

**이용자시스템과 공인전자문서센터 간
연계 인터페이스 기술규격**

**Technical Standard for Communication
Interfaces between User System and
ARC(Authorized Retention Center)**

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	4
3. 연계 인터페이스 개요	5
3.1 개요	5
3.2 온라인 서비스	5
3.2.1 동기식 처리	6
3.2.2 비동기식 처리	6
3.3 오프라인 서비스	8
4. 연계 메시지 기본 요건	9
4.1 개요	9
4.2 요청 및 응답 메시지 일반 구조	9
4.2.1 요청 메시지 구조	9
4.2.1.1 메시지 구조	10
4.2.1.2 필드 설명	10
4.2.2 응답 메시지 기본 구조	11
4.2.2.1 메시지 구조	11
4.2.2.2 필드 설명	12
4.3 연계 유형별 요청 및 응답 메시지 구조	12
4.3.1 문서 등록 (SubmitDocument)	13
4.3.1.1 요청 (SubmitDocumentRequest)	13
4.3.1.2 응답 (SubmitDocumentResponse)	14
4.3.2 문서 발급 (GetDocument)	15
4.3.2.1 요청 (GetDocumentRequest)	15
4.3.2.2 응답 (GetDocumentResponse)	16
4.3.3 증명서를 사용한 문서 발급 (GetDocumentByCert)	17
4.3.3.1 요청 (GetDocumentByCertRequest)	18
4.3.3.2 응답 (GetDocumentByCertResponse)	20
4.3.4 문서 이관 (TransferDocument)	20
4.3.4.1 요청 (TransferDocumentRequest)	20

4.3.4.2 응답 (TransferDocumentResponse)	21
4.3.5 문서 폐기 (DeleteDocument)	21
4.3.5.1 요청 (DeleteDocumentRequest)	21
4.3.5.2 응답 (DeleteDocumentResponse)	22
4.3.6 문서 보관 연장 (ExtendRetention)	22
4.3.6.1 요청 (ExtendRetentionRequest)	23
4.3.6.2 응답 (ExtendRetentionResponse)	23
4.3.7 증명서 발급 (IssueCert)	24
4.3.7.1 요청 (IssueCertRequest)	24
4.3.7.2 응답 (IssueCertResponse)	24
4.3.8 증명서 갱신 (UpdateCert)	25
4.3.8.1 요청 (UpdateCertRequest)	25
4.3.8.2 응답 (UpdateCertResponse)	25
4.3.9 증명서 검증 (VerifyCert)	26
4.3.9.1 요청 (VerifyCertRequest)	26
4.3.9.2 응답 (VerifyCertResponse)	26
4.3.10 증명서 다운로드 (GetCert)	27
4.3.10.1 요청 (GetCertRequest)	27
4.3.10.2 응답 (GetCertResponse)	27
4.3.11 검색 (Search)	28
4.3.11.1 요청 (SearchRequest)	28
4.3.11.2 응답 (SearchResponse)	28
5. 보안 및 메시지 검증	29
5.1 개요	29
5.2 인증	29
5.3 기밀성	30
5.4 무결성	31
5.5 부인방지	31
5.6 전자서명 검증 시 고려사항	32

1. 규격의 개요

1.1 목적

“이용자시스템과 공인전자문서센터 간 연계 인터페이스 기술규격”(이하 본 규격)은 이용자가 공인전자문서센터의 서비스를 이용 시 이용자시스템과 공인전자문서센터 간 송·수신되는 메시지 및 이를 생성 및 처리하는 인터페이스에 대한 최소한의 요건을 제시함으로써, 이용자에게 신뢰할 수 있는 공인전자문서 서비스를 제공하기 위한 규격이다.

