다.
- ☐ 첨부파일 크기는 개별 첨부파일의 크기를 할당한 것으로 배열 형태로 규정하며, 첨부파일의 개수로 크기를 결정하여야 한다. 즉, 첨부파일의 갯수가 10개인 경우 첨부파일의 크기는 10개의 인자를 가진다.
- ☐ 최초등록증명서 크기는 TIP에 포함된 원본문서에 대하여 이관 공인전자문서센터가 발급했던 최초등록증명서의 크기를 할당한다.

3.2.5.1.3 TIP 메타데이터 목록

하기의 표는 본 규격에서 정의하는 TIP의 모든 메타데이터 목록을 나열할 것이다.

| 번호 | 메타데이터 구성요소 | 반복 수 | 비고 |
|--------------------------|------------|------|----|
| 헤더정보 (HeaderInformation) | | 1..1 | |

| | | | | |
|----------------------------|-----------------------------------|-------------------------------|-------|------|
| 1 | 패키지버전 (Version) | | 1..1 | |
| 2 | 패키지종류 (Type) | | 1..1 | |
| 3 | XML 영역 크기 (XMLSize) | | 1..1 | |
| 4 | 첨부파일개수 (AttachFileQuantity) | | 1..1 | |
| 5 | 첨부파일크기 (AttachFileSize) | | 1..* | |
| 6 | 최초등록증명서크기 (CertificateSize) | | 1..1 | |
| XML 영역 (XML) | | | 1..1 | |
| 패키지 메타데이터(PackageMetadata) | | | 1..1 | |
| 7 | 패키지식별자 (PackageID) | | 1..1 | |
| 8 | 패키지내용설명 (Description) | | 1..1 | |
| 9 | 사용자확장영역 (Extensions) | | 0..1 | |
| 보관이력 (ArchiveHistory) | | | 1..1 | |
| 10 | 보관기록 (ArchiveRecord) (1..*) | 기록번호 (RecordNumber) | 1..1 | |
| 11 | | 공인전자문서센터ID (ArcID) | 1..1 | |
| 12 | | 공인전자문서센터명 (ArcName) | 1..1 | |
| 13 | | 보관시작 일시 (ArcStartDateTime) | 1..1 | |
| 14 | | 보관만료 일시 (ArcEndDateTime) | 1..1 | |
| 15 | | AIP패키지ID (AipPackageID) | 1..1 | |
| 16 | | 이관정보 | 이관 일시 | 1..1 |

| | | | | | | | |
|---------------------------------|----------------------------------|--------------------------|---------------------------------------|-------------------|---------------------|------|--|
| | | | (TransferDateTime) | | | | |
| 17 | | (TransferInfo) (1..1) | 이 관 사 유 (TransferReason) (1..1) | | 코 드 (ReasonCode) | 1..1 | |
| 18 | 텍 스트 (ReasonText) | | | | 0..1 | | |
| 19 | 암 호 화 (Encryption) (1..1) | | 암 호 화 처 리 구 분 (EncryptionType) | | 1..1 | | |
| 20 | | | 인 증 서 (Certificate) (0..1) | 발 급 자 (Issuer) | 1..1 | | |
| 21 | | | | 일련번호 (Serial) | 1..1 | | |
| 패키지 인증정보(PackageAuthentication) | | | | | | 1..1 | |
| 22 | 서명일시 (DateTime) | | | | | 1..1 | |
| 23 | 서명 (Signature) | | | | | 1..1 | |
| 24 | 인 증 서 (Certificate) (1..1) | 발급자 (Issuer) | | | | 1..1 | |
| 25 | | 일련번호 (Serial) | | | | 1..1 | |
| 26 | 서명자ID (SignerID) | | | | | 1..1 | |
| 27 | 서명자 명 (SignerName) | | | | | 0..1 | |

3.2.5.1.4 메타데이터 집합 정보 유형 정의

(1) 헤더정보

| | | | | | |
|---------------|---------------------------------------|-----|-------------------|-----|--|
| 관리번호 | TP-A-001 | 영문명 | HeaderInformation | | |
| 정의 | 패키지 구조에 대한 간략한 정보 | | | | |
| 사용 설명 | 패키지의 종류와 패키지의 각 영역을 파싱하기 위한 정보를 기술한다. | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |

| | |
|----|-----|
| 비고 | --- |
|----|-----|

(2) XML 영역

| | | | | | |
|---------------|---|-----|-----|-----|--|
| 관리번호 | TP-A-002 | 영문명 | XML | | |
| 정의 | 각 공인전자문서센터에서의 전자문서 보관 및 이관 정보 | | | | |
| 사용 설명 | 패키지 메타데이터, 보관이력, 패키지 인증정보로 구성된다. | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | XML영역 부분은 수관 공인전자문서센터에서 TIP를 AIP로 변환하는 과정에서 사용되지는 않으며, 전자문서 관리목적 및 재 이관 등을 고려하여 유지·관리 되어야 함 | | | | |

(3) 첨부파일(원본 전자문서)

| | | | | | |
|---------------|---|-----|------------|-----|--|
| 관리번호 | TP-A-003 | 영문명 | AttachFile | | |
| 정의 | 이용자가 공인전자문서센터에 등록한 전자문서 원본 파일(들) | | | | |
| 사용 설명 | 이관대상 AIP로부터 전자문서 원본파일들을 추출하여 첨부한다. | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..* | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 이관대상 AIP에 첨부된 원본 전자문서 파일이 복수개인 경우, 해당 파일들을 추출하여 AIP에 첨부되어 있던 순서대로 TIP에 첨부하여야 함. | | | | |

(4) 최초등록증명서

| | | | |
|-------|---|-----|----------|
| 관리번호 | TP-A-004 | 영문명 | OpRecord |
| 정의 | 이용자가 공인전자문서센터에 전자문서를 등록했을 때 발급된 최초등록증명서 | | |
| 사용 설명 | 보관중인 최초등록증명서를 찾아 첨부한다. | | |
| 사용 사례 | --- | | |

| | | | | | |
|---------------|--|----|--|-----|--|
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 최초등록증명서는 이관대상 원본 전자문서가 공인전자문서센터에 보관된 시점을 보장하는 중요한 정보이며, 이·수관 프로세스에서는 TIP에 첨부된 원본 전자문서 파일들에 대한 무결성을 보장하는 역할을 함 수관 공인전자문서센터는 최초등록증명서를 검증한 후 증명서 내의 등록증적을 이용하여 수관 공인전자문서센터의 증명서 발급 정책으로 재발급하여야 함 | | | | |

(5) XML영역 - 패키지 메타데이터

| | | | | | |
|---------------|-------------------------------|-----|-----------------|-----|--|
| 관리번호 | TP-A-002-001 | 영문명 | PackageMetadata | | |
| 정의 | 패키지 전체에 대한 정보 | | | | |
| 사용 설명 | 패키지 식별정보, 패키지에 대한 설명 등을 기술한다. | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | | | | | |

