전자문서 정보패키지 기술규격

Technical Standard for Electronic Document Information Package

v3.00

2014년 1월

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

1. 규격의 개요

1.1 목적

“전자문서 정보패키지 기술규격”(이하 본 규격)은 공인전자문서센터에 보관되고 발급되는 전자문서를 정보패키지화 함으로써, 전자문서의 진본성을 유지하고 위·변조를 방지하며 이를 통해 공인전자문서센터의 신뢰성을 도모함을 그 목적으로 한다.

또한 전자문서 정보패키지의 명확하고 적절한 기술 규격화를 통해 공인전자문서센터를 기반으로 한 e-비지니스 활성화 도모 및 타 공인전자문서센터 시스템이나 외부 시스템과의 상호운용성을 높이는 것을 그 목적으로 한다.

1.2 적용 대상 및 범위

본 규격은 공인전자문서센터 시스템을 개발하고자 하는 업체(또는 기관)와 공인전자문서센터 시스템에 문서를 등록하고자 하는 업체(또는 기관)를 대상으로 한다. 또한 공인전자문서센터에 전자문서를 보관하는 과정부터 발급하는 과정까지를 본 규격의 적용 범위로 정한다.

또한 전자문서의 정보패키지는 국제표준인 ISO 14721을 근거로 하며, 공인전자문서센터의 전자문서의 관리를 위한 일련의 과정에 필요한 메타데이터 및 요건들은 국제표준인 ISO 15489와 ISO 23018을 참고로 하였다.

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

□ KCAC.TS.CERTVAL; 공인인증서 경로검증 기술규격 v1.11, 한국인터넷진흥원, 2009

□ NIPA-TS-CERTIFICATE; 전자문서 증명서 포맷 및 운용절차 기술규격 v3.00, 정보통신산업진흥원, 2013

1.4 규격 어휘

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

□ 필수 요소 : 이 규격에서 제시하는 규칙을 절대적으로 따라야 할 때 사용한다. 규격에 부합하기 위해서는 이것을 엄밀하게 따라야 하며, 이것을 벗어나는 것을 인정하지 않는다. (영문 : Must, Must Not)

- ~ 한다.
- ~ 하여야 한다.
- ~ 안된다.
- ~ 않는다.

□ 권고(선택) 요소 : 이 규격에서 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 : 규격의 입장에서 바람직하지 않지만, 반드시 금지하지 않는다. (영문 : Should Not)

- ~ 하지 않도록 한다.

□ 허용 요소 : 규격의 입장에서 허락한다는 것을 나타낸다. (영문 : May)

- ~ 할 수 있다.

2. 용어 정의

2.1 용어

1) 보존 정보패키지(Archival Information Package)란 이용자의 전자문서를 안전하게 보관하기 위하여 공인전자문서센터에서 생산한 패키지를 말한다. 보존 정보패키지는 보관을 위해 필요한 메타데이터와 첨부파일과 공인전자문서센터의 인증정보로 구성된다.

2) 배부 정보패키지(Dissemination Information Package)란 공인전자문서센터가 보관중인 전자문서의 유통을 위하여, 진본성 검증을 위한 원본증명서를 첨부한 형태로 생산하여 이용자에게 전송하는 패키지를 말한다.

3) 전자문서(Electronic Document)란 첨부파일을 묶어주는 개념적 단위를 말한다.

4) 첨부파일(File)이란 실제 내용을 담고 있는 전자적인 형태의 파일로서 정보패키지의 최소단위를 말한다.

5) 접근(Access)이란 이용자가 정보를 탐색하고, 활용하거나 검색하는 권리, 기회, 수단을 말한다.

6) 원본증명서의 정의는 “전자문서 증명서 포맷 및 운용절차 기술규격 v3.00”(이하 증명서 규격)의 정의를 따른다.

7) 불변경증명서의 정의는 증명서 규격의 정의를 따른다.

2.2 약어

1. XML : eXtensible Markup Language, 확장성 마크업 언어

2. GMT : Greenwich Mean Time, 그리니치 표준시

3. AIP : Archival Information Package, 보존 정보패키지

4. DIP : Dissemination Information Package, 배부 정보패키지

3. 전자문서 정보패키지 개요

3.1 전자문서 정보패키지의 목적

공인전자문서센터는 이용자의 전자문서를 이용자가 원하는 기간 동안 신뢰할 수 있고 안전한 방법으로 보관하는 한편 이용자의 요청에 따라 언제든지 전자문서를 열람 또는 발급해줄 수 있어야 한다. 즉, 공인전자문서센터는 전자문서의 진본성 유지, 장기 보관, 이용의 편의성 등을 보장할 수 있어야 한다.

전자문서의 진본성을 유지한다는 것은 공인전자문서센터에 보관된 전자문서가 이용자가 등록한 전자문서와 동일하며 보관기간 동안 위조 및 변조되지 않았음을 보장할 수 있다는 것이다. 이와 관련하여, 기본적으로 공인전자문서센터 자체의 신뢰성 및 업무 투명성, 책임성 등이 먼저 보장되어야 하며, 이를 기반으로 전자문서의 진본성 보장을 위한 전자문서의 보관시점 증명 및 보관기간 동안의 무결성에 대한 증명이 가능해야 한다.

또한 공인전자문서센터는 이용자의 전자문서를 이용자가 원하는 기간 동안 보관할 수 있어야 하며 이는 단기간 보관 뿐 아니라 장기적인 보관이 가능해야 함을 의미한다. 단기 보관과 달리 장기 보관의 경우는 시간의 흐름에 따른 전자적 환경의 노후화에 대처할 수 있는 기술적인 조치가 필요하다.

마지막으로 공인전자문서센터는 어떤 상황에서도 이용자에게 편리한 전자문서 서비스를 제공할 수 있어야 한다. 이를 위하여 공인전자문서센터는 전자문서와 관련된 상세 메타데이터들을 전자문서와 함께 묶어 관리해야할 필요가 있다.

상기의 요건들을 만족하기 위하여, 공인전자문서센터는 공인전자문서센터의 전자서명을 포함한 상세 메타데이터들을 전자문서와 함께 하나의 파일로 패키징한 정보패키지의 형식으로 변환하여 보관한다.

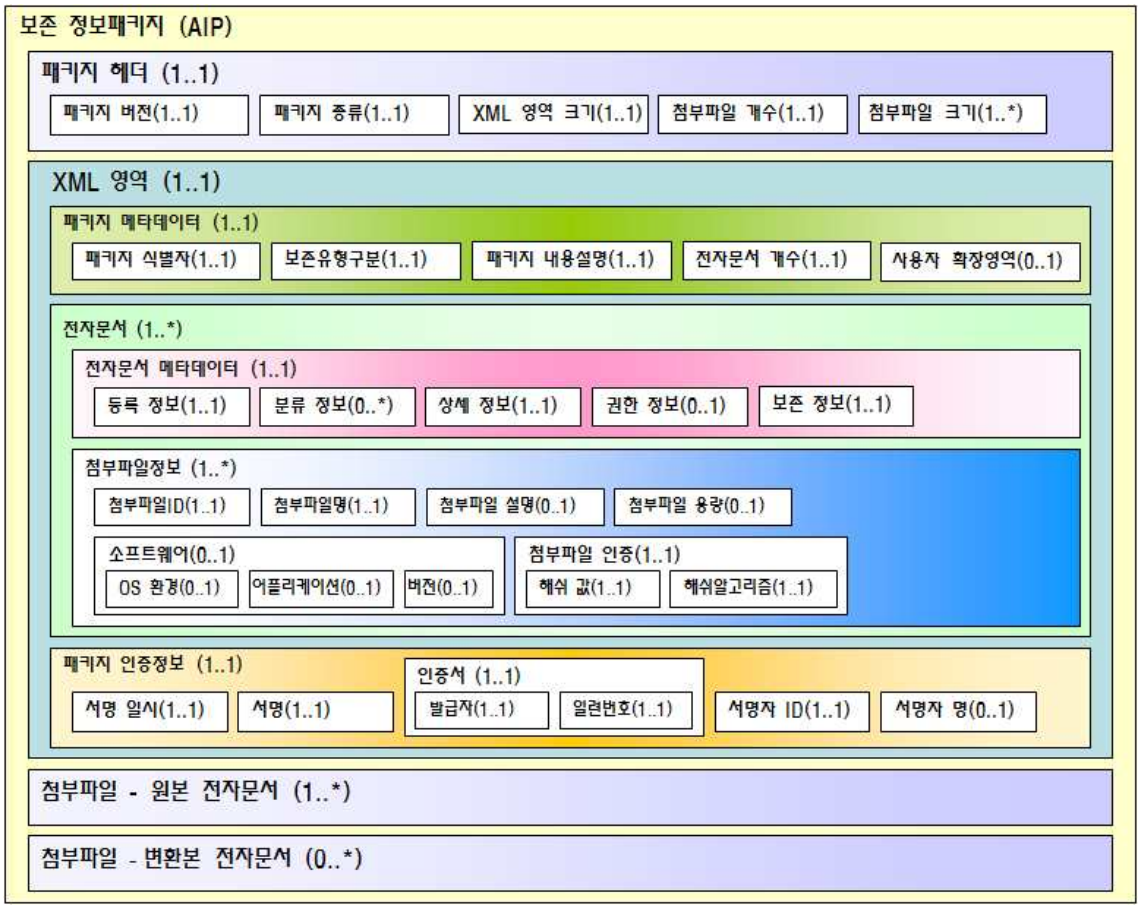
3.2 전자문서 정보패키지의 구조

정보패키지는 전자문서와 메타데이터로 구성된다. 메타데이터란 전자문서와 관련된 모든 상세 정보를 말하며, 전자문서의 내용을 비롯하여 전자문서의 생산에서부터 보관, 이용, 보관만료에 대한 정보, 그리고 정보패키지를 구성하기 위한 정보들로 이루어져 있다.