1.2 적용 대상 및 범위

공인전자문서센터는 서비스를 이용하는 이용자를 위해 다양한 접근방안을 제공하여야 한다. 웹에서 문서를 등록, 검색, 열람하거나 증명서를 발급 받을 수 있는 ASP 기반의 포털 어플리케이션 제공 외에도 이용자 내부의 통합 시스템과 공인전자문서센터가 네트워크를 통해 연계하여 서비스를 제공받거나, CD나 FTP를 통해 문서를 교환할 수가 있어야 한다. 또한 시스템 간 연계에 있어서도 핸드폰이나 PDA와 같은 모바일기기와의 연계를 통해 문서 등록요청, 검색 및 열람 요청 등의 서비스를 제공할 수도 있다.

본 규격에서는 공인전자문서센터가 제공하는 이러한 다양한 서비스 제공방안 중에서 주로 이용자 시스템과 공인전자문서센터 간 네트워크를 통한 연계 방안의 준수요건을 정의하며, 이외의 서비스 제공방안에 대해서도 최소한의 준수요건을 언급하고자 한다.

공인전자문서센터는 본 규격에서 제시하는 연계방안 외에도 시행령이나 시행규칙 및 관련 고시에 적합하다면, 추가 연계 인터페이스를 정의하거나 이용자 정의 프로토콜을 사용하여 서비스를 제공할 수도 있다. 다만 신뢰성있는 데이터의 송·수신을 위하여, 인증, 기밀성, 무결성, 부인방지 등의 전송보안 요건은 준수하여야 한다.

1.3 참고 자료

- ☐ 행정기관의 자료관시스템 규격, 행정자치부 정부기록보존소, 2003
- ☐ 정부전자문서유통표준, 행정자치부, 2005
- ☐ Web Services Description Language(WSDL) Version2.0 Part 0: Primer, W3C, 2005

- ☐ SOAP Version1.2 Part 0: Primer, W3C, 2005
- ☐ Web Service Security V1.1, OASIS, 2004
- ☐ ebXML Registry Services and Protocols V3.0, OASIS, 2005
- ☐ KCAC.TS.CERTVAL; 공인인증서 경로검증 기술규격 v1.11, 한국인터넷진흥원, 2009
- ☐ 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 규격에서 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) “연계 인터페이스”란 두 시스템들 간에 정보를 주고받기 위해 상호 합의된 메시지를 생성하고 처리할 수 있도록 제공된 함수 및 명령어를 말한다.
- 2) “보존 정보패키지”(이하 AIP), “배부 정보패키지”(이하 DIP)의 정의는 “전자문서 정보패키지 기술규격 v3.00”(이하 패키지 규격)의 정의를 따른다.
- 3) “증명서”란 공인전자문서센터가 이용자에게 전자문서등록, 전자문서발급, 전자문서서관, 전자문서폐기의 사실에 대한 증명, 발급된 전자문서가 원본 전자문서임에 대한 증명, 열람되는 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.
- 4) “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. IDN : Identification Number, 식별 번호
6. VID : Virtual ID, 가상 식별 정보
7. AIP : Archival Information Package, 보존 정보패키지
8. DIP : Dissemination Information Package, 배부 정보패키지

3. 연계 인터페이스 개요

3.1 개요

공인전자문서센터는 이용자에게 공인전자문서 서비스를 제공하기 위하여, 이용자시스템과 공인전자문서센터 시스템 간 공인전자문서센터 고유의 연계 인터페이스를 구축할 수 있다.

연계 인터페이스에는 네트워크를 통한 온라인 서비스의 형태도 있고 오프라인의 형태도 가능하다. 또한 온라인 서비스인 경우 동기식 처리 방식이나 비동기식 처리 방식도 가능하다.

즉, 이용자에게 편리하고 효율적이며 신뢰성있는 공인전자문서 서비스를 제공할 수 있다면, 어떤 방식의 연계 인터페이스도 가능하다.

3.2 온라인 서비스

온라인 서비스는 공인전자문서센터가 인터넷 망을 이용하여 이용자에게 공인전자문서 서비스를 제공하는 방식으로, 공인전자문서센터는 서비스 이용의 편의성을 위하여 반드시 온라인 서비스 방식의 연계 인터페이스를 구축하여야 한다.