(6) XML영역 - 보관이력

| | | | | | |
|---------------|--|-----|----------------|-----|--|
| 관리번호 | TP-A-002-002 | 영문명 | ArchiveHistory | | |
| 정의 | 각 이관 공인전자문서센터에서 전자문서가 보관되고 이관된 이력 | | | | |
| 사용 설명 | 이관 공인전자문서센터에서의 전자문서 보관정보 및 이관정보를 기술하며, 이 · 수관이 발생할 때마다 추가됨 | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | | | | | |

(7) XML영역 - 패키지 인증정보

| | | | | | |
|---------------|--|-----|-----------------------|-----|--|
| 관리번호 | TP-A-002-003 | 영문명 | PackageAuthentication | | |
| 정의 | XML 영역의 무결성 보장을 위한 정보 | | | | |
| 사용 설명 | XML 영역에 대하여 W3C “XML-Signature Syntaxand Processing“ (RFC3275)의 enveloped signature 포맷을 준수하여 전자서명을 수행 | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | | 자릿수 | |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 하위 요소인 KeyInfo 요소의 KeyInfoType은 “KeyValue“와“X509Data “로 제한하며, “X509Data“ 사용 시 “X509Certificate“은 반드시 포함되어야 하며, 패키지 검증시 인증서에 대한 검증이 반드시 이루어져야 한다. | | | | |

3.2.5.1.5 메타데이터 상세 항목

(1) 헤더정보 - 패키지버전

| | | | | | |
|---------------|-------------------------------|-----|---------|-----|---|
| 관리번호 | TP-B-001 | 영문명 | Version | | |
| 정의 | TIP 스키마의 버전 | | | | |
| 사용 설명 | 본 규격을 준용한 패키지의 버전은 3.0으로 설정한다 | | | | |
| 사용 사례 | 1.0, 1.1, 1.5, 2.0, 3.0 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 3 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(2) 헤더정보 - 패키지종류

| | | | |
|-------|---------------------|-----|------|
| 관리번호 | TP-B-002 | 영문명 | Type |
| 정의 | 해당되는 패키지의 유형 | | |
| 사용 설명 | 해당되는 패키지의 유형을 표현한다. | | |

| | | | | | |
|------------------|---------------------------|----|--------|-----|---|
| 사용 사례 | "TIP" | | | | |
| 반복수 | 1..1 | 타입 | string | 자릿수 | 3 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 이 · 수관 포맷인 "TIP" 값을 사용한다. | | | | |

(3) 헤더정보 - XML 영역 크기

| | | | | | |
|---------------|--|-----|---------|-----|---|
| 관리번호 | TP-B-003 | 영문명 | XMLSize | | |
| 정의 | XML 영역의 크기를 할당한다. | | | | |
| 사용 설명 | --- | | | | |
| 사용 사례 | 1000 bytes 표현시 => 000003E8 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | Long | 자릿수 | 4 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | Hexadecimal을 사용하여 network byte order(big endian)로 배열 | | | | |

(4) 헤더정보 - 첨부파일개수

| | | | | | |
|---------------|--|-----|--------------------|-----|---|
| 관리번호 | TP-B-004 | 영문명 | AttachFileQuantity | | |
| 정의 | 정보패키지에 첨부된 첨부파일(원본문서)의 전체 개수 | | | | |
| 사용 설명 | --- | | | | |
| 사용 사례 | 20 개 표현시 => 0014 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | Short | 자릿수 | 2 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | Hexadecimal을 사용하여 network byte order(big endian)로 배열 | | | | |

(5) 헤더정보 - 첨부파일크기

| | | | |
|-------|--------------------------------------|-----|----------------|
| 관리번호 | TP-B-005 | 영문명 | AttachFileSize |
| 정의 | 정보패키지에 첨부된 첨부파일(원본문서)의 크기 | | |
| 사용 설명 | 이 정보는 배열 형식으로 첨부파일의 크기에 대한 정보를 기재한다. | | |

| | | | | | |
|---------------|--|----|--------|-----|---|
| 사용 사례 | 1000 bytes 표현시 => 00000000000003E8 | | | | |
| 반복수 | - TIP : 1..* | 타입 | Double | 자릿수 | 8 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | HexaDecimal을 사용하여 network byte order(big endian)로 배열 | | | | |

(6) 헤더정보 - 최초등록증명서크기

| | | | | | |
|---------------|---|-----|-----------------|-----|---|
| 관리번호 | TP-B-006 | 영문명 | CertificateSize | | |
| 정의 | 정보패키지에 첨부된 최초등록증명서의 크기 | | | | |
| 사용 설명 | 전자문서가 최초로 공인전자문서센터에 등록되었을 때 공인전자문서센터에서 발급되었던 최초등록증명서의 크기를 할당한다. | | | | |
| 사용 사례 | 1000 bytes 표현시 => 000003E8 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | Long | 자릿수 | 4 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | HexaDecimal을 사용하여 network byte order(big endian)로 배열 | | | | |

(7) 패키지 메타데이터 - 패키지식별자

| | | | | | |
|---------------|--|-----|-----------|-----|-------|
| 관리번호 | TP-B-007 | 영문명 | PackageID | | |
| 정의 | TIP의 고유 식별자 | | | | |
| 사용 설명 | 패키지 식별자로써 공인전자문서센터 사업자와 정보패키지 유형을 판별할 수 있도록 OID 활용. 이후의 식별자는 사업자가 자체적으로 할당. 영문과 숫자만으로 구성 | | | | |
| 사용 사례 | 공인전자문서센터 사업자의 TIP 관리 OID + 사업자 할당 식별자 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 128이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(8) 패키지 메타데이터 - 패키지내용설명

| 관리번호 | TP-B-008 | 영문명 | Description | | |
|---------------|--|-----|-------------|-----|--------|
| 정의 | 정보패키지에 대한 추가정보 | | | | |
| 사용 설명 | 정보패키지에 대해 추가적인 정보를 기술한다. 이때, 이용자는 대표적인 문구를 보고 검색하는 경우가 많기 때문에 간략하게 기술한다. | | | | |
| 사용 사례 | “xxx 문서를 이·수관 하기위한 정보 패키지임” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 1000이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(9) 패키지 메타데이터 - 사용자확장영역

| 관리번호 | TP-B-009 | 영문명 | Extensions | | |
|---------------|--|-----|-------------|-----|----|
| 정의 | 본 규격에서 제시한 메타데이터 이외에 이용자가 추가적인 서비스에 활용하기 위해 자체적으로 규정하는 영역 | | | | |
| 사용 설명 | | | | | |
| 사용 사례 | | | | | |
| 반복수 | - TIP : 0..1 | 타입 | Object Type | 자릿수 | -- |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 이관 공인전자문서센터와 수관 공인전자문서센터는 부가적인 데이터의 이관목적으로 본 사용자확장영역을 협의 하에 사용할 수 있음 | | | | |