공인전자문서센터 서비스에서 사용되는 정보패키지에는 이용자의 전자문서를 공인

전자문서센터에서 보관하기 위한 보존 정보패키지(AIP)와 보관중인 전자문서를 유통하기 위한 배부 정보패키지(DIP)가 있다.

3.2.1 AIP 구조



상기의 구조를 간단히 설명하면 다음과 같다.

□ AIP는 크게 패키지 헤더, XML 영역, 첨부파일 영역이 연접된 형태로 구성되어 있다.

○ 패키지 헤더 : 정보패키지 분석을 위한 메타데이터를 기재

○ XML 영역 : 정보패키지 관리 정보가 포함된 하위 요소로 구성

○ 첨부파일 : 이용자의 원본 전자문서 및 공인전자문서센터에서 변환본을 생성한 경우 변환본 파일이 첨부됨

□ XML 영역은 패키지 메타데이터, 전자문서 영역, 패키지 인증정보로 구성되어 있다.

○ 패키지 메타데이터 : 정보패키지를 식별하고 요약 설명하는 메타데이터를 기재

○ 전자문서 영역 : 원본 전자문서 및 변환본 전자문서 관련 정보가 포함된 하위 요소로 구성 (변환본 생성 여부 및 생성 수에 따라 복수개 가능)

○ 패키지 인증정보 : 정보패키지에 대한 전자서명값 및 관련 메타데이터를 기재

□ 전자문서 영역은 전자문서 메타데이터와 첨부파일정보로 구성되어 있다.

○ 전자문서 메타데이터 : 원본 전자문서 및 변환본 전자문서에 대한 각 분야별 정보가 포함된 하위 요소로 구성

○ 첨부파일정보 : 실제 전자문서 파일들에 대한 메타데이터를 기재

□ 전자문서 메타데이터는 등록 정보, 분류 정보, 상세 정보, 권한 정보, 보존 정보로 구성되어 있다.

3.2.2 DIP 구조

상기의 구조를 간단히 설명하면 다음과 같다.

□ DIP는 크게 패키지 헤더, 첨부파일, 원본증명서 영역이 연접된 형태로 구성되어 있다.

○ 패키지 헤더 : 정보패키지 분석을 위한 메타데이터를 기재

○ 첨부파일 : 원본 전자문서 파일이 첨부됨

○ 원본증명서 : 전자문서의 진본성을 증명하기 위한 원본증명서가 첨부됨

3.3 전자문서 정보패키지 프로세스

3.3.1 전자문서 보관

일반적인 전자문서 보관 및 패키징 프로세스는 다음과 같다.

□ 이용자는 공인전자문서센터에 전자문서(들)와 함께 필수 정보 및 부가 정보를 등록한다. (필수 정보 및 부가 정보는 AIP의 메타데이터로 사용)

□ 공인전자문서센터는 이용자와 미리 협약된 경우 이용자가 등록한 전자문서 원본에 대한 변환본을 생성한다.

□ 공인전자문서센터는 전자문서 관리를 위한 메타데이터를 생성한다.

□ 공인전자문서센터는 서명 대상 데이터를 조합한 후 이에 대한 전자서명값을 생성한다.

□ 공인전자문서센터는 메타데이터와 전자서명값을 조합하여 XML 영역을 생성한다.

□ 공인전자문서센터는 패키지 헤더, XML 영역, 원본 전자문서, 변환본 전자문서를 연접하여 AIP를 생성한다.

□ 공인전자문서센터는 생성된 AIP를 안전하게 보관 후 등록증적을 생성하여 보관한다.

공인전자문서센터는 AIP 생성 시, 이용자가 등록한 전자문서 원본에 대한 변환본(장기보존본 또는 업무활용본)을 생성하여 추가할 수 있으며, 이 경우 AIP의 XML 영역 내에 원본 전자문서 영역과는 별도로 변환본 전자문서 영역을 생성하여야 한다.

전자문서 원본 파일 중 일부 파일에는 변환작업이 발생하였으나, 일부 파일이 그 자체로 변환포맷과 동일하거나 이진파일 등이어서 변환이 발생하지 않은 경우, 변환본 파일 대신 원본 파일을 그대로 순서에 맞게 포함시키도록 한다. 즉, 원본 전자문서 영역에 포함되는 첨부파일정보의 개수와 변환본 전자문서 영역에 포함되는 첨부파일정보의 개수는 동일하다.

변환본 전자문서가 생성된 경우, 첨부파일 영역에는 먼저 원본 전자문서 파일들을 첨부하고, 다음에 변환본 전자문서 파일들을 첨부하도록 한다. 만약 공인전자문서센

터 정책상 변환본 전자문서 영역이 복수 개가 생성되는 경우는 XML 영역에 기재된 변환본 전자문서 메타데이터의 순서대로 각 변환본 전자문서 파일들을 첨부하도록 한다.

변환본 중 업무활용본의 경우는 전자문서 등록 과정이 아닌 전자문서 열람 과정 중에 변환하여 이용자에게 열람 서비스를 제공할 수 있으나, 장기보존본의 경우는 반드시 전자문서 등록 과정 중에 변환하여 정보패키지에 포함하여야 한다.

3.3.2 전자문서 발급

일반적인 전자문서 발급 프로세스는 다음과 같다.

□ 이용자는 발급받고자 하는 전자문서를 선택하여 발급 요청을 한다.

□ 공인전자문서센터는 AIP의 무결성 검증 후, 원본 전자문서를 추출한다.

□ 공인전자문서센터는 추출된 원본 전자문서를 대상으로 원본증명서를 생성한다

□ 이용자가 전자문서 암호화 발급을 요청한 경우, 공인전자문서센터는 이용자가 요청한 방식으로 원본 전자문서를 암호화한다.

□ 공인전자문서센터는 패키지 헤더, 원본 전자문서, 원본증명서를 연접하여 DIP를 생성한다.

□ 공인전자문서센터는 DIP를 이용자에게 안전하게 전달 후 발급증적을 생성하여 보관한다.

□ 이용자 시스템은 발급된 DIP의 패키지 헤더 내의 메타데이터 정보를 이용하여, 연접된 원본 전자문서 및 원본증명서를 분리한다.

□ 전자문서가 암호화된 경우 이용자 시스템은 암호화 방식에 따라 복호화를 수행한다.

□ 이용자 시스템은 분리된 원본 전자문서를 해쉬하여, 원본증명서에 포함된 원본 전자문서 해쉬값과 실제로 일치하는지 비교 검증을 수행한다.

DIP를 생성하는 이유는 발급된 전자문서 유통 시 원본증명서를 이용하여 전자문서의 진본성 검증을 쉽게 수행할 수 있도록 하기 위함이다. DIP에 원본증명서가 첨부

되는 전자문서 발급 기능은 원본증명서에 포함된 원본 전자문서의 해쉬값과 발급된 전자문서의 비교 검증을 통하여, 발급된 전자문서가 이용자가 공인전자문서센터에 보관한 원본 전자문서와 동일함(진본성) 및 유통 과정 중에 위·변조가 발생하지 않았음(무결성)을 지속적으로 확인할 수 있다.

전자문서 발급 시 전자문서 내용에 대한 기밀성을 유지하기 위하여 암호화를 적용할 수 있다. 이용자는 이를 위하여 전자문서 발급 요청 시 전자문서를 암호화하기 위한 패스워드 또는 발급된 전자문서를 열람할 주체의 인증서를 공인전자문서센터에 전달하여야 한다.

암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용하되, 공개키 암호화 방법은 RecipientInfo로 KeyTransRecipientInfo 형식을, 패스워드 암호화 방법은 PasswordRecipientinfo 형식을 각각 사용하도록 하며, 암호화 대상은 전자문서 발급 포맷 내에 첨부된 각 개별 전자문서 파일들을 대상으로 한다.

이때 주의할 점은 원본증명서에 포함된 원본 전자문서의 해쉬값은 암호화되기 전 평문 상태의 원본 전자문서를 해쉬한 값이며, 발급된 DIP의 원본 전자문서에 대한 해쉬값 비교 검증 시에도 전자문서가 암호화된 상태이면 먼저 복호화를 수행한 후 해쉬값을 구하여 비교 검증을 해야 한다. 물론, 원본 전자문서를 해쉬할 때 사용되는 해쉬 알고리즘은 원본증명서에 포함된 원본 전자문서 해쉬값을 계산할 때 사용한 해쉬 알고리즘을 사용하여야 한다. 만약 DIP에 첨부된 원본 전자문서가 복수개라면 각 파일들이 순서대로 연접된 상태에서 해쉬를 수행하여야 한다.

3.3.3 전자문서 열람

전자문서 열람 기능은 원본증명서가 첨부되지 않은 채로 전자문서 원본 또는 변환본(장기보존본 또는 업무활용본)의 내용을 다양한 방식으로 이용자에게 전달하는 서비스이다.

일반적인 전자문서 열람 프로세스는 다음과 같다.

□ 이용자는 열람하고자 하는 전자문서를 선택한 후 열람 요청을 한다.

※ 공인전자문서센터의 열람 기능 구현 방식 및 공인전자문서센터와 이용자 간 협약에 따라 이용자가 열람하고자 하는 전자문서의 포맷을 스스로 선택하거나 또는 디폴트로 특정 포맷에 대한 열람만을 지원할 수도 있음

□ 공인전자문서센터는 AIP의 무결성 검증 후, 공인전자문서센터가 지원하는 열람 정책에 따라 원본 전자문서 또는 등록과정 중에 변환되어 AIP에 포함된 변환본을 추출한다.

※ 공인전자문서센터의 정책에 따라 열람과정 중에 열람을 위한 변환본을 생성하는 것도 가능함

□ 공인전자문서센터는 지원하는 열람 방식을 통하여 원본 전자문서 또는 변환본 전자문서를 이용자에게 전달한다.