공인전자문서센터는 HTTP, FTP, SMTP(EMail), #Mail 등 다양한 인터넷 프로토콜 및 서비스를 이용하여 이용자에게 전자문서 서비스를 제공할 수 있으며, 공인전자문서센터 고유의 TCP/IP 소켓 프로토콜을 개발하여 적용하는 것도 가능하다.

온라인 서비스에서는 프로토콜에 상관없이 이용자 측의 요청메시지와 이에 대응하는 공인전자문서센터 측의 응답메시지가 한 쌍을 이루면서 공인전자문서 서비스에 대한 신뢰성을 확보하게 된다.

온라인 서비스는 공인전자문서센터의 실제 작업 처리 결과를 이용자시스템이 언제 수신할 수 있는지에 따라 동기식 처리와 비동기식 처리로 구분된다.

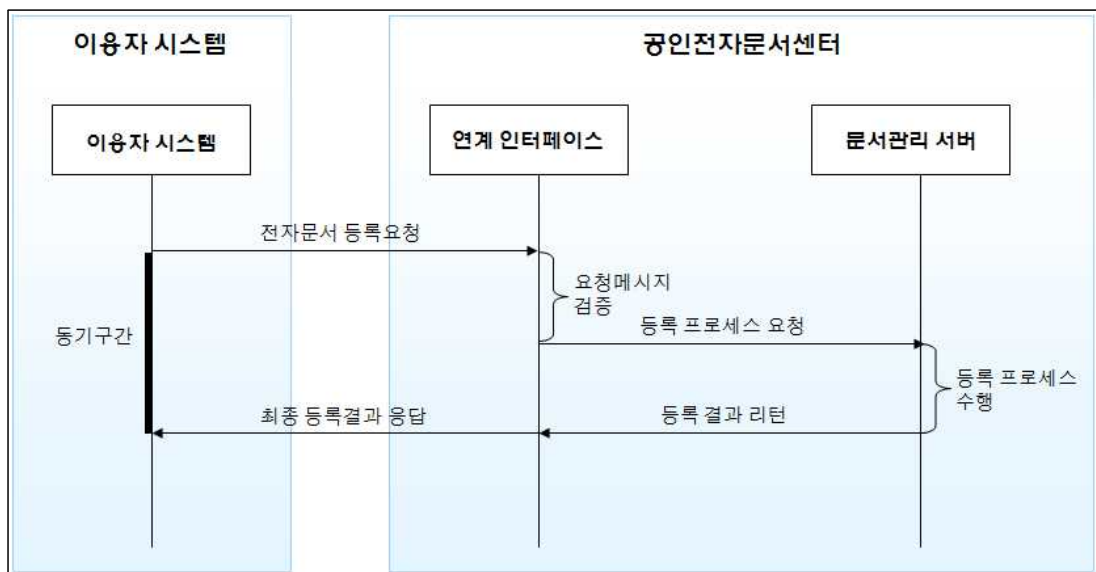
동기식 처리와 비동기식 처리의 구분은 메시지 송·수신에 사용되는 인터넷 프로토콜이 아닌, 전달되는 메시지의 내용, 즉 의미적으로 구분하도록 한다. 인터넷 프로토콜인 SMTP(EMail)를 예로 들자면(물론, 보안 요건 및 기타 요건들은 모두 준수한다고 가정), 이용자가 공인전자문서센터의 EMail 계정으로 문서를 전송하였을 때, 동기식 처리에서는 공인전자문서센터가 지체없이 문서등록 작업을 수행한 후 해당 결과를 이용자의 EMail 계정으로 회신하는데 반해, 비동기식 처리에서는 공인전자문서센터가 이용자의 전자문서를 정상적으로 수신하였음에 대해서만 1차적으로 회신한 후, 문서등록 작업에 대한 최종 결과를 다시 이용자에게 회신하게 된다. 이것은 SMTP 뿐 만 아니라 모든 인터넷 프로토콜에서 동일하다.