(10) 보관이력 - 보관기록 - 기록번호

| | | | | | |
|-------|---|-----|------------------|-----|----|
| 관리번호 | TP-B-010 | 영문명 | RecordNumber | | |
| 정의 | 보관기록의 고유번호 | | | | |
| 사용 설명 | 최초 공인전자문서센터인 경우는 1을 부여하고, 수관받은 공인전자문서센터인 경우는 마지막 보관기록번호의 다음번호를 부여 | | | | |
| 사용 사례 | 1 | | | | |
| 반복수 | - TIP : 1..1 | 타입 | Positive Integer | 자릿수 | -- |

| | |
|---------------|---|
| 코드 값 & 기본값 목록 | --- |
| 비고 | 이용자의 전자문서를 등록받은 최초 공인전자문서센터인 경우는 최초 이관이 되며 보관기록이 1개 이므로 기록번호를 1값으로 부여하며, 다음 공인전자문서센터에서 또다시 이관이 발생하게 되면 보관기록이 추가되므로 기록번호를 2값으로 부여한다. |

(11) 보관이력 - 보관기록- 보관정보 - 공인전자문서센터ID

| | | | | | |
|---------------|----------------------------------|-----|--------|-----|------|
| 관리번호 | TP-B-011 | 영문명 | ArcID | | |
| 정의 | 전자문서의 보관을 수행한 공인전자문서센터의 ID | | | | |
| 사용 설명 | 전자문서의 보관을 수행한 공인전자문서센터의 ID를 기술한다 | | | | |
| 사용 사례 | “KISA” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | String | 자릿수 | 12이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(12) 보관이력 - 보관기록- 보관정보 - 공인전자문서센터명

| | | | | | |
|------------------|----------------------------------|-----|---------|-----|-------|
| 관리번호 | TP-B-012 | 영문명 | ArcName | | |
| 정의 | 전자문서의 보관을 수행한 공인전자문서센터의 이름 | | | | |
| 사용 설명 | 전자문서의 보관을 수행한 공인전자문서센터의 이름을 기술한다 | | | | |
| 사용 사례 | “한국인터넷진흥원” | | | | |
| 반복수 | - TIP : 1..0 | 타입 | String | 자릿수 | 128이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(13) 보관이력 - 보관기록- 보관정보 - 보관시작일시

| | | | |
|-------|--------------------------------------|-----|------------------|
| 관리번호 | TP-B-013 | 영문명 | ArcStartDateTime |
| 정의 | 전자문서가 해당 공인전자문서센터에 보관된 일시 | | |
| 사용 설명 | 전자문서가 공인전자문서센터에 등록되거나 수관된 일시를 GMT 형식 | | |

| | | | | | |
|---------------|-----------------------------|----|----------|-----|----|
| | 으로 기재 | | | | |
| 사용 사례 | “YYYY-MM-DDThh:mm:ss” + “Z” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | datetime | 자릿수 | 20 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(14) 보관이력 - 보관기록- 보관정보 - 보관만료일시

| | | | | | |
|---------------|---|-----|----------------|-----|----|
| 관리번호 | TP-B-014 | 영문명 | ArcEndDateTime | | |
| 정의 | 전자문서가 공인전자문서센터에서 폐기된 일시 | | | | |
| 사용 설명 | 전자문서가 공인전자문서센터에서 폐기될 예정일시를 GMT 형식으로 기재 | | | | |
| 사용 사례 | “YYYY-MM-DDThh:mm:ss” + “Z” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | datetime | 자릿수 | 20 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 이관 공인전자문서센터의 폐업으로 발생한 이·수관 시, 이관 공인전자문서센터의 이관처리일시(TIP의 이관일시)와 수관 공인전자문서센터의 수신일시(AIP의 등록일시) 사이에 발생하는 시간차 동안 전자문서가 공인전자문서센터에 보관 중이었음을 증명할 수 없게 되므로, 이·수관 완료 후 이관 공인전자문서센터에서 전자문서가 폐기될 시점을 기재하여, 공인전자문서센터 내에서의 전자문서보관의 연속성을 보장하기 위함임. 만약 이관 공인전자문서센터의 전자문서 폐기증적이 존재한다면, 이관 공인전자문서센터에서의 전자문서 보관기간 만료일시 정보로서, 본 보관만료일시 필드의 정보보다 우선 적용하도록 함 | | | | |

(15) 보관이력 - 보관기록- 보관정보 - AIP 패키지 ID

| | | | | | |
|--------|--|-----|--------------|-----|-------|
| 관리번호 | TP-B-015 | 영문명 | AipPackageID | | |
| 정의 | 이관 공인전자문서센터의 API ID | | | | |
| 사용 설명 | 이관 공인전자문서센터의 AIP의 패키지식별자(PackageID) 기재 | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 128이하 |
| 코드 값 & | --- | | | | |

| | |
|--------|-----|
| 기본값 목록 | |
| 비고 | --- |

(16) 보관이력 - 보관기록- 이관정보 - 이관일시

| | | | | | |
|---------------|---|-----|------------------|-----|----|
| 관리번호 | TP-B-016 | 영문명 | TransferDateTime | | |
| 정의 | 전자문서가 이관 공인전자문서센터에서 이관작업이 수행된 일시 | | | | |
| 사용 설명 | 이관 공인전자문서센터의 이관작업 수행 일시를 GMT 형식으로 기재 | | | | |
| 사용 사례 | “YYYY-MM-DDThh:mm:ss” + “Z” | | | | |
| 반복수 | - TIP : 1.1 | 타입 | datetime | 자릿수 | 20 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 의미적으로는 이관 공인전자문서센터에서 이관작업이 수행된 시각으로서 서명일시보다 미래이나, 기능적으로는 패키지의 메타데이터를 먼저 구성한 후 전자서명을 수행하기 때문에 서명일시보다 과거임. 따라서 혼란을 없애기 위해서 서명일시와 동일한 시각값을 설정. 이·수관이 성공한 후 전자문서가 폐기되는 시점인 보관만료일시보다는 항상 과거임 | | | | |

(17) 보관이력 - 보관기록- 이관정보 - 이관사유 - 코드

| | | | | | |
|---------------|--|-----|------------|-----|---|
| 관리번호 | TP-B-017 | 영문명 | ReasonCode | | |
| 정의 | 이관 사유의 코드 | | | | |
| 사용 설명 | 이관 사유의 코드값을 기재 | | | | |
| 사용 사례 | “00”, “01”, “99” | | | | |
| 반복수 | - TIP : 1.1 | 타입 | string | 자릿수 | 2 |
| 코드 값 & 기본값 목록 | “00” : 사용자요청이관 “01” : 공인전자문서센터요청이관 “99” : 이관 공인전자문서센터 폐업 | | | | |
| 비고 | --- | | | | |