공인전자문서센터 정책에 따라 원본 전자문서 및 변환본 전자문서 둘 다 열람 서비스의 대상이 될 수 있으며, 만약 공인전자문서센터에서 문서변환 서비스를 제공한다면, 해당 변환 포맷에 대하여 반드시 이용자에게 열람 서비스를 제공하여야 한다.

변환본 중 업무활용본의 경우는 전자문서 등록 과정 중에 변환본을 생성하지 않았더라도 열람 과정 중에 변환본을 생성하여 열람 서비스를 제공할 수도 있다. 이때, 생성된 변환본은 공인전자문서센터에 저장 및 재사용될 수 없음에 주의한다.

이용자가 변환본 전자문서를 열람하는 경우, 이용자는 변환본 전자문서의 내용이 원본과 동일함을 보증하는 불변경증명서 발급을 요청할 수 있다.

일반적으로 전자문서 열람은 전자문서의 내용을 확인하기 위한 일회성의 서비스로 제공되나, 공인전자문서센터가 제공하는 열람 서비스의 구현방식에 따라 열람 과정 중 변환본 전자문서 및 불변경증명서를 파일로 저장하여 유통하는 경우, 해당 변환본 전자문서 내용의 무결성 보장이 가능하다.

기본적인 메시지 보안 요건을 준수하는 범위 내에서, 공인전자문서센터는 이용자에게 다양한 방식의 열람 서비스를 제공할 수 있다.

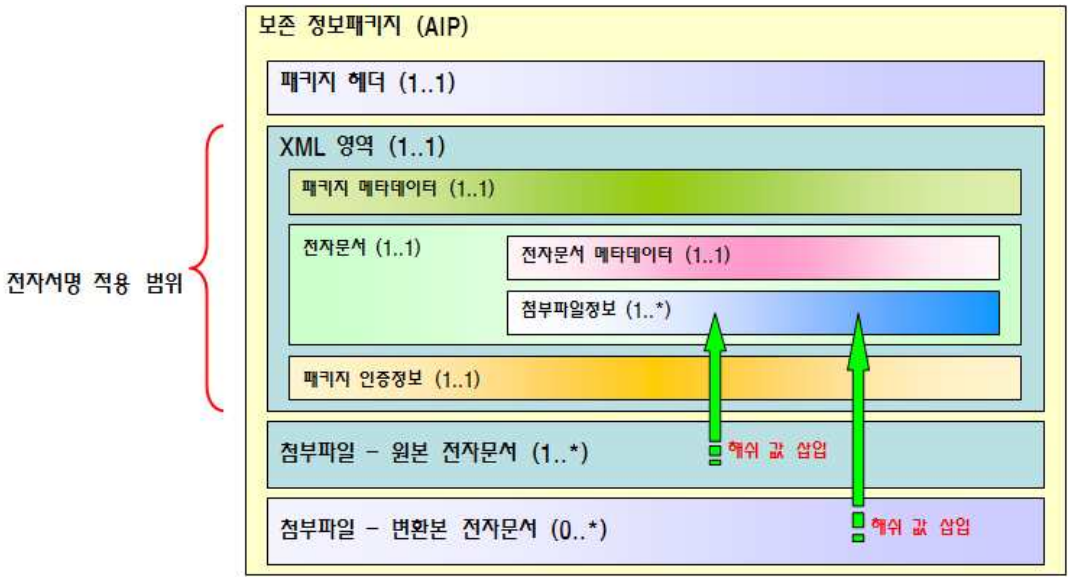
3.4 AIP 전자서명

AIP 생성 시 보관 중인 전자문서 및 메타데이터의 무결성 확보 및 AIP 생성주체에 대한 인증을 위하여 전자서명을 수행한다.

전자서명은 XML 영역에 대하여 수행하며, XML 영역 다음에 첨부되는 이용자의 원본 전자문서 및 변환본 전자문서에 대해서는 해쉬 알고리즘을 이용하여 해쉬 값을 생성한 다음 XML 영역의 메타데이터에 삽입하여 무결성을 확보하도록 한다.

전자서명 생성 방법은 XML Digital Signature의 enveloped 방식으로 하도록 한다.

이것은 XML 내 전자서명 값이 들어가는 엘리먼트를 null로 한 다음 전체에 대한 전자서명값을 생성하고 이를 엘리먼트에 삽입하는 방식이다.



4. AIP 메타데이터

4.1 AIP 메타데이터 목록

<table>
<tr><th>번호</th><th colspan="6">메타데이터 구성요소</th><th>반복수</th></tr>
<tr><td></td><td colspan="7">헤더정보(HeaderInformation)</td></tr>
<tr><td>1</td><td colspan="6">패키지 버전
(Version)</td><td>1..1</td></tr>
<tr><td>2</td><td colspan="6">패키지 종류
(Type)</td><td>1..1</td></tr>
<tr><td>3</td><td colspan="6">XML 영역 크기
(XML1Size)</td><td>1..1</td></tr>
<tr><td>4</td><td colspan="6">첨부파일 개수
(AttachFileQuantity)</td><td>1..1</td></tr>
<tr><td>5</td><td colspan="6">첨부파일 크기
(AttachFileSize)</td><td>1..*</td></tr>
<tr><td colspan="8">XML 영역(ElectronicDocumentInformationPackage)</td></tr>
<tr><td>6</td><td colspan="3" rowspan="5">패키지 메타데이터
(PackageMetaData)
(1..1)</td><td colspan="3">패키지 식별자
(PackageID)</td><td>1..1</td></tr>
<tr><td>7</td><td colspan="3">보존유형구분
(RetentionType)</td><td>1..1</td></tr>
<tr><td>8</td><td colspan="3">패키지 내용설명
(Description)</td><td>1..1</td></tr>
<tr><td>9</td><td colspan="3">전자문서 개수
(DocumentQuantity)</td><td>1..1</td></tr>
<tr><td>10</td><td colspan="3">사용자 확장 영역
(Extensions)</td><td>0..1</td></tr>
<tr><td>11</td><td rowspan="6">전자문서
(Electronic Document)
(1..1)</td><td rowspan="6">전자문서 메타데이터
(Document Metadata)
(1..1)</td><td rowspan="6">등록정보
(RegisterInfo)
(1..1)</td><td colspan="3">전자문서 식별자
(DocumentID)</td><td>1..1</td></tr>
<tr><td>12</td><td>일시
(DateTimeInfo)
(1..1)</td><td colspan="2">등록일시
(RegisterDateTime)</td><td>1..1</td></tr>
<tr><td>13</td><td rowspan="4">생산자
(ProductParty)
(1..1)</td><td rowspan="2">개인
(Person)
(1..1)</td><td>개인 ID
(PersonID)</td><td>1..1</td></tr>
<tr><td>14</td><td>개인명
(PersonName)</td><td>0..1</td></tr>
<tr><td>15</td><td rowspan="2">기관
(Organization)(0..1)</td><td>기관 ID
(OrganizationID)</td><td>1..1</td></tr>
<tr><td>16</td><td>기관명</td><td>0..1</td></tr>
</table>

						(Organizat ionName)	
17					전자메일 (ElectronicMail)		1..*
18					부서명 (DepartmentName)		0..1
19					직위명 (PositionName)		0..1
20					주소 (Address)		1..*
21					전화번호 (PhoneID)		1..*
22			분류정보 (ClassificationInfo) (0..*)	분류체계 구분 (ClassificationSchemeType)			1..1
23				분류체계ID (ClassificationSchemeID)			1..1
24				분류체계명 (ClassificationSchemeName)			0..1
25				분류코드 (ClassificationCode)			1..1
26				분류코드명 (Description)			0..1
27			상세정보 (DetailInfo) (1..1)	내용설명 (DetailDescription)			0..1
28				첨부파일 개수 (AttachFileQuantity)			1..1
29				전자문서 형태 코드 (DocumentForm)			1..1
30				제목 (Title) (1..1)	본제목 (MainTitle)		1..1
31					부제목 (SubTitle)		0..1
32				색인어 (Index) (0..*)	키워드단계 (KeywordStep)		1..1
33					키워드 (Keyword)		1..1
34				전자문서 유형(텍스트) (DocumentType)			0..1
35			권한정보 (RightsInfo) (0..1)	보안 (Security) (1..1)	보안등급 (SecurityLevel)		1..1
36					보안등급 설명 (SecurityDescription)		0..1
37			보존정보 (RetentionInfo)	보존만료일 (RetentionExpiredDate)			1..1
38				암호화	암호화 처리구분		1..1

				(Encryption) (1..1)	(EncryptionType)		
39			(1..1)		인증서 (Certificate) (0..1)	발급자 (Issuer)	1..1
40						일련번호 (Serial)	1..1
41		첨부파일정보 (AttachFileInfo) (1..*)		첨부파일ID (FileID)			1..1
42				첨부파일명 (FileName)			1..1
43				첨부파일 설명 (Description)			0..1
44				첨부파일 용량 (Volume)			0..1
45				소프트웨어 (Software) (0..1)	OS환경 (OperatingSystem)		0..1
46					어플리케이션 (Application)		0..1
47					버전 (Version)		0..1
48				첨부파일 인증 (Authentication)(1..1)	해쉬 값 (HashValue)		1..1
49					해쉬 알고리즘 (Algorithm)		1..1
50	**패키지 인증정보 (PackageAuthentication) (1..1)**			서명일시 (DateTime)			1..1
51				서명 (Signature)			1..1
52				인증서 (Certificate) (1..1)	발급자 (Issuer)		1..1
53					일련번호 (Serial)		1..1
54				서명자 ID (SignerID)			1..1
55				서명자 명 (SignerName)			0..1

4.2 메타데이터 집합 정보 유형 정의

1 패키지 메타데이터

관리번호	IP-ABIE-001
영문명	PackageMetaData
정의	패키지 전체에 대한 정보
목적	패키지의 식별정보 및 패키지에 대한 전체적인 설명을 기술
비고	---

2 등록 정보

관리번호	IP-ABIE-003
영문명	RegisterInfo
정의	전자문서 생산 및 공인전자문서센터 등록과 관련된 정보
목적	전자문서 생산자(소유자) 정보와 공인전자문서센터 등록일시를 기술
비고	---

3 분류 정보

관리번호	IP-ABIE-004
영문명	ClassificationInfo
정의	전자문서에 대한 관리 및 관련 업무를 위한 분류체계
목적	전자문서와 업무적 기능과의 관계를 기록함으로써 전자문서에 대한 관리 용이성 및 업무에서의 활용도 제고 ※ 관점에 따른 다양한 분류가 가능
비고	이용자가 스스로의 관리목적을 위해 분류정보 기재. 공인전자문서센터는 이용자가 전자문서와 함께 등록한 분류정보를 정보패키지에 추가하거나 이용자와 미리 협의된 분류정보를 추가하는 것도 가능함. 만약 분류정보가 필요없다면 분류정보 자체를 생략할 수 있음.