3.2.1 동기식 처리

동기식 처리란, 요청메시지를 송신한 이용자시스템이 공인전자문서센터의 응답을 기다리는 상황에서 이를 수신한 공인전자문서센터가 즉시 요청받은 작업을 수행한 후 응답메시지를 생성하여 수신 대기 중인 이용자시스템에 송신하는 것을 의미한다.

즉, 이용자시스템이 공인전자문서센터로부터 요청 작업에 대한 처리 결과를 즉시 수신할 수 있는 방식이다.

일반적으로, 요청 작업량이 많지 않거나 이용자시스템이 공인전자문서센터의 작업 처리 결과를 충분히 기다릴 수 있는 상황에서 이용된다.



상기의 프로세스는 이용자의 전자문서 등록 요청에 대하여, 공인전자문서센터가 동기식으로 처리하는 절차를 표현한 것으로서 절차를 설명하면 다음과 같다.

- ☐ 이용자 시스템은 전자문서 등록요청메시지를 공인전자문서센터 시스템에 전달한다.
- ☐ 공인전자문서센터 시스템은 요청메시지에 대하여 검증을 수행한 후, 이용자가 요청한 등록 작업을 수행한다.
- ☐ 공인전자문서센터 시스템은 등록결과에 대한 응답메시지를 생성하여 요청메시지 전송 후 응답메시지를 기다리고 있는 이용자 또는 이용자 시스템에 전달한다.

3.2.2 비동기식 처리

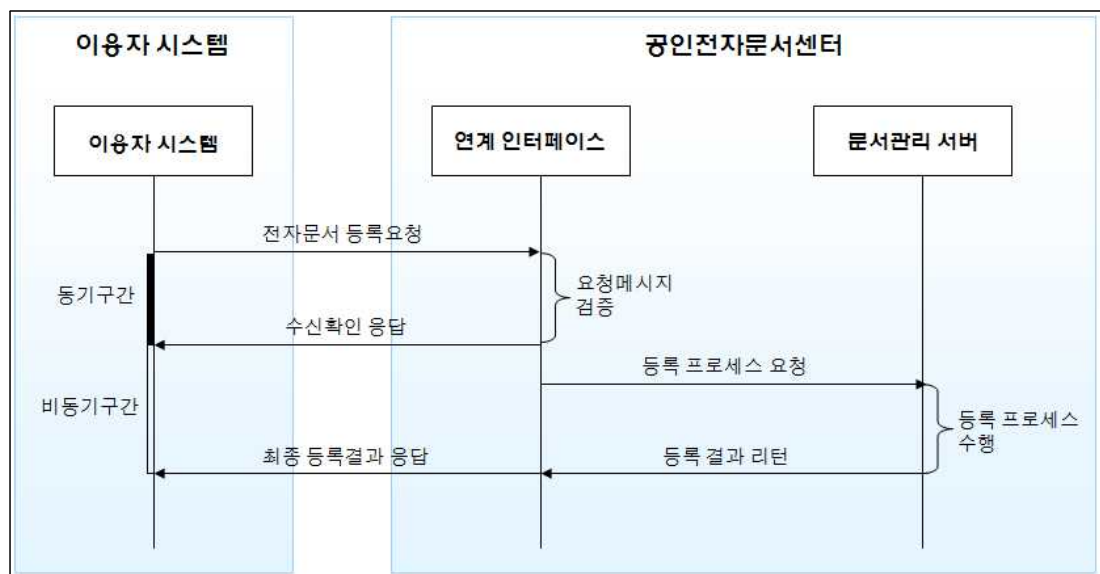
비동기식 처리란, 요청메시지를 수신한 공인전자문서센터가 이용자시스템에 요청메

시지 수신 여부에 대한 간단한 확인 응답메시지만을 전송하여 해당 연결을 종료하도록 하고, 실제 요청받은 작업을 비동기적으로 수행한 후 이에 대한 결과를 최종적으로 이용자시스템에 송신하는 방식이다.