(18) 보관이력 - 보관기록- 이관정보 - 이관사유 - 텍스트

| | | | |
|------|---------------------------|-----|------------|
| 관리번호 | TP-B-018 | 영문명 | ReasonText |
| 정의 | 이관 공인전자문서센터의 이관 사유에 대한 설명 | | |

| | | | | | |
|---------------|-----------------------------------|----|--------|-----|-------|
| 사용 설명 | 이관 공인전자문서센터의 이관 사유에 대한 설명을 상세히 기재 | | | | |
| 사용 사례 | | | | | |
| 반복수 | - TIP : 0..1 | 타입 | string | 자릿수 | 512이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(19) 보관이력 - 보관기록- 이관정보 - 암호화 - 암호화 처리구분

| | | | | | |
|---------------|--|-----|----------------|-----|---|
| 관리번호 | TP-B-019 | 영문명 | EncryptionType | | |
| 정의 | TIP의 전자문서 첨부파일에 대한 암호화 처리 지시자 | | | | |
| 사용 설명 | TIP의 전자문서 첨부파일에 대한 암호화 적용여부를 지시하는 정보로서, 암호화하지 않음, 패스워드 암호화, 공개키 암호화의 3가지 방식 중 하나를 선택 | | | | |
| 사용 사례 | “1” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 1 |
| 코드 값 & 기본값 목록 | - 공개키 암호화 적용 : “1” - 패스워드 암호화 적용 : “2” - 암호화 미적용 : “0” | | | | |
| 비고 | 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용하되, 공개키 암호화 방법은 RecipientInfo로 KeyTransRecipientInfo 형식을, 패스워드 암호화 방법은 PasswordRecipientinfo 형식을 각각 사용하도록 함. 암호화하지 않거나(0) 패스워드 암호화(2)일 경우, 다음 요소인 인증서(Certificate) 필드는 생략함 | | | | |

(20) 보관이력 - 보관기록- 이관정보 - 암호화 - 인증서 - 발급자

| | | | | | |
|---------------|---|-----|--------|-----|-------|
| 관리번호 | TP-B-020 | 영문명 | Issuer | | |
| 정의 | 전자문서 첨부파일을 암호화하는데 사용한 수관 공인전자문서센터 인증서의 발급자 정보 | | | | |
| 사용 설명 | 전자문서 첨부파일을 암호화하는데 사용한 수관 공인전자문서센터 인증서의 발급자 DN을 기재함 | | | | |
| 사용 사례 | “CN=CA,OU=AccreditedCA,O=KoreaCertificateAuthority,C=KR” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 300이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | RFC2253의 “LDAP-DN” 포맷을 준수하여야 하며, CN, OU, O, C 의 순서로 배열한다. | | | | |

| | |
|--|---|
| | 상위 요소인 인증서 요소는 전자문서 첨부파일을 공개키 암호화하여 발급하는 경우에만 사용하도록 하며, 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용함 |
|--|---|

(21) 보관이력 - 보관기록- 이관정보 - 암호화 - 인증서 - 일련번호

| | | | | | |
|---------------|---|-----|--------|-----|------|
| 관리번호 | TP-B-021 | 영문명 | Serial | | |
| 정의 | 전자문서 첨부파일을 암호화하는데 사용한 수관 공인전자문서센터 인증서의 일련번호 | | | | |
| 사용 설명 | 전자문서 첨부파일을 암호화하는데 사용한 수관 공인전자문서센터 인증서의 일련번호를 기재함 | | | | |
| 사용 사례 | “036a481d” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 50이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | HexaDecimal의 string 형식으로 표현하도록 하며 string의 자리수가 홀수인 경우는 앞에 “0”을 추가한다. 상위 요소인 인증서 요소는 전자문서 첨부파일을 공개키 암호화하여 발급하는 경우에만 사용하도록 하며, 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용함 | | | | |

(22) 패키지 인증정보 - 서명일시

| | | | | | |
|---------------|--|-----|----------|-----|----|
| 관리번호 | TP-B-022 | 영문명 | DateTime | | |
| 정의 | 전자 서명을 실행한 일시 | | | | |
| 사용 설명 | XML 영역에 대한 전자 서명을 실행한 일시를 GMT 형식으로 기재함 | | | | |
| 사용 사례 | “YYYY-MM-DDThh:mm:ss” + "Z" | | | | |
| 반복수 | - TIP : 1..1 | 타입 | datetime | 자릿수 | 20 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

(23) 패키지 인증정보 - 서명

| | | | |
|-------|---|-----|-----------|
| 관리번호 | TP-B-023 | 영문명 | Signature |
| 정의 | XML 영역에 대한 전자서명 | | |
| 사용 설명 | XML 영역에 대한 전자서명 정보로서 W3C “XML-Signature | | |

| | | | | | |
|---------------|--|----|----------------|-----|--------|
| | Syntax and Processing" (RFC3275)의 enveloped signature 포맷을 준수하여 생성함 | | | | |
| 사용 사례 | --- | | | | |
| 반복수 | - TIP : 1.1 | 타입 | Signature Type | 자릿수 | 5000이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | 하위 요소인 KeyInfo 요소의 KeyInfoType은 "KeyValue"와 "X509Data"로 제한하며, "X509Data" 사용 시 "X509Certificate"은 반드시 포함되어야 하며, 패키지 검증시 인증서에 대한 검증이 반드시 이루어져야 한다. | | | | |

(24) 패키지 인증정보 - 인증서 - 발급자

| | | | | | |
|---------------|---|-----|--------|-----|-------|
| 관리번호 | TP-B-024 | 영문명 | Issuer | | |
| 정의 | 전자서명 인증서의 발급자 정보 | | | | |
| 사용 설명 | XML 영역에 대한 전자 서명을 실행한 인증서의 발급자 DN을 기재함 | | | | |
| 사용 사례 | “CN=CA,OU=AccreditedCA,O=KoreaCertificateAuthority,C=KR” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 300이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | RFC2253의 “LDAP-DN” 포맷을 준수하여야 하며, CN, OU, O, C 의 순서로 배열한다. | | | | |

(25) 패키지 인증정보 - 인증서 - 일련번호

| | | | | | |
|---------------|--|-----|--------|-----|------|
| 관리번호 | TP-B-025 | 영문명 | Serial | | |
| 정의 | 전자서명 인증서의 일련번호 | | | | |
| 사용 설명 | XML 영역에 대한 전자 서명을 실행한 인증서의 일련번호를 기재함 | | | | |
| 사용 사례 | “036a481d” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 50이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | Hexadecimal의 string 형식으로 표현하도록 하며 string의 자리수가 홀 | | | | |

| | |
|--|---------------------|
| | 수인 경우는 앞에 “0”을 추가한다 |
|--|---------------------|

(26) 패키지 인증정보 - 서명자ID

| | | | | | |
|------------------|-------------------------------------|-----|----------|-----|------|
| 관리번호 | TP-B-026 | 영문명 | SignerID | | |
| 정의 | 서명 행위자의 식별자 | | | | |
| 사용 설명 | TIP를 생성하는 이관 공인전자문서센터의 ID 또는 약자를 기재 | | | | |
| 사용 사례 | “KISA” | | | | |
| 반복수 | - TIP : 1..1 | 타입 | string | 자릿수 | 12이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | | | | | |

(27) 패키지 인증정보 - 서명자 명

| | | | | | |
|------------------|--------------------------------|-----|------------|-----|-------|
| 관리번호 | TP-B-027 | 영문명 | SignerName | | |
| 정의 | 서명 행위자의 이름 | | | | |
| 사용 설명 | TIP를 생성하는 이관 공인전자문서센터의 기관명을 기재 | | | | |
| 사용 사례 | “한국인터넷진흥원” | | | | |
| 반복수 | - TIP : 0..1 | 타입 | string | 자릿수 | 128이하 |
| 코드 값 & 기본값 목록 | --- | | | | |
| 비고 | --- | | | | |