4 상세 정보

관리번호	IP-ABIE-005
영문명	DetailInfo
정의	패키지에 첨부된 전자문서들에 대한 구체적인 정보

목적	전자문서가 가지고 있는 특성을 요약 정의함으로써, 전자문서에 대한 효과적인 접근점을 제공
비고	---

5 권한 정보

관리번호	IP-ABIE-006
영문명	RightsInfo
정의	전자문서의 이용 및 접근을 관리하고 통제하기 위한 정보
목적	비밀 또는 비공개로 분류된 기록물의 적절한 관리를 위한 요소로서 정보객체의 보안등급, 공개여부, 열람범위 등 이용과 접근에 대한 정보를 기록하여 전자문서에 대한 불법 접근을 방지
비고	---

6 보존 정보

관리번호	IP-ABIE-007
영문명	RetentionInfo
정의	문서의 보존만료일 및 보존시 암호화 여부에 대한 정보
목적	공인전자문서센터에서의 보존기간에 대한 근거를 확보하고 보존기간 동안 전자문서에 대한 접근을 차단하는 역할을 수행
비고	---

7 첨부파일 정보

관리번호	IP-ABIE-008
영문명	AttachFileInfo
정의	생산기관 또는 개인이 생산한 첨부파일에 대한 정보
목적	개별 첨부파일에 대한 활용 정보 및 무결성 정보를 기술
비고	첨부파일 인증정보는 각각의 첨부파일에 대하여 생성하며 검증함

8 패키지 인증정보

관리번호	IP-ABIE-002
영문명	PackageAuthentication

정의	패키지의 무결성 보장을 위한 정보
목적	패키지에 첨부된 전자문서 및 메타데이터의 진본성, 무결성 입증을 가능하게 하기 위한 근거의 역할
비고	패키지에 첨부된 전자문서의 무결성값이 포함된 XML 영역에 대한 인증 및 무결성을 보장함으로써, 결과적으로 전자문서의 진본성 및 무결성을 보장함

4.3 메타데이터 기본 정보 항목 정의

① 패키지 버전

관리번호	IP-BBIE-001	영문명	Version		
정의	AIP 스키마의 버전				
사용 설명	소숫점 한자리까지만 사용하며, 본 규격을 준용한 AIP의 버전은 3.0로 기재함				
사용 사례	1.0, 1.1, 1.5, 2.0, 3.0				
반복수	1..1	타입	string	자릿수	3
코드 값 & 기본값 목록	---				
비고	---				

② 패키지 종류

관리번호	IP-BBIE-002	영문명	Type		
정의	패키지의 유형				
사용 설명	패키지의 유형을 기재하며, 본 AIP에서는 AIP로 기재함				
사용 사례	"AIP"				
반복수	1..1	타입	string	자릿수	3
코드 값 & 기본값 목록	"AIP"				
비고	AIP는 보존정보패키지를 의미함				

③ XML 영역 크기

관리번호	IP-BBIE-003	영문명	XML~~1~~Size		
정의	AIP 내 XML 영역의 크기				
사용 설명	HexaDecimal 형식을 사용하여 network byte order(big endian)로 배열				
사용 사례	1000 bytes 표현시 => 000003E8				
반복수	1..1	타입	Long Integer	자릿수	4
코드 값 & 기본값 목록	---				
비고					

④ 첨부파일 개수

관리번호	IP-BBIE-006	영문명	AttachFileQuantity		
정의	AIP에 첨부된 전자문서 파일의 전체 개수				
사용 설명	HexaDecimal 형식을 사용하여 network byte order(big endian)로 배열				
사용 사례	20 개 표현시 => 0014				
반복수	1..1	타입	Short Integer	자릿수	2
코드 값 & 기본값 목록	---				
비고	전자문서 등록과정 중 변환본이 발생한 경우 원본 및 변환본 전자문서 파일들의 총 개수를 기재				

⑤ 첨부파일의 크기

관리번호	IP-BBIE-007	영문명	AttachFileSize		
정의	AIP에 첨부된 전자문서의 크기				
사용 설명	HexaDecimal 형식을 사용하여 network byte order(big endian)로 배열				
사용 사례	1000 bytes 표현시 => 00000000000003E8				
반복수	1..*	타입	Double Integer	자릿수	8
코드 값 & 기본값 목록	---				
비고	8bytes 값의 배열 형식으로 각각의 전자문서의 크기 정보를 기재. 즉 첨부파일 개수가 10인 경우 첨부파일의 크기 정보는 10번 반복 기재됨				

⑥ 패키지 식별자

관리번호	IP-BBIE-009	영문명	PackageID		
정의	AIP의 고유 식별자 ID				
사용 설명	패키지 식별자를 사용하여 공인전자문서센터 사업자와 정보패키지 유형을 판별할 수 있도록 공인전자문서센터의 OID 활용. OID 다음의 식별자는 사업자가 자체적으로 할당. 영문과 숫자만으로 구성				
사용 사례	공인전자문서센터 사업자의 AIP 관리 OID + 사업자 할당 식별자				
반복수	1..1	타입	string	자릿수	128이하
코드 값 & 기본값 목록	---				
비고	식별자 생성 시 구분자로 사용되는 '-', '_', '.'는 허용됨				

⑦ 보존유형구분

관리번호	IP-BBIE-010	영문명	RetentionType		
정의	AIP 내 전자문서들의 보존 유형 코드				
사용 설명	AIP 내 전자문서들이 어떤 형태로 존재하는 지 유형을 기재함				
사용 사례	“01“, “03“, “04“				
반복수	1..1	타입	string	자릿수	2
코드 값 & 기본값 목록	- 원본 존재 : “01“ - 원본과 장기보존포맷 존재 : “02“ - 원본과 장기보존포맷, 업무활용포맷 존재 : “03“ - 원본과 업무활용포맷 존재 : “06“				
비고	변환포맷이 장기보존포맷인 경우는 반드시 AIP 생성 시 장기보존포맷으로 변환하여 포함하여야 하며, 업무활용포맷인 경우는 AIP 생성 시 변환하여 포함하거나 또는 열람서비스 시 변환작업을 수행하는 것도 가능함 코드값은 이전 버전의 규격에 정의된 값을 그대로 사용하였음				

⑧ 패키지내용설명

관리번호	IP-BBIE-011	영문명	Description		
정의	패키징되는 전자문서에 대한 설명				
사용 설명	AIP에 패키징된 전자문서(들)의 내용을 열람하지 않아도 어떤 전자문서에 대한 패키지인지 파악할 수 있도록 구체적인 설명을 기술				
사용 사례	“공인전자문서센터에 관리되는 전자문서 패키지마다 필요한 메타데이터 요소에 대해 정의하는 메타데이터 설명서이다.“				
반복수	1..1	타입	string	자릿수	1000이하
코드 값 & 기본값 목록	---				
비고	전자문서 본문의 내용이 본 필드에 기술될 수 있으므로 이용자에게 숙지 후 이용자가 직접 기재하도록 하며, 추후 증명서 발급 시 이용자의 선택에 의하여 증명서에 본 필드의 내용이 포함될 수 있음				

⑨ 전자문서 개수

관리번호	IP-BBIE-012	영문명	DocumentQuantity		
정의	XML 내에 포함되는 전자문서 영역의 개수				
사용 설명	XML 내에 포함된 전자문서 영역(전자문서 엘리먼트)의 개수를 기재함				
사용 사례	2				
반복수	1..1	타입	Positive Integer	자릿수	--
코드 값 & 기본값 목록	---				

비고	전자문서를 등록하는 과정 중 변환본이 생성되지 않아 원본 전자문서만 존재한다면 1을 기재하고, 변환본이 생성되었다면 생성된 변환본의 전자문서 엘리먼트의 개수만큼 더하여 기재 원본 전자문서 엘리먼트 개수(1) + 변환본 전자문서 엘리먼트 개수

⑩ 사용자 확장 영역

관리번호	IP-BBIE-015	**영문명**	Extensions		
정의	본 규격에서 제시한 메타데이터 이외에 이용자가 추가적인 서비스에 활용하기 위해 자체적으로 규정하는 영역				
사용 설명	확장 영역 하위에 어떠한 메타데이터가 와도 상관없음				
사용 사례	---				
반복수	0..1	**타입**		**자릿수**	---
코드 값 & 기본값 목록	---				
비고					

⑪ 전자문서 식별자

관리번호	IP-BBIE-016	**영문명**	DocumentID		
정의	전자문서 영역(전자문서 엘리먼트)의 고유 식별자 ID				
사용 설명	XML 내에서 전자문서 영역을 식별하기 위한 식별자로서, 공인전자문서센터에서 임의로 부여 가능. 영문과 숫자만으로 구성				
사용 사례	"생산기관 시스템 OID+생산기관 시스템 할당 식별자" "0000000001"				
반복수	AIP : 1..1	**타입**	string	**자릿수**	128이하
코드 값 & 기본값 목록	---				
비고	식별자 생성 시 구분자로 사용되는 '-', '_', '.'는 허용됨				