따라서 비동기식 처리는 이용자의 요청 및 이에 대한 공인전자문서센터의 수신확인 응답의 동기 구간과 이용자의 요청에 대한 공인전자문서센터의 작업 수행 후 해당 결과를 전송하는 비동기 구간으로 이루어져 있다.

요청메시지 수신 여부에 대한 확인 응답메시지는 요청메시지에 대한 구조 검증 및 유효성 검증까지를 수행한 후 해당 결과를 전송하도록 한다. 요청메시지에 대한 검증이 성공한 경우는 수신 성공 메시지를 보내도록 하며, 실패한 경우는 실패 사유에 따른 수신 실패 메시지를 보내도록 한다. 물론 검증 실패의 경우는 다음의 비동기 작업 처리 작업을 수행하지 않는다.

비동기식 처리에서는, 이용자시스템이 공인전자문서센터에 요청메시지를 전송하여 수신확인 응답메시지를 받는 동기구간의 송·수신 방식과 해당 작업 처리 결과로 생성된 최종 결과를 공인전자문서센터가 이용자시스템에 전송하는 비동기 구간의 송·수신 방식이 다를 수 있으며, 이는 다른 종류의 온라인 송·수신 프로토콜 뿐만 아니라 오프라인 방식의 응답도 가능하다.



상기의 프로세스는 이용자의 전자문서 등록 요청에 대하여, 공인전자문서센터가 비동기식으로 처리하는 절차를 표현한 것으로서 절차를 설명하면 다음과 같다.

- ☐ 이용자 시스템은 전자문서 등록요청메시지를 공인전자문서센터 시스템에 전달한다.
- ☐ 공인전자문서센터 시스템은 요청메시지에 대하여 검증을 수행한 후, 요청메시

지에 대한 수신확인 응답메시지를 생성하여 이용자 시스템에 전송한다.

- ☐ 만약 요청메시지에 대한 검증이 실패한 경우는 해당 사유를 응답 메시지에 포함하여 전송하도록 하고, 이후의 비동기식 처리 과정을 수행하지 않는다.
- ☐ 공인전자문서센터 시스템은 요청메시지에 이상이 없는 경우, 이용자가 요청한 등록 작업을 수행한다.
- ☐ 공인전자문서센터 시스템은 사전에 이용자와 협의된 방식으로 최종 등록결과를 이용자 또는 이용자 시스템에 전달한다.

위에서 기술한 것처럼, 공인전자문서센터에서 등록 작업을 수행한 후 비동기적으로 이용자 시스템에 등록 처리 결과를 전달하는 절차 또는 방식을 제한하지 않는다.

즉, 온라인 서비스 상의 다양한 프로토콜을 포함하여, CD나 TAPE 등의 저장매체를 통한 오프라인 방식도 가능하다.

단, 최종 처리 결과가 비동기적으로 전달되는 과정에서의 인증, 기밀성, 무결성, 부인방지 등의 기본적인 보안요건은 준수되어야 한다.

3.3 오프라인 서비스

오프라인 서비스는 온라인 서비스와 달리 인터넷 망을 이용하지 않고 이용자와 공인전자문서센터 간 직접 방문에 의하여 데이터(또는 메시지)를 전달하는 방식을 의미한다.

데이터를 전달하기 위하여 사용하는 저장매체의 종류를 제한하지 않으며, 디스크 스토리지, CD, TAPE, USB 저장장치 등 다양한 저장매체를 사용할 수 있다.

오프라인 서비스의 경우 온라인 서비스와는 달리 오프라인 상에서 데이터가 전달되기 위하여 특정한 메시지의 형식으로 변환할 필요는 없으나, 오프라인으로 데이터가 전달되는 과정에서의 인증, 기밀성, 무결성, 부인방지 등의 보안요건을 만족해야 함은 동일하다.