3.2.6 전자서명의 범위

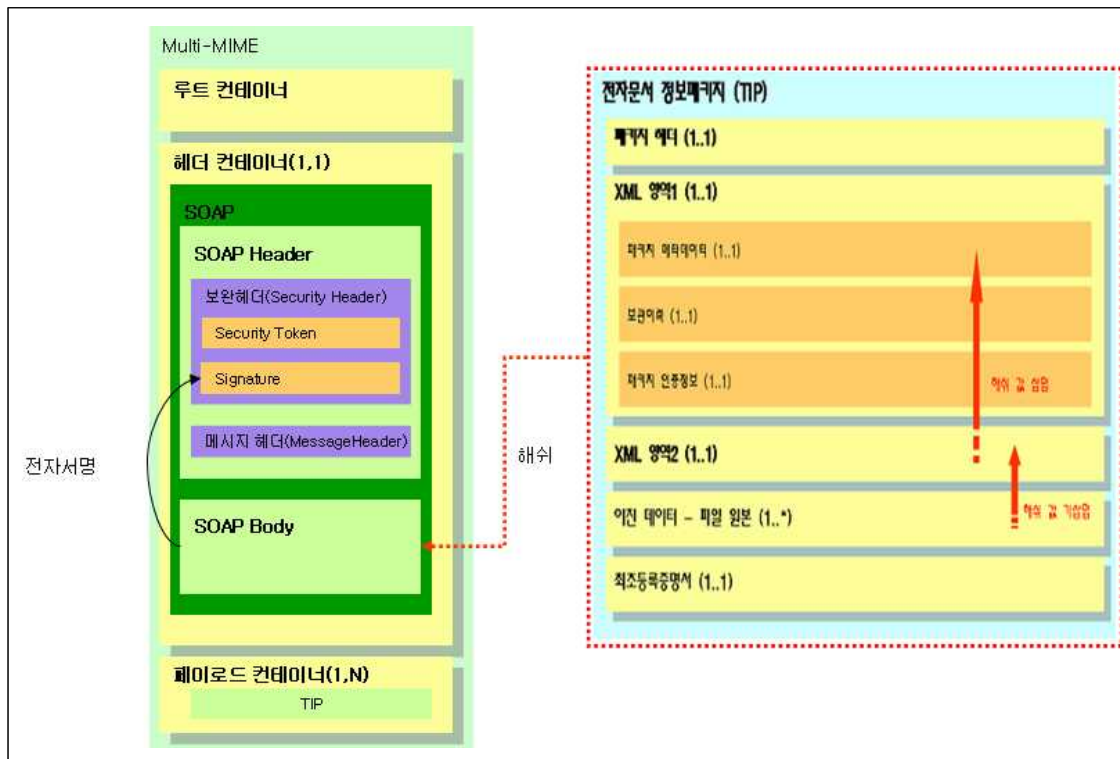
3.2.6.1 이 · 수관 메시지 전자서명

이 · 수관 메시지에 대한 무결성 검증 및 부인 방지를 위해, 이관 공인전자문서센터 및 수관 공인전자문서센터는 이 · 수관 메시지에 전자서명을 추가해야 한다.

이 · 수관 메시지에 대한 전자서명은 W3C에서 권고하는 "XML Signature Syntax and Processing" 규약을 준수한 WS-Security 규약(WS-Security 규약 V1.1)에 기술된 형식으로 생성 하여야 하며, 전자서명정보를 담은 <Signature> 항목은 SOAP Header의 하위 항목으로 기술된다.

서명 대상은 실제 송·수신 메시지를 포함하는 SOAP Body 부분이다.

그리고 이 · 수관 메시지 전체에 대한 무결성 검증 및 부인 방지를 위하여, 페이로드 컨테이너 부분에 첨부된 각 TIP의 해쉬 값을 생성하여 SOAP Body에 삽입하여야 한다.



3.2.6.2 패키지 전자서명

TIP에 대한 전자서명의 범위는 XML 영역에만 한정한다. 전자서명의 생성 방법은 W3C “XML-Signature Syntax and Processing” (RFC3275)의 enveloped signature 포맷을 준수하여 생성하여야 한다.

TIP에 첨부되는 전자문서 첨부파일에 대한 무결성 검증은, 최초등록증명서에 포함된 원본 전자문서의 해쉬값을 이용하여 수행하고, 최초등록증명서는 그 자체로 무결성 검증이 가능한 서명데이터이기 때문에 별도의 무결성 검증 방안을 적용할 필요는 없다.

증명서 규격 상 최초등록증명서에 포함된 원본 전자문서의 해쉬값은 AIP에 첨부된 파일들을 하나로 연결하여 계산된 값이므로, TIP에 첨부된 파일들도 동일한 순서로 연결한 후 계산하여야 한다.



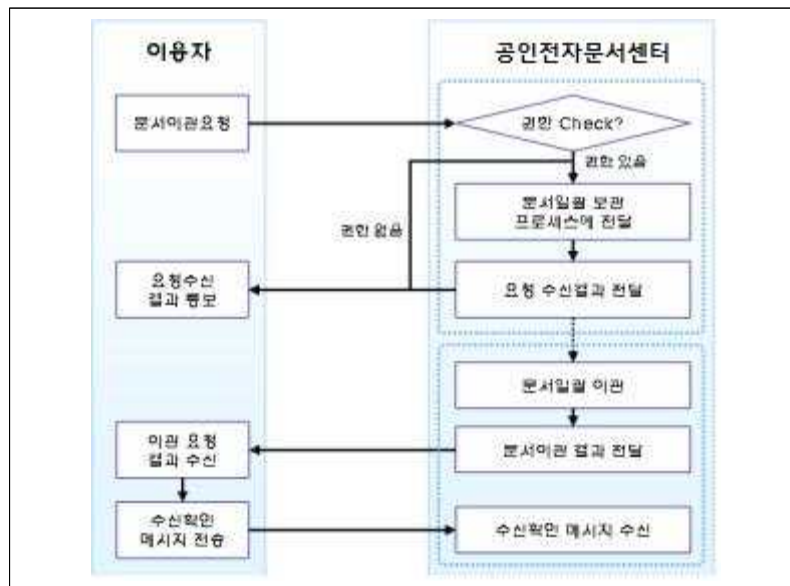
3.3 온라인 이·수관 단계별 처리 방안

3.3.1 개요

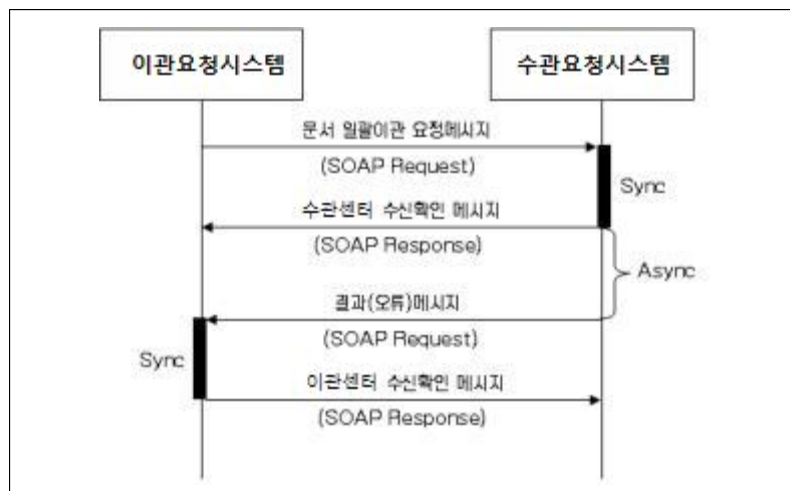
시스템연계에 의한 실시간 전자문서이관인 경우 통신 프로토콜은 SOAP Binding을 지원하며, 메시지 패키징 구조는 “3.2 이·수관 정보구조”에 따라 생성된다.