⑫ 등록일시

관리번호	IP-BBIE-018	**영문명**	RegisterDateTime		
정의	이용자가 등록한 전자문서를 공인전자문서센터에서 AIP로 생성하여 저장한 일시				
사용 설명	공인전자문서센터에서 이용자의 전자문서를 AIP로 생성하여 저장한 시각을 GMT 형식으로 기재				
사용 사례	"YYYY-MM-DDThh:mm:ss" + "Z"				
반복수	1..1	**타입**	datetime	**자릿수**	20

코드 값 & 기본값 목록	--
비고	의미적으로는 AIP를 생성 및 저장 완료한 시각으로서 AIP 서명일시보다 미래이나, 기능적으로는 AIP의 각 메타데이터를 먼저 구성한 후 전자서명을 수행하기 때문에 AIP 서명일시보다 과거임. 따라서 혼란을 방지하기 위해서 AIP 서명일시와 동일한 시각값을 설정. 증명서 규격에 정의된 등록증적의 OpTime 필드에 설정된 시각값과 동일한 값이 설정되어야 함

⑬ 생산자 - 개인ID

관리번호	IP-BBIE-022	**영문명**	PersonID		
정의	전자문서 생산자 또는 소유자의 개인 고유 식별자				
사용 설명	등록되는 전자문서에 대한 모든 권한을 가지고 있는 공인전자문서센터 서비스 이용자 ID를 기재				
사용 사례	“hongkil09“				
반복수	1..1	**타입**	string	**자릿수**	12이하
코드 값 & 기본값 목록	--				
비고	전자문서의 소유자로서 공인전자문서센터 서비스의 실제 이용자 정보를 기재 이용자가 자신의 전자문서를 직접 등록하는 경우는 해당 이용자의 ID를 기재하며, 이용자로부터 등록권한을 위임받은 제3자가 대행 등록하는 경우, 대행등록자의 ID가 아닌 실제 전자문서의 소유자인 이용자의 ID를 기재해야함에 주의할 것				

⑭ 생산자 - 개인명

관리번호	IP-BBIE-023	**영문명**	PersonName		
정의	전자문서 생산자 또는 소유자의 이름				
사용 설명	등록되는 전자문서에 대한 모든 권한을 가지고 있는 공인전자문서센터 서비스 이용자의 이름을 기재				
사용 사례	“홍길동“				
반복수	0..1	**타입**	string	**자릿수**	128이하
코드 값 & 기본값 목록	---				
비고	---				

⑮ 생산자 - 기관ID

관리번호	IP-BBIE-024	영문명	OrganizationID		
정의	생산자가 속한 기관의 식별자				
사용 설명	이용자 정보등록 시 등록된 기관의 식별자를 기재함				
사용 사례	“kisa“				
반복수	1..1	타입	string	자릿수	20이하
코드 값 & 기본값 목록					
비고					

⑯ 생산자 -기관명

관리번호	IP-BBIE-025	영문명	OrganizationName		
정의	생산자가 속한 기관의 이름				
사용 설명	이용자 정보등록 시 등록된 기관의 이름을 기재함				
사용 사례	“한국인터넷진흥원”				
반복수	0..1	타입	string	자릿수	255이하
코드 값 & 기본값 목록	---				
비고	기관명은 반드시 fulltext로 입력				

⑰ 생산자 - 전자메일

관리번호	IP-BBIE-026	영문명	ElectronicMail		
정의	생산자의 이메일 주소				
사용 설명	이용자 정보등록 시 등록된 이메일 주소는 반드시 기재하며 추가 할 수 있음				
사용 사례	- 기관 이메일주소 : admin@kisa.kr - 개인 이메일주소 : person@kisa.kr				
반복수	1..*	타입	string	자릿수	128이하
코드 값 & 기본값 목록	이메일 주소는 1개 이상을 기재하여야 함				
비고	이메일 주소를 2개 기입한다면, 기관 이메일 주소를 먼저 기재				

⑱ 생산자 - 부서명

관리번호	IP-BBIE-027	영문명	DeparmentName
정의	생산자가 속한 부서의 이름		

사용 설명	생산자가 속한 부서명을 기재하며 생략 가능함				
사용 사례	“전략기획팀“				
반복수	0..1	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	---				

⑲ 생산자 - 직위명

관리번호	IP-BBIE-028	영문명	PositionName		
정의	생산자의 직위명				
사용 설명	생산자가 속한 기관에서의 직위명을 기재하며 생략 가능함				
사용 사례	“팀장”, “연구원”				
반복수	0..1	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	---				

⑳ 생산자 - 주소

관리번호	IP-BBIE-029	영문명	Address		
정의	생산자 개인 또는 기관이 위치한 행정구역상의 주소				
사용 설명	이용자 정보등록 시 등록된 주소 정보를 기재. 개인 또는 기관의 주소를 1개 이상 기재. 기관의 주소가 있을 경우에는 기관의 주소를 우선 기재				
사용 사례	“서울시 마포구 성산동 277-33 문정빌딩 3층“				
반복수	1..*	타입	string	자릿수	512이하
코드 값 & 기본값 목록	---				
비고	주소를 2개 기입한다면, 기관 주소를 먼저 기재				

㉑ 생산자 - 전화번호

관리번호	IP-BBIE-030	영문명	PhoneID
정의	생산자 개인 또는 기관의 전화번호		
사용 설명	개인의 모바일폰이나 기관의 전화번호 등에서 하나 이상을 기재함. 기관 전화번호를 먼저 기재하도록 함		
사용 사례	“02-0000-0000“		

반복수	1..*	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	전화번호를 2개 기입한다면, 기관 전화번호를 먼저 기재				

㉒ 분류체계 구분

관리번호	IP-BBIE-060	영문명	ClassificationSchemeType		
정의	AIP에 적용하고자 하는 분류 체계에 대한 유형 구분자				
사용 설명	분류 체계가 공인전자문서센터에서 정의되어 있는 분류체계인지, 이용자가 자체 정의한 분류체계인지를 구분하는 지시자를 선택				
사용 사례	“0”				
반복수	1..1	타입	string	자릿수	1
코드 값 & 기본값 목록	- 이용자 정의 : “0” - 공인전자문서센터 정의 : “1” - 산업별 표준분류체계 : “2”				
비고	분류정보를 사용하지 않는 경우는 분류정보 필드 전체를 생략하도록 함. 이용자 정의인 경우는 전자문서 등록 시 이용자로부터 입력받거나 사전에 이용자와 공인전자문서센터 간에 협의된 분류정보를 기재할 수도 있음. 또한 이와 상관없이 공인전자문서센터의 자체적인 관리목적상의 분류정보를 추가 입력할 수도 있음. 만약 분류정보가 필요없다면 분류정보 필드 전체를 생략할 수 있음				

㉓ 분류체계 ID

관리번호	IP-BBIE-061	영문명	ClassificationSchemeID		
정의	AIP에 적용하고자 하는 분류 체계의 식별자				
사용 설명	공인전자문서센터가 분류 체계를 운영하는 경우, 분류 체계를 식별할 수 있는 식별자를 기재. 산업별 표준분류체계의 경우는 해당 분류체계의 ID가 있으면 해당 ID를, 없으면 분류체계를 제정한 기관의 ID를 기재하면 됨. 만약 공인전자문서센터가 자체 정의하거나 이용자가 자체 정의한 분류체계인 경우, 공인전자문서센터의 OID를 기재하거나 이용자의 ID를 기재하는 것을 권고함. 분류정보가 존재하면 반드시 생성				
사용 사례	“KSIC” “200032”				
반복수	1..1	타입	string	자릿수	50이하
코드 값 & 기본값 목록	---				
비고	분류체계구분 값이 “0”일 경우는 이용자 ID를, “1”일 경우 공인전자문서센터 OID를, ”2”일 경우는 표준분류체계 ID 또는 제정기관 ID(또는 약자 등)를 기재				

㉔ 분류체계명

관리번호	IP-BBIE-062	영문명	ClassificationSchemeName		
정의	AIP에 적용하고자 하는 분류 체계에 대한 이름				
사용 설명	분류체계 ID에 대한 이름을 기재함. 위 분류체계 ID와 마찬가지로 표준 분류체계인 경우 해당 분류체계명이나 제정기관명을 기재하면 됨. 만약 공인전자문서센터가 자체 정의하거나 이용자가 자체 정의한 분류체계인 경우, 공인전자문서센터의 명이나 이용자의 명을 기재하는 것을 권고함. 선택적 생성 가능.				
사용 사례	“한국표준산업분류” “한국인터넷진흥원”				
반복수	0..1	타입	string	자릿수	128이하
코드 값 & 기본값 목록	---				
비고	분류체계구분 값이 “0“일 경우는 이용자명을, “1“일 경우 공인전자문서센터명을, ”2“일 경우는 표준분류체계명 또는 제정기관명을 기재				

㉕ 분류코드

관리번호	IP-BBIE-063	영문명	ClassificationCode		
정의	전자문서가 속한 분류 영역의 고유값				
사용 설명	분류체계 내에서 해당 분류 영역을 식별할 수 있는 고유 값을 기재				
사용 사례	“1145“, ”01-02-03“				
반복수	1..1	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	분류코드는 각 분류체계에서 해당 분류 영역을 식별할 수 있는 고유값이며 분류코드의 형식을 제한하지는 않음 이용자 분류체계의 경우, 이용자가 직접 코드를 기재할 수도 있지만, 이용자가 분류코드 명을 입력 시 공인전자문서센터 시스템 내에서 해당 분류코드 명에 대응하는 고유의 분류코드를 자동으로 생성하는 것도 가능함				