오프라인 서비스의 경우 전달 과정 중에 데이터가 유출되거나 유실·누락될 가능성이 많기 때문에, 반드시 정당한 수신자만이 데이터에 접근할 수 있도록 하고 수신 후에는 전체 데이터에 대한 무결성 확인이 가능해야 하며, 또한 제 3자 보안이 필요한 데이터에 대해서는 기밀성 유지 방법을 적용하여야 한다.

특히 온라인 서비스와는 달리, 데이터 전달 과정에 대한 감사기록이 공인전자문서센터 시스템에 남지 않기 때문에, 공인전자문서센터는 오프라인 상의 데이터 전달 및 접수에 대한 증빙자료를 반드시 유지하여야 한다.

4. 연계 메시지 기본 요건

4.1 개요

본 장에서는 온라인 상에서 이용자 시스템과 공인전자문서센터 간 송·수신되는 요청메시지와 응답메시지의 기본 요건에 대해서 정의하며, 이를 오프라인 서비스에 적용하는 것도 가능하다.

온라인 상의 동기식 처리 및 비동기식 처리 과정 중 동기식 구간은 본 장에 제시된 요건을 준수하여야 한다.

본 장에 제시된 연계 인터페이스 메시지의 유형 및 각 유형별 요건은 신뢰성 있는 공인전자문서 서비스를 위한 최소한의 요건을 제시한 것으로서 이용자시스템과 공인전자문서센터 간 동기적으로 송·수신되는 요청메시지와 응답메시지는 반드시 본장에서 제시하는 기본 요건을 만족하여야 한다.

단, 본 규격에서는 메시지 요건만을 정의하며 통신 프로토콜이나 메시지 생성 언어 및 시스템 개발 언어 등을 제시하지는 않으므로, 각 공인전자문서 센터는 본 규격상의 메시지 요건을 준수하여 스스로의 서비스에 적합한 메시지 생성방식을 적용할 수 있다.

4.2 요청 및 응답 메시지 일반 구조

온라인 상에서의 공인전자문서 서비스 이용 시 생성 및 처리되는 송·수신 메시지는 항상 이용자 측의 요청메시지와 이에 대한 응답인 공인전자문서센터 측의 응답메시지의 한 쌍이 대응을 이룬다.

요청메시지와 응답메시지는 모두, 신뢰성 있는 메시지 송·수신을 위한 Header 부분과 실제 전달하고자 하는 내용이 포함된 Body의 두 부분으로 구분된다.

4.2.1 요청 메시지 구조

요청 메시지는 MessageHeader와 MessageBody로 이루어져 있다.

MessageHeader에는 작업 종류, 요청·응답 구분, 메시지 식별자, 타임스탬프 등의 요청 메시지에 대한 일반적인 정보를 나타내는 필드들이 포함되며, MessageHeader의 구조는 응답 메시지에서도 동일하다.

MessageBody에는 실제 요청의 내용인 RequestData가 포함되며, RequestData의 구조는 각 연계 유형별로 제시된 필수 요건을 준수하여 각 공인전자문서센터에서 자체적으로 정의하여 사용하도록 한다.

공인전자문서센터는 RequestData 구조 정의 시, 동일 작업에 대하여 복수개의 데이

터 처리를 요청하는 방식으로도 정의할 수 있다. 즉, 복수개의 AIP가 생성되도록 전자문서 등록 요청 메시지를 생성할 수도 있고, 복수개의 전자문서가 발급되도록 전자문서 발급 요청 메시지를 생성할 수도 있다. 물론 이용자 시스템이 하나의 요청메시지를 사용하여 복수개의 데이터 처리를 요청하였다면, 공인전자문서센터도 이에 대응하는 응답메시지에 복수개의 데이터 처리 결과를 포함하여야 한다.