3.3.2 통신 프로토콜 및 메시지 처리 흐름

3.3.2.1 처리절차



3.3.2.2 프로토콜 정의



일반적으로 이·수관은 대용량 문서에 대하여 발생하기 때문에 그림과 같이 Async 방식으로 이루어지나, 단 건에 대한 처리 또는 대용량 문서라도 시스템에서의 처리가 가능한 경우라면 Sync 방식도 가능하다. 이 경우 이관 공인전자문서센터의 문서이관 요청메시지에 대하여 수관 공인전자문서센터의 수신확인메시지 대신 결과메시지가 바로 전달되게 된다

3.3.3 오류 처리 방안

이관 공인전자문서센터는 이관 요청메시지를 보낸 후 수관 공인전자문서센터로부터 수신확인에 대한 메시지를 받지 못하였거나, 송신 실패 메시지를 수신하였을 경우, 이관요청메시지를 재전송하여 수관 공인전자문서센터가 이관요청메시지를 정상적으로 수신하였음을 반드시 확인하여야 한다.

수관 공인전자문서센터 역시, 이관요청에 대한 처리 완료 후 결과메시지를 수관 공인전자문서센터에 전달하고 나면, 반드시 결과메시지 수신 여부를 확인하여 이관 공인전자문서센터가 이를 정상적으로 수신하였음을 확인하여야 한다.

수신한 응답메시지에서 FailCount가 1이상인 경우에 이관 공인전자문서센터는 실패한 전자문서에 대한 실패코드를 파악하여 데이터 오류인지 여부를 확인한 후, 각 실패 상황에 맞게 조치하도록 한다.

3.3.4 온라인 보안 처리 방안

온라인으로 전달되는 이관 요청메시지 및 응답메시지에 대하여 이·수관 공인전자문서센터는 전자서명 값을 통해 상대 공인전자문서센터에 대한 인증 및 메시지의 무결성 등에 대한 기술적 검증 및 추후 부인방지 기능을 수행할 수 있어야 한다.

또한, 이관 요청메시지 및 응답메시지에 대한 기밀성 보장을 위해서, 해당 메시지의 기밀성을 보장할 수 있는 기술을 적용하여야 한다. 이를 위하여 기본적으로 이관 공인전자문서센터와 수관 공인전자문서센터 간 통신 세션을 암호화하는 방식을 적용하여야 하며, 여기에 추가적으로 TIP에 첨부된 전자문서를 CMS(RFC3852)의 EnvelopedData 형식으로 암호화하여 이·수관할 수 있다.

온라인 상에서의 메시지 전송보안은 연계 인터페이스 규격의 “5. 보안 및 메시지 검증”과 동일한 보안기준을 준수하여야 한다.

3.4 오프라인 이·수관 단계별 처리 방안

3.4.1 개요

모든 공인전자문서센터는 오프라인 상으로 전자문서를 이관하는 기능을 반드시 제공하여야 하는데, 오프라인으로 전자문서를 이관하기 위해서는 이관 공인전자문서센터가 고유의 시스템 구조에 의해 관리하던 전자문서 및 최초등록증명서, 기타 관리정보들을 시스템 및 언어 독립적인 정보구조(“3.2.3 이·수관 요청메시지”) 형태로 Export하여야 하며, 수관 공인전자문서센터는 반대로 이 정보를 읽어서 수관 공인전자문서센터 내부의 시스템 구조에 맞게 Import하여야 한다.

3.4.2 오프라인 처리 단계

3.4.2.1 이관 공인전자문서센터의 사전 준비 작업

(1) 기초정보 전달

이관 공인전자문서센터는 보관하고 있던 전자문서에 대한 이관 요청이 발생되면, 이용자 및 수관 공인전자문서센터와 전자문서 이·수관에 대한 합의를 이루어야 한다. 기본적인 합의가 이루어진 상태에서 이관 공인전자문서센터는 이관대상에 대한 정보 및 이관방식에 대한 구체화를 위해 이관에 대하여 이관대상이 되는 전자문서에 대한 종합적인 정보를 취합하여, 이를 수관 공인전자문서센터 및 각 이용자에게 전달하고 이에 대한 추가 확인을 받는다. 이관대상 전자문서에 대한 종합적인 정보는 다음과 같은 구조로 취합되어서 전달되도록 한다. 이 정보는 이관을 준비하는 단계에서 수관 공인전자문서센터 및 이용자에게 이관대상에 대한 기초정보를 전달하기 위한 목적으로 1차 발급이 되는데, 현 단계에서 서비스가 중단된 것이 아니므로 이관대상이 되는 전자문서, 증명서에 대한 전체 건수 및 전체 용량 정보는 다소 차이가 발생할 수 있음을 통지한다.

○ 수관 공인전자문서센터에 전달할 내용

| 항 목 | | | 데이터 값 | 비고 |
|-------|----------------|-------------|-------|----|
| 종합 정보 | 이관 공인전자문서센터 정보 | 공인전자문서센터 ID | | |
| | | 공인전자문서센터 명 | | |
| | | 주소 | | |

| | | | | | | | |
|------------------------------|--------------------------------------|----------------|------------------------------|----------------|--|--|--|
| | | 연락처(Tel) | | | | | |
| | | 이관 담당 자 | 이름 | | | | |
| | | | 주소 | | | | |
| | | | 연락처(Tel) | | | | |
| | | | 연락처(휴대폰) | | | | |
| | 이관대상 사용자 수 | | | | | | |
| | 이관대상 정보의 용량 | | | | | | |
| | 이관대상 전자문서 총 건수 | | | | | | |
| | 이관작업 개시 예정일 | | | | | | |
| | 사 용 자 별 이 관 정 보 | 기업 A | 기업 이 관 총 합 정보 | 이관대상 사용자 수 | | | |
| | | | | 이관대상 정보의 용량 | | | |
| | | | | 이관대상 전자문서 총 건수 | | | |
| 기관 사 용 자 별 정보 | | | 사 용 자 (가) | 사용자명 | | | |
| | | | | 소속 부서(팀) | | | |
| | | | | 연락처(Tel) | | | |
| | | | | 연락처(휴대폰) | | | |
| | | | | 이메일 | | | |
| | | | | 이관대상 전자문서 총 건수 | | | |
| 사 용 자 (나) | | ... | ... | | | | |
| 사용자 A | | 사용자 명 | | | | | |
| | | 소속기관 | | | | | |
| | | 연락처(Tel) | | | | | |
| | | 연락처(휴대폰) | | | | | |
| | | 이메일 | | | | | |
| | | 이관대상 전자문서 총 건수 | | | | | |

| | | | | |
|------------|----------------|------------------|-----|--|
| | 사용자 B | ... | ... | |
| 부 가 정 보 | 정 보 전 달 매 체 | 유형 | | 유형(CD, DVD, WORM Storage, SAN Storage, DAS 등) |
| | | 제조사 | | |
| | | 모델명 | | |
| | | 전체 용량 | | |
| | | 연계인터페이스 모듈 제공 여부 | | |