㉖ 분류코드 명

관리번호	IP-BBIE-064	영문명	Description		
정의	분류코드의 명칭				
사용 설명	분류코드의 이름으로서, 해당 분류영역에 대한 직관적인 명칭을 사용				
사용 사례	“계약서”, “경영-회계-지급결의”				
반복수	AIP : 0..1	타입	string	자릿수	128이하
코드 값 &	---				

기본값 목록	
비고	이용자 분류체계인 경우 이용자가 기재함

㉗ 내용설명

관리번호	IP-BBIE-065	영문명	DetailDescription		
정의	전자문서에 대한 설명				
사용 설명	전자문서에 대하여 보다 상세한 내용을 기술할 필요가 있다면 기술				
사용 사례	---				
반복수	0..1	타입	string	자릿수	1000이하
코드 값 & 기본값 목록	---				
비고	전자문서 본문의 내용이 본 필드에 기술될 수 있으므로 이용자에게 숙지 후 이용자가 직접 기재할 것				

㉘ 첨부파일 개수

관리번호	IP-BBIE-066	영문명	AttachFileQuantity		
정의	원본 또는 변환본 전자문서를 구성하는 각 첨부파일 개수				
사용 설명	각 전자문서 영역 내에 포함된 첨부파일의 개수를 각각 기재. 이용자가 직접 기재하지 않고 프로그램에서 자동 부여				
사용 사례	4				
반복수	1..1	타입	Positive Integer	자릿수	---
코드 값 & 기본값 목록	---				
비고	AIP에 원본 및 변환본이 존재하는 경우, 첨부된 원본 파일 개수와 변환본 파일 개수를 각각의 전자문서의 첨부파일 개수로 기재				

㉙ 전자문서 형태 코드

관리번호	IP-BBIE-067	영문명	DocumentForm		
정의	전자문서가 원본 전자문서인지, 장기보존 포맷 또는 업무활용 포맷의 전자문서인지 구분해주는 정보				
사용 설명	변환되지 않았다면 “0”을, 변환되었다면 각 포맷에 따른 값을 부여				
사용 사례	“0“, “1“, “2“				
반복수	1..1	타입	string	자릿수	1
코드 값 & 기본값 목록	- “0“ : 원본 포맷의 전자문서 - “1“ : 장기보존 포맷의 전자문서 - “2“ : 업무활용 포맷의 전자문서				

비고	변환이 이루어지지 않은 전자문서는 포맷에 상관없이 반드시 “0” (원본 포맷) 값을 사용해야 함. 변환본인 경우 변환의 목적에 따라, 먼 미래에도 열람할 수 있기 위한 장기보존용 포맷이라면 “1” 값을, 현시점에서의 열람 등 여러 가지 목적을 위한 업무활용 포맷이라면 “2” 값을 각각 구분하여 설정하도록 한다. 장기보존 포맷으로의 변환은 반드시 AIP 생성 시 수행되어 AIP에 포함되어야 하며, 업무활용 포맷은 AIP 생성 시 변환이 수행되어 AIP에 포함될 수도 있지만, AIP에는 원본만 보관하다가 이용자의 열람요청 시 변환하여 이용자에게 전달하는 것도 가능함

㉚ 제목 - 본제목

관리번호	IP-BBIE-068	**영문명**	MainTitle		
정의	정보의 내용을 대표할 수 있는 문구				
사용 설명					
사용 사례	“전자문서 정보패키지 기술규격 개발 보고서” “전자문서 정보패키지 메타데이터 요소”				
반복수	1..1	**타입**	string	**자릿수**	128이하
코드 값 & 기본값 목록	---				
비고	---				

㉛ 제목- 부제목

관리번호	IP-BBIE-069	**영문명**	SubTitle		
정의	본제목 외에 참고할 수 있는 문구				
사용 설명	각각의 정보에 본 제목 외에 이를 잘 표현할 수 있는 2차 제목을 기재				
사용 사례	---				
반복수	0..1	**타입**	string	**자릿수**	128이하
코드 값 & 기본값 목록	---				
비고	필요 시 기재				

㉜ 색인어 - 키워드 단계

관리번호	IP-BBIE-070	**영문명**	KeywordStep
정의	전자문서에 대한 키워드의 차수(등급)		
사용 설명	키워드 단계는 제시된 키워드들의 중요도에 따른 등급을 입력		
사용 사례	“1”, “2”		

반복수	1..1	타입	string	자릿수	1
코드 값 & 기본값 목록	---				
비고	키워드들에 등급을 부여할 필요가 있는 경우, 등급에 따라 분류한 후 해당 등급을 기재. 키워드 단계는 “1”(최고 등급)부터 기술(등급구분이 필요 없는 경우 “1”을 사용)				

㉝ 색인어 - 키워드

관리번호	IP-BBIE-071	영문명	Keyword		
정의	전자문서의 내용을 대표할 수 있는 주제어				
사용 설명	색인어는 전자문서에 대한 검색을 용이하게 하기 위해 필요한 단어(명사)로 기술				
사용 사례	“공인전자문서센터”, “기술규격”				
반복수	1..1	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	키워드 단계에 따라 분류된 키워드를 기재				

㉞ 전자문서 유형 (텍스트)

관리번호	IP-BBIE-072	영문명	DocumentType		
정의	전자문서의 분류 유형				
사용 설명	전자문서의 유형을 분류하여 기재한 텍스트				
사용 사례	“계약서“, “전표“				
반복수	0..1	타입	string	자릿수	35이하
코드 값 & 기본값 목록	---				
비고	---				

㉟ 보안 - 보안등급

관리번호	IP-BBIE-074	영문명	SecurityLevel		
정의	전자문서에 대한 이용 및 접근을 관리하고 통제하기 위한 코드				
사용 설명	공인전자문서센터의 정책상 보안 등급을 설정하여 전자문서에 대한 이용자의 이용 및 접근을 통제하기 위함				
사용 사례	“1“				
반복수	1..1	타입	string	자릿수	3이하

코드 값 & 기본값 목록	- 1급비밀 : “1“ - 2급비밀 : “2“ - 3급비밀 : “3“ - 대외비 : “4“ - 일반 : “5“ - 기타 : “9“
비고	설정된 보안등급은 공인전자문서센터에 보관된 전자문서에 대한 이용자 접근통제로 사용되며, 이용자의 전자문서에 대한 운영자 접근통제 수단은 아님

㊱ 보안 - 보안등급 설명

관리번호	IP-BBIE-075	**영문명**	SecurityDescription		
정의	보안등급에 대한 추가 정보				
사용 설명	보안등급에 대한 상세 설명을 기술				
사용 사례	“내규에 의해서 일반문서로 분류한다. 일반인이 이용을 요청할 때 모든 부분을 제공할 수 있다.”				
반복수	0..1	**타입**	string	**자릿수**	255이하
코드 값 & 기본값 목록	---				
비고					

㊲ 보존만료일

관리번호	IP-BBIE-081	**영문명**	RetentionExpiredDate		
정의	AIP 최대 보관 기간 만료일				
사용 설명	AIP의 최대 보관 기간 만료 일시를 GMT 형식으로 기재함				
사용 사례	“YYYY-MM-DDThh:mm:ss“ + ”Z"				
반복수	1..1	**타입**	datetime	**자릿수**	20
코드 값 & 기본값 목록	---				
비고	전자문서 등록 시 이용자가 설정하거나 또는 이용자와 공인전자문서센터 간 사전에 협의된 내용이 있다면 해당 내용을 적용 이용자의 전자문서가 실제 공인전자문서센터에 보관되는 기간, 즉 문서보관 시스템에 설정되는 보관만료 일시는 본 필드에 설정된 보존만료일 내에서 이용자와 공인전자문서센터 간 협의된 내용에 따라 설정하도록 하며, 보존만료일 내에서 보관 기간의 연장도 가능함. 문서보관 시스템에서의 보관 기간을 연장하는 경우 본 필드에 설정된 보존만료일을 경과할 수 없으므로, 보관기간의 연장이 예상되는 문서를 등록시 본 필드에 설정하는 보존만료일을 충분히 여유있게 설정하도록 함 만약 전자문서 등록 시 이용자가 설정한 보존만료일이 공인전자문서센				

	터의 정책에 위배되는 경우 해당 사유에 대한 문서등록 오류를 리턴하도록 함

㊳ 암호화 - 암호화 처리구분

관리번호	IP-BBIE-082	영문명	EncryptionType		
정의	AIP의 전자문서 첨부파일에 대한 공개키 암호화 여부 지시자				
사용 설명	AIP의 전자문서 첨부파일에 대한 공인전자문서센터의 인증서(공개키) 암호화 적용여부를 지시하는 정보임				
사용 사례	"1"				
반복수	1..1	타입	string	자릿수	1
코드 값 & 기본값 목록	- 공개키 암호화 적용 : "1" - 암호화 미적용 : "0"				
비고	공개키 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용함				

㊴ 암호화 - 인증서 - 발급자

관리번호	IP-BBIE-083	영문명	Issuer		
정의	AIP의 전자문서 첨부파일을 공개키 암호화 하였을 때 공인전자문서센터 인증서의 발급자 정보				
사용 설명	AIP의 전자문서 첨부파일을 공개키 암호화 하였을 때 공인전자문서센터 인증서의 DN을 기재함				
사용 사례	"CN=CA,OU=AccreditedCA,O=KoreaCertificateAuthority,C=KR"				
반복수	1..1	타입	string	자릿수	300이하
코드 값 & 기본값 목록	---				
비고	RFC2253의 "LDAP-DN" 포맷을 준수하여야 하며, CN, OU, O, C 의 순서로 배열한다. 공개키 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용함				

㊵ 암호화 - 인증서 - 일련번호

관리번호	IP-BBIE-084	영문명	Serial		
정의	AIP의 전자문서 첨부파일을 공개키 암호화 하였을 때 공인전자문서센터 인증서의 일련번호				
사용 설명	AIP의 전자문서 첨부파일을 공개키 암호화 하였을 때 공인전자문서센터 인증서의 일련번호를 기재함				
사용 사례	"036a481d"				
반복수	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. 공개키 암호화 방법은 CMS(RFC3852)의 EnvelopedData 형식을 준용함

㊶ 첨부파일 ID

관리번호	IP-BBIE-085	영문명	FileID		
정의	전자문서 파일의 고유 식별자ID				
사용 설명	전자문서 영역 내에서 전자문서 파일을 식별할 수 있는 값으로 생성				
사용 사례	---				
반복수	1..1	타입	string	자릿수	128이하
코드 값 & 기본값 목록	---				
비고	첨부파일 ID는 원본 또는 변환본 등의 전자문서 영역 내에서 해당 첨부파일을 식별할 수 있도록 유일하면 됨				

㊷ 첨부파일명

관리번호	IP-BBIE-086	영문명	FileName		
정의	확장자가 포함된 첨부파일명				
사용 설명	첨부파일 생산기관(또는 개인)이 부여한 파일명을 그대로 사용				
사용 사례	“전자문서 정보패키지 기술규격.hwp“, "전자문서 정보패키지 기술규격.pdf"				
반복수	1..1	타입	string	자릿수	128이하
코드 값 & 기본값 목록	---				
비고	확장자를 포함한 full name을 기술. 변환본의 경우는 원본 파일명에서 확장자만 변환포맷의 확장자로 변경하여 사용				

㊸ 첨부파일 설명

관리번호	IP-BBIE-088	영문명	Description		
정의	첨부 파일에 대한 설명				
사용 설명	첨부 파일에 대한 설명이 필요한 경우 기술				
사용 사례	---				
반복수	0..1	타입	string	자릿수	256이하
코드 값 & 기본값 목록	---				
비고	개별 첨부파일에 대한 설명이 필요한 경우 이용자가 직접 기술				

㊹ 첨부파일 용량

관리번호	IP-BBIE-089	영문명	Volume		
정의	첨부 파일의 크기에 대한 정보				
사용 설명	첨부 파일의 크기 정보를 기재				
사용 사례	12345, 234356385				
반복수	0..1	타입	Positive Integer	자릿수	---
코드 값 & 기본값 목록	---				
비고	첨부파일의 크기는 Byte 단위로 기재				

㊺ 소프트웨어 - OS환경

관리번호	IP-BBIE-092	영문명	OperatingSystem		
정의	전자문서 생성 시의 시스템 환경에 대한 정보				
사용 설명	전자문서가 생성되었던 장비에 설치된 OS를 기재				
사용 사례	“MacOS X 10.6“, “Window XP Professional(한글)“				
반복수	0..1	타입	string	자릿수	50이하
코드 값 & 기본값 목록					
비고	전자문서 활용 시 도움이 되도록 최대한 상세한 OS 정보를 기재				

㊻ 소프트웨어 - 어플리케이션

관리번호	IP-BBIE-093	영문명	Application		
정의	전자문서 생성에 사용되었거나 열람이 가능한 어플리케이션 정보				
사용 설명	원본 전자문서인 경우는 생성에 사용된 어플리케이션 정보를 변환본 전자문서인 경우는 열람을 지원하는 어플리케이션 정보를 기재				
사용 사례	“한글 2005:”, “엑셀 2003”, "acrobat reader“				
반복수	0..1	타입	string	자릿수	50이하
코드 값 & 기본값 목록	---				
비고	전자문서 활용 시 알맞은 뷰어 또는 에디터를 찾기 위한 정보임				

㊼ 소프트웨어 - 버전

관리번호	IP-BBIE-094	영문명	Version		
정의	어플리케이션의 버전 정보				
사용 설명	생산에 이용된 어플리케이션 또는 열람본 뷰어에 대한 버전 정보를 기재함				
사용 사례	“6.7.7.1023“				
반복수	0..1	타입	string	자릿수	17이하
코드 값 & 기본값 목록	---				
비고	필요 시 어플리케이션에 대한 자세한 버전 정보 기재하도록 하며, 열람본 뷰어의 경우 뷰어 버전에 따라 열람 가능 여부가 결정된다면 반드시 기재				

㊽ 첨부파일 인증 - 해쉬 값

관리번호	IP-BBIE-095	영문명	HashValue		
정의	첨부하여 삽입한 이진 파일에 대한 해쉬 값에 대한 정보				
사용 설명	패키지에 최종적으로 첨부된 이진 파일에 대하여 해쉬 알고리즘을 통하여 산출된 해쉬 값을 삽입				
사용 사례	“dWamo4egDmazsgTDmh5shgf0xbQ=“				
반복수	1..1	타입	string	자릿수	100이하
코드 값 & 기본값 목록	---				
비고	binary 해쉬 값을 RFC1341의 Base64Encoding 규칙을 준수하여 변환한 후 설정한다. Base64Encoding 시 Base64 치환 테이블에 정의된 문자만을 사용하여야 하며, 개행문자나 공백문자 등은 사용할 수 없음. 본 필드값에 대한 비교 검증을 수행하거나, 본 필드값을 다른 연산의 입력값으로 사용하는 경우, Base64Encoding 규칙을 준수하여 생성되었음을 먼저 확인하도록 한다. 이때 규칙 준수 여부에 대한 확인은 Encoding에 사용된 문자 준수 여부 및 패딩규칙 준수 여부로 한정하며, 신뢰하는 원본 데이터와의 비교검증을 의미하지는 않음 본 해쉬 값은 패키지에 연접된 첨부파일들에 대한 무결성 검사에 사용되므로, 전자문서 파일이 암호화되어 첨부되었다면, 암호화된 파일을 해쉬하여야 함에 주의				

㊾ 첨부파일 인증 - 해쉬 알고리즘

관리번호	IP-BBIE-096	영문명	Algorithm
정의	첨부파일에 대하여 해쉬를 하는 경우에 해쉬 알고리즘에 대한 정보		
사용 설명	적용한 해쉬 알고리즘에 대한 식별자를 기재		
사용 사례	"sha1", "sha256“		

반복수	1..1	타입	string	자릿수	100이하
코드 값 & 기본값 목록	---				
비고	사용되는 해쉬 알고리즘의 종류를 본 규격에서는 규정하지 않으며, 알고리즘의 안전성 등을 고려하여 평가지침 등에서 규정한 알고리즘을 사용				

⑤⓪ 패키지 인증 - 서명일시

관리번호	IP-BBIE-097	영문명	DateTime		
정의	패키지 전체에 대해서 서명을 실행한 일시				
사용 설명	패키지에 대해서 서명을 실행한 일시를 GMT 형식으로 기재함				
사용 사례	“YYYY-MM-DDThh:mm:ss“ + "Z"				
반복수	1..1	타입	datetime	자릿수	20
코드 값 & 기본값 목록	---				
비고	---				

⑤① 패키지 인증- 서명

관리번호	IP-BBIE-098	영문명	Signature		
정의	패키지에 대한 전자서명				
사용 설명	패키지 전체에 대한 전자서명 정보로서 W3C “XML-Signature Syntax and Processing“ (RFC3275)의 enveloped signature 포맷을 준수하여 생성함				
사용 사례	---				
반복수	1..1	타입	string	자릿수	5000이하
코드 값 & 본값 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 함				

⑤② 인증서 - 발급자

관리번호	IP-BBIE-099	영문명	Issuer
정의	패키지에 전자서명을 적용한 인증서의 발급자 정보		
사용 설명	패키지에 전자서명을 적용한 인증서의 발급자 DN을 기재		

사용 사례	"CN=CA,OU=AccreditedCA,O=KoreaCertificateAuthority,C=KR"				
반복수	1..1	타입	string	자릿수	300이하
코드 값 & 기본값 목록	---				
비고	RFC2253의 "LDAP-DN" 포맷을 준수하여야 하며, CN, OU, O, C 의 순서로 배열				

㊸ 인증서 - 일련번호

관리번호	IP-BBIE-100	영문명	Serial		
정의	패키지에 전자서명을 적용한 인증서의 일련번호				
사용 설명	패키지에 전자서명을 적용한 인증서의 일련번호를 기재				
사용 사례	"036a481d"				
반복수	1..1	타입	string	자릿수	50이하
코드 값 & 기본값 목록	---				
비고	HexaDecimal의 string 형식으로 표현하도록 하며 string의 자리수가 홀수인 경우는 앞에 "0"을 추가				

㊹ 서명 - 서명자 ID

관리번호	IP-BBIE-101	영문명	SignerID		
정의	서명 행위자의 식별자				
사용 설명	서명 행위에 대한 서명자의 고유 식별자를 기재				
사용 사례	---				
반복수	1..1	타입	string	자릿수	12이하
코드 값 & 기본값 목록	---				
비고	정보의 진본성을 입증하기 위한 행위가 일어날 때마다 이 요소도 함께 생성됨				

㊺ 서명 - 서명자 명

관리번호	IP-BBIE-102	영문명	SignerName
정의	서명 행위자의 이름		
사용 설명	서명 행위에 대한 서명자의 이름을 기재		
사용 사례	---		

반복수	0..1	타입	string	자릿수	128이하
코드 값 & 기본값 목록	---				
비고	---				

5. DIP 메타데이터

5.1 DIP 메타데이터 목록

AIP와 달리 DIP는 XML 영역이 존재하지 않아 패키지 헤더 다음에 바로 전자문서 및 원본증명서가 첨부되는 구조이기 때문에, DIP의 메타데이터는 첨부된 각 전자문서와 원본증명서를 분리해 내기 위한 헤더정보로만 구성된다.

헤더에 기재되는 메타데이터의 목록 및 정의는 다음과 같다.