※ DAS: Direct Attached Storage, SAN: Storage Area Network, NAS: Network Attached Storage

○ 이용자(기업 이용자)에게 전달할 내용

| 항 목 | | | 데이터 값 | 비고 |
|------------|------------------------|---------------|----------|----|
| 종 합 정 보 | 이관 공인 전자문서센 터 정보 | 공인전자문서센터 ID | | |
| | | 공인전자문서센터 명 | | |
| | | 주소 | | |
| | | 연락처(Tel) | | |
| | | 이관 담당 자 | 이름 | |
| | | | 주소 | |
| | | | 연락처(Tel) | |
| | | | 연락처(휴대폰) | |
| | 수관 공인 전자문서센 터 정보 | 공인전자문서센터 ID | | |
| | | 공인전자문서센터 명 | | |
| | | 주소 | | |
| | | 연락처(Tel) | | |

| | | | | | |
|---------------------------------|-------------------------|----------------|----------|--|--|
| | | 수관 담당 자 | 이름 | | |
| | | | 주소 | | |
| | | | 연락처(Tel) | | |
| | | | 연락처(휴대폰) | | |
| | 이관대상 사용자 수(기업 내 사용자 정보) | | | | |
| | 이관대상 정보의 용량 | | | | |
| | 이관대상 전자문서 총 건수 | | | | |
| | 이관작업 개시 예정일 | | | | |
| 사 용 자 별 관 정 보 | 사용자 A | 사용자 명 | | | |
| | | 소속기관 | | | |
| | | 연락처(Tel) | | | |
| | | 연락처(휴대폰) | | | |
| | | 이메일 | | | |
| | | 이관대상 전자문서 총 건수 | | | |
| | 사용자 B | ... | ... | | |

○ 이용자(일반 이용자)에게 전달할 내용

| 항 목 | | | 데이터 값 | 비고 |
|--|------------------------|-------------|-------|----|
| 이 · 수 관 공 인 전 자 문 서 센 터 정 보 | 이관 공인 전자문서센 터 정보 | 공인전자문서센터 ID | | |
| | | 공인전자문서센터 명 | | |
| | | 주소 | | |
| | | 연락처(Tel) | | |
| | | 이관 담당 | 이름 | |
| | | | 주소 | |

| | | | | | | |
|----------------|------------------------|---------------|----------|--|--|--|
| | | 자 | 연락처(Tel) | | | |
| | | | 연락처(휴대폰) | | | |
| | 수관 공인 전자문서센 터 정보 | 공인전자문서센터 ID | | | | |
| | | 공인전자문서센터 명 | | | | |
| | | 주소 | | | | |
| | | 연락처(Tel) | | | | |
| | | 수관 담당 자 | 이름 | | | |
| | | | 주소 | | | |
| | | | 연락처(Tel) | | | |
| | | | 연락처(휴대폰) | | | |
| 이관대상 정보의 용량 | | | | | | |
| 이관대상 전자문서 총 건수 | | | | | | |
| 이관작업 개시 예정일 | | | | | | |

(2) 이관범위 및 방식에 대한 합의

오프라인 이관인 경우에는 특별히 어떠한 Portable 저장장치를 사용할 것인지, 저장매체에 대한 봉인은 어떠한 방식으로 할 것인지, 저장매체의 운송수단은 어떠한 것을 사용할 것인지 등을 추가적으로 합의하도록 한다.

3.4.2.2 이관 공인전자문서센터의 Export 절차

이관 공인전자문서센터는 이관매체의 최대 저장용량을 기준으로 이관데이터를 분할하여 Export 하도록 한다. 저장매체의 용량에 따라 공인전자문서센터 간 전자문서 이관이 한 번에 완료되는 것이 아닐 수 있으므로 저장매체는 다음과 같은 정보데이터가 존재하게 된다.

① 이관 종합 정보 파일

- 이관 저장매체 내에 있는 전체정보를 종합한 Information 파일
- 물리적으로 하나의 이관 저장매체 내에 있는 TIP에 대한 메타정보 파일

| 항 목 | | 반복 | Type |
|-------|----------------|------|------|
| 종합 정보 | 이관 공인전자문서센터 정보 | 1..1 | |

| | | | | |
|--------------------------------------|------------------------|----------------|------|-----------|
| 보 | 공인전자문서센터 ID | | 1..1 | |
| | 공인전자문서센터 명 | | 1..1 | |
| | 주소 | | 1..1 | |
| | 연락처(Tel) | | 1..1 | |
| | 이관 담당자 | | 1..1 | Structure |
| | | 이름 | 1..1 | |
| | | 주소 | 1..1 | |
| | | 연락처(Tel) | 1..1 | |
| | | 연락처(휴대폰) | 1..1 | |
| | 이관대상 사용자 수(저장매체 당) | | 1..1 | |
| | 이관대상 정보의 용량(저장매체 당) | | 1..1 | |
| | 이관대상 전자문서 총 건수(저장매체 당) | | 1..1 | |
| | 이관 요청일 | | 1..1 | |
| | 요청메시지 파일의 총 건수(저장매체 당) | | 1..1 | |
| | 이관요청메시지 파일 | | 1..∞ | |
| | | 요청메시지 파일 명 | 1..1 | |
| | | 메시지 파일 용량 | 1..1 | |
| 사 용 자 별 이 관 정 보 | 기업 A | | 0..∞ | Structure |
| | | 기업이관종합정보 | 1..1 | |
| | | 이관대상 사용자 수 | 1..1 | |
| | | 이관대상 정보의 용량 | 1..1 | |
| | | 이관대상 전자문서 총 건수 | 1..1 | |
| | | 기관 이용자별 정보 | 0..∞ | Structure |
| | | 이용자명 | 1..1 | |
| | | 소속 부서(팀) | 1..1 | |
| | | 연락처(Tel) | 1..1 | |

| | | | | | | |
|------------------|-----------|----------------|----------------|---|-----------|-----------|
| | | | 연락처(휴대폰) | 1..1 | | |
| | | | 이메일 | 1..1 | | |
| | | | 이관대상 전자문서 총 건수 | 1..1 | | |
| | 개인 이용자 정보 | | | 0..∞ | Structure | |
| | | 이용자 명 | | | 1..1 | |
| | | 소속기관 | | | 1..1 | |
| | | 연락처(Tel) | | | 1..1 | |
| | | 연락처(휴대폰) | | | 1..1 | |
| | | 이메일 | | | 1..1 | |
| | | 이관대상 전자문서 총 건수 | | | 1..1 | |
| | 부 가 정 보 | 정보전달 매체 | | | 1..1 | Structure |
| | | | Serial No | | | 1..1 |
| 유형 | | | 1..1 | 유형(CD, DVD, WORM Storage, SAN Storage, DAS 등) | | |
| 제조사 | | | 1..1 | | | |
| 모델명 | | | 1..1 | | | |
| 전체 용량 | | | 1..1 | | | |
| 연계인터페이스 모듈 제공 여부 | | | 1..1 | | | |