번호	메타데이터	유형	반복수	비 고
	헤더정보(HeaderInformation)			
1	패키지 버전 (Version)	string(3bytes)	1..1	본 버전의 규격을 준용한 DIP의 버전은 “3.0”으로 기재함
2	패키지 종류 (Type)	string(3bytes)	1..1	“DIP”로 기재
3	암호화 방식 (EncryptionType)	string(1byte)	1..1	- 공개키 암호화 적용 : “1“ - 패스워드 암호화 적용 : “2” - 암호화 미적용 : “0“
4	첨부파일 개수 (AttachFileQuantity)	short(2bytes)	1..1	- HexaDecimal을 사용하여 network byte order(big endian)로 배열 예) 20 개 표현시 => 0014
5	첨부파일 크기 (AttachFileSize)	double(8bytes)	1..*	- HexaDecimal을 사용하여 network byte order(big endian)로 배열 예) 1000 bytes 표현시 => 00000000000003E8
6	원본증명서 크기 (CertificateSize)	long(4bytes)	1..1	- HexaDecimal을 사용하여 network byte order(big endian)로 배열. 예) 1000 bytes 표현시 => 000003E8

6. 전자문서 정보패키지 검증

본 장에서는 전자문서 정보패키지 이용 시 이용 주체가 정보패키지에 대한 오류 및 보안침해 여부를 확인할 수 있도록 하기 위하여, 전자문서 정보패키지 검증 방법을 제시한다.

전자문서 정보패키지 검증은 편의상 구조 검증, 무결성 검증, 내용 검증으로 구분된다.

6.1 구조 검증

정보패키지의 구조 검증은, 검증 대상인 정보패키지가 본 규격에서 정의하고 있는 정보패키지의 구조와 각 요소의 type 및 값의 제약 범위 등을 준수하고 있음을 확인하는 작업이다.

검증 시스템은 정보패키지의 구조 검증 시, 정보패키지의 스키마를 참조하여 검증 대상인 정보패키지가 해당 스키마를 준수하는가의 여부를 검증하면 된다.

만약 정보패키지의 구조 검증이 실패한다면, 검증 시스템은 해당 오류의 원인을 정보패키지의 이용 주체에게 출력하도록 하고, 정보패키지의 이용 주체는 해당 정보패키지를 이용하지 않아야 한다.

구조 검증 과정은 각 정보패키지의 종류에 관계없이 수행되어져야 한다.

6.2 무결성 검증

정보패키지의 무결성 검증은 패키지의 종류에 따라 검증 방법이 달라진다.

AIP의 경우는 XML 영역에 첨부된 전자서명 및 첨부파일 해쉬값으로 무결성 검증을 수행하게 된다.

전자서명 검증은 AIP의 XML 영역에 첨부된 전자서명값을 검증하는 과정으로서, 본 규격에 정의된 요소인 Signature에 대한 검증을 수행하도록 하며, 생성 시와 마찬가지로 W3C “XML-Signature Syntax and Processing“ (RFC3275)에 기술된 검증 방법을 준용하여 검증을 수행하도록 한다.

더불어 전자서명에 사용된 인증서의 유효성 확인 작업도 전자서명 검증과 함께 전자서명 검증 과정 중에 반드시 수행되어야 한다.

인증서 유효성 확인 작업은 공인인증체계의 “공인인증서 경로검증 기술규격

[KCAC.TS.CERTVAL]"을 준용하여 검증한다.

서명 인증서의 유효성 검증에 실패한 경우, AIP의 무결성을 보증할 수 없으므로 검증 시스템은 해당 오류의 원인을 AIP의 이용 주체에게 출력하도록 하고, AIP의 이용 주체는 해당 정보패키지를 이용하지 않아야 한다. 단, 서명 인증서의 유효성 검증에는 실패하였더라도, 전자서명 장기검증 기술이 적용되었고 해당 검증 기술에 따라 검증하여 성공하였다면, 서명 인증서의 유효성 검증의 결과와는 관계없이 AIP의 전자서명 검증에 성공한 것으로 처리한다.

장기검증 기술은 본 버전의 규격에서는 다루지 않으며, 한국인터넷진흥원 또는 유관 기관이 제정한 기술규격을 준용하도록 한다.

원본 전자문서 및 변환본 전자문서의 첨부파일 영역에 대한 무결성 검증은 XML 영역 내의 첨부파일정보에 포함된 각 첨부파일의 해쉬값과 실제 첨부파일을 해쉬한 값을 비교함으로써 수행된다.

즉, 검증 시스템은 첨부파일 영역에 첨부된 개별 첨부파일을 해쉬한 후, XML 영역 내의 첨부파일정보에 포함된 각 첨부파일의 해쉬값과 비교하여 동일함을 확인하여야 한다.

해쉬값을 검증하는 과정과 전자서명을 검증하는 과정은 필요에 따라 순서가 바뀔 수 있다.

검증 시스템이 DIP 검증을 수행할 때에는, DIP에 첨부된 전자문서 첨부파일과 원본증명서에 포함된 전자문서 해쉬값에 대한 비교 검증을 수행하여 발급된 전자문서의 무결성을 확인하게 된다.

검증 시스템은 먼저 원본증명서에서 전자문서 해쉬값과 해쉬 알고리즘을 추출한 후, 추출한 해쉬 알고리즘으로 DIP에 첨부된 원본전자문서를 해쉬하여 생성된 해쉬값과 원본증명서에서 추출한 전자문서 해쉬값이 일치하는가를 검증하도록 한다. 만약 DIP에 첨부된 전자문서가 복수개라면 연접된 상태로 해쉬를 수행하여야 한다.

정보패키지의 전자서명이나 해쉬값에 대한 검증에 실패한 경우, 정보패키지의 무결성을 보증할 수 없으므로 검증 시스템은 해당 오류의 원인을 정보패키지의 이용 주체에게 출력하도록 하고, 정보패키지의 이용 주체는 해당 정보패키지를 이용하지 않아야 한다.

6.3 내용 검증

정보패키지의 내용 검증은, 검증 대상 정보패키지의 각 요소에 기재된 값이 본 규격에서 제시한 제약사항을 준수하고 있으며 상호모순은 없는가를 확인하는 작업이다.

정보패키지에 기재된 각 요소의 값에 대하여, 정보패키지 스키마를 통하여 검증 가능한 모든 제약사항에 대한 검증, 즉 구조 검증 과정을 통하여 확인할 수 있는 항목을 제외한 나머지의 모든 항목에 대한 검증을 내용 검증이라고 볼 수 있다.

예를 들어, datetime type 요소들 간의 전·후 관계, 인증서 발급자를 기재할 때의 DN 형식의 준수 여부, 첨부파일정보에서 첨부파일크기 값, datetime type 요소에서 각 시간단위의 최대값 초과 여부, 전자메일 형식, 정보패키지에 기재된 주체들의 식별자에 대한 검증이 필요할 경우 이에 대한 검증, 분류체계 구분값에 따른 분류체계 ID 및 분류코드 설정값 등은 본 내용 검증 과정에서 오류 여부를 확인할 수 있다.

이외에도 정보패키지의 각 요소에 기재된 값이 본 규격의 본문에서 제시한 내용에 위배되거나, 각 요소들 간에 모순이 있다면, 본 내용 검증 과정에서 해당 오류를 확인할 수 있어야 한다.

정보패키지의 내용 검증에 실패한 경우, 검증 시스템은 해당 오류의 원인을 정보패키지의 이용 주체에게 출력하도록 하고, 정보패키지의 이용 주체는 해당 정보패키지를 이용하지 않아야 한다.

DIP의 경우는 전자문서 및 원본증명서 분리를 위한 패키지 헤더 이외의 메타데이터가 존재하지 않으므로 본 내용 검증은 수행하지 않는다.

7. 버전 호환성

본 버전의 규격을 준수하여 구현된 시스템은 하위 버전의 규격을 준수하여 생성된 패키지에 대한 검증 및 처리가 가능해야 한다. 이때 검증의 기준은 하위 버전의 규격이며, 단 규격 상의 오류 내용은 제외한다. 처리의 과정 중에 새로운 패키지가 생성된다면 해당 패키지는 본 버전의 규격을 준수하여 생성되어야 하며, 생성을 위해 필요한 정보가 기존 패키지에 부족한 경우는 패키지 생성 시스템에서 적절히 생성하도록 한다.

규 격 연 혁

버전	제・개정일	제・개정내역
v1.00	2006년 11월 28일	・제정
v1.10	2007년 8월 27일	・전자문서정보패키지 검증절차 추가 ・모호하게 표현되거나 설명이 부족한 부분을 보완 ・필드(엘리먼트)의 길이, 반복수, 설정값 등을 보완 ・오류가 있거나 규격본문과 스키마가 일치하지 않는 부분 보완
v1.20	2009년 11월 4일	・AIP 생성시 첨부파일을 장기보존본으로 변환하는 조건에 대해서 설명 추가 ・패키지 식별자와 전자문서 식별자에서 '-', '_', '.'를 사용하도록 허용・권한정보필드의 모든 하위필드가 옵션이므로 권한정보 필드 자체도 옵션 필드로 보완 수정 ・AIP 스키마에서 패키지내의 전자문서의 갯수를 1~*로 버그 수정 ・패키지 스키마에서 extensions의 type을 string에서 ObjectType으로 보완 수정
v2.00	2011년 12월 30일	・각 패키지 스키마에서 불필요하거나 필드 옵션 처리 및 생성하지 않는 것으로 처리 ・전자문서 발급 시 패스워드 암호화 방식 추가 ・원본 발급 및 변환본 열람의 개념을 명확하게 제시 ・기타, 불필요한 필드 삭제 및 모호한 설명 보완
v2.10	2013년 6월 20일	・규격 용어 현행화
v3.00	2014년 1월 1일	・SIP 관련 내용 삭제 ・AIP 잉여 필드 삭제 및 생산자 의미 변경 ・DIP 포맷 변경 및 검증 방식 변경 ・불변경증명서 내용 추가