② 이관 요청메시지 파일

- 이관 요청메시지에 대한 Single-Mime Packaging
- 이관 요청메시지 파일과 TIP 파일은 물리적으로 다른 파일로 분리됨
- 하나의 저장매체에 대한 이관요청메시지가 2개 이상 존재 가능
- TIP에 대한 정보를 담고 있는 이관 요청 및 응답메시지 구조는 “3.2 이 · 수관 정보구조”에 기술된 구조 참조

③ 이관 문서 파일

- 실제 전자문서를 포함하는 TIP 파일로 저장매체에 위치함
- 이관 요청메시지 파일에 포함되지 않으며 별도의 파일로 존재

이관 종합 정보 파일, 이관 요청메시지 파일, 이관 문서 파일이 위치한 저장매체 간의 관계를 1 : n : 1 로 표현할 수 있다.

이관 모듈은 Export 작업을 수행할 때, 저장매체의 가용 저장공간을 1/10 이상은 남겨둡으로써, 수관 공인전자문서센터가 수관 완료 후 응답메시지를 기록할 수 있도록 한다.

3.4.2.3 이관데이터 전달 방안

export가 완료된 이관매체는 물리적인 운송수단을 통해 상대방에게 전달되며, 이관 공인전자문서센터에 의해 저장매체의 입출력장치가 봉인된 형태로 전달된다. 수관 공인전자문서센터의 담당자는 이관데이터가 수록된 저장매체를 전달 받으면, 이관 공인전자문서센터의 봉인상태를 확인한 후 수신확인에 대한 확인서를 이관 공인전자문서센터로 전달한다.

3.4.2.4 수관 공인전자문서센터의 Import 절차

수관 공인전자문서센터는 저장매체를 수신하면 저장매체를 수관 모듈이 설치된 서버에 연결하고 정보를 Import한다.

Import 절차는 다음과 같으며, 각 이관요청메시지에 대한 응답메시지는 이관요청메시지별로 각각 생성되어 이관 공인전자문서센터에 전달되어야 한다.

○ Import 절차

- 이관 종합 정보 파일을 읽어 매체 내에 기록된 전체 이관 요청메시지 파일의 총 건수를 확인하고 각 파일에 대한 정보를 바탕으로 요청메시지 파일 단위로 처리를 시작한다.
- 각 요청메시지 파일의 메시지 헤더에 있는 전자서명값의 유효성을 검증함으로써 메시지에 대한 인증 및 무결성 검증을 수행한다.
- 요청메시지 내의 전자문서 단위로 TIP 파일의 위치정보 및 해쉬값 등의 속성정보를 추출한다.
- 저장매체로부터 TIP 파일을 추출하여 요청메시지에서 추출한 속성정보와 비교 검증을 수행한다.
- TIP 파일에 대하여 구조 검증, 전자서명 검증, 전자문서 해쉬값 검증, 최초등록증명서 검증 등을 수행하여 이관 대상 전자문서의 무결성을 확인한다.
- 전자문서 및 관련 정보를 수관 공인전자문서센터의 전자문서보관 구조에 맞춰 등록한다.

- 전자문서 등록이 정상적으로 완료되면, 수관 공인전자문서센터는 등록된 전자문서에 대한 등록증적으로 생성하는 한편, 수관받은 최초등록증명서를 재발급한다.
- 수관 모듈은 처리된 결과를 바탕으로 이관요청에 대한 응답메시지를 생성한다.
- 생성된 응답메시지는 이관요청메시지를 수록한 저장매체에 저장한 후, 다시 수관 공인전자문서센터의 봉인절차를 거쳐 봉인된다.
- 수관 공인전자문서센터는 봉인된 저장매체와 처리내역정보를 물리적인 운송수단을 통해 이관 공인전자문서센터에게 다시 전달한다.

3.4.3 오프라인 보안 처리 방안

오프라인으로 전달되는 이관 요청메시지 및 응답메시지에 대하여 이·수관 공인전자문서센터는 전자서명 값을 통해 상대 공인전자문서센터에 대한 인증 및 메시지의 무결성 등에 대한 기술적 검증 및 추후 부인방지 기능을 수행할 수 있어야 한다.

온라인 이·수관과는 달리 오프라인 이·수관에서는 통신 세션을 암호화할 수 없기 때문에, 이관 대상 전자문서에 대한 기밀성 보장하기 위한 방법으로 TIP에 첨부된 전자문서 자체를 암호화한 후 오프라인 이·수관 작업을 수행한다. 전자문서에 대한 기본적인 암호화 포맷은 CMS(RFC3852)의 EnvelopedData 형식을 사용하도록 하며, 이관 공인전자문서센터와 수관 공인전자문서센터 간 협의된 경우 안전한 다른 암호화 방식을 추가로 사용할 수 있다. 전자문서를 전달하기 위한 저장매체는 물리적인 침해행위를 방지하기 위하여 보안캐비닛 등으로 최대한 안전하게 보호되어야 하며, 침해 여부를 확인할 수 있도록 봉인작업이 수행되어야 한다.

단, 전자문서에 대한 암호화작업 여부는 이용자와의 합의를 통해 결정하며, 기밀성을 필요로 하는 중요 전자문서가 아닌 경우에는 처리 시간 단축을 위해 생략할 수도 있다. 이 경우 공인전자문서센터는 추후 이와 관련된 분쟁이 발생하지 않도록 이용자에게 기밀성 및 암호화와 관련된 내용을 충분히 숙지시킨 후 이에 대한 근거를 유지하여야 한다.

규격 연혁

| 버전 | 제 · 개정일 | 제 · 개정내역 |
|-------|---------------|--|
| v1.00 | 2008년 5월 9일 | · 제정 |
| v1.10 | 2009년 11월 4일 | <ul style="list-style-type: none"> · 첨부파일 갯수를 2bytes로 버그 수정 · 잘못된 어휘 삭제 · 온라인 이수관요청메시지에 대해서 동기/비동기 응답메시지가 가능하다는 내용을 명확하게 함 |
| v2.00 | 2011년 12월 30일 | <ul style="list-style-type: none"> · 전자문서 이관 시 최초등록증명서 발급여부 확인 후 미발급 시 발급하는 내용 추가 · 전자문서 수관 시 최초등록증명서 재발급 절차 및 생성 방법 추가 · TIP의 보관만료 일시 및 이관 일시에 대한 설명 보완 · 오프라인 암호화 시 기본 암호화 방식을 CMS (RFC3852)의 EnvelopedData 형식을 사용하도록 하고 공인전자문서센터 간 협의된 경우 다른 안전한 암호화 방식을 허용하는 내용 추가 |
| v2.10 | 2013년 6월 20일 | · 규격 용어 현행화 |
| v3.00 | 2014년 1월 1일 | <ul style="list-style-type: none"> · TIP 내 SIP 영역 삭제 · TIP 내 암호화 관련 필드 추가 · TIP 전자문서 무결성 검증 |