4.2.1.1 메시지 구조

메시지 필드 명			type (크기)
Message	MessageHeader (1..1)	Version	string (3byte)
		OperationType (1..1)	char (1byte)
		MessageType (1..1)	char (1byte)
		MessageID (1..1)	string (36byte)
		TimeStamp (1..1)	string (15byte)
	MessageBody (1..1)	RequestData (1..1)	structure

4.2.1.2 필드 설명

필드명	설명	생성규칙	예
Version	연계 인터페이스 메시지 구조의 버전	본 규격을 준용한 연계 인터페이스 메시지의 버전은 "3.0"으로 설정	"3.0"
OperationType	각 작업에 대한 코드값	문서등록(1), 문서발급(2), 증명서를 사용한 문서발급(4), 문서이관(5), 문서폐기(6), 문서보관 연장(7), 증명서발급(8), 증명서갱신(9), 증명서검증(a), 증명서다운로드(b), 검색(c)	'a' * '3' 값은 사용하지 않음 * 자체 연계 유형 정의 시 'g'~'z'까지를 사용할 것
MessageType	요청메시지와 응답메시지의 구분 코드값	request(1), response(2)	'1'
MessageID	message의 ID	요청 : "req_" + 16byte random number를 16진수 string으로 변환한 값, 응답 : "res_" + 요청 메시지에 첨부된, 16진수 string 값으로 변환된 16byte	"req_0aa2c56e3bce534aefc3b23dec42fae3"

		random number	
TimeStamp	메시지가 전송된 GMT 시각	"yyyymmddhhmiss" + "Z"	"20060918160955Z"
TotalCount	RequestData의 수		3212
RequestData	공인전자문서 서비스 요청 내용	연계 유형별로 공인전자문서센터에서 자체적으로 정의하여 사용	

4.2.2 응답 메시지 기본 구조

응답 메시지도 요청 메시지와 같이 MessageHeader와 MessageBody로 이루어져 있다.

MessageHeader의 구조는 요청 메시지와 동일하다.

MessageBody는 이용자가 요청한 작업의 처리결과와 내용인 ResponseData를 포함하며, ResponseData의 내부구조는 요청메시지에서와 마찬가지로, 각 연계 유형별로 제시된 필수 요건을 준수하여 각 공인전자문서센터에서 자체적으로 정의하여 사용하도록 한다.

요청메시지에서 복수개의 데이터 처리를 요청하였다면, 응답메시지의 ResponseData는 각각의 데이터 처리 결과를 포함하여야 한다.

단일건에 대한 처리 실패의 경우 응답메시지에 포함되는 처리결과는 당연히 실패이나, 복수건에 대한 처리의 경우는 부분 실패가 발생할 수 있으며, 이 경우에는 공인전자문서센터의 정책에 따라 처리 결과코드 및 관련 정보로 응답 메시지를 구성할 수 있다.

이때 주의할 점은 실패 사유 및 이를 통한 사후 조치 작업과 관련된 명확하고 모순 없는 응답 메시지가 생성되어야 한다. 예를 들어, 복수건에 대하여 부분 실패하였으나 처리결과를 성공으로 한 경우, 실패한 건들에 대해서 이용자에게 알리지 않아 이용자가 모든 건에 대하여 성공으로 인식하게 하거나, 또는 실패 건에 대한 재처리작업을 수행할 수 없다거나 하는 것은 불가하다.

4.2.2.1 메시지 구조

메시지 필드 명			type (크기)
Message	MessageHeader (1..1)	Version	string (3byte)
		OperationType (1..1)	char (1byte)

		MessageType (1..1)	char (1byte)
		MessageID (1..1)	string (36byte)
		TimeStamp (1..1)	string (15byte)
	MessageBody (1..1)	ResponseData (1..1)	structure

4.2.2.2 필드 설명

필드명	설명	생성규칙	예
Version	연계 인터페이스 메시지 구조의 버전	본 규격을 준용한 연계 인터페이스 메시지의 버전은 "2.0"으로 설정	"3.0"
OperationType	각 작업에 대한 코드 값	문서등록(1), 문서발급(2), 증명서를 사용한 문서발급(4), 문서이관(5), 문서폐기(6), 문서보관 연장(7), 증명서발급(8), 증명서갱신(9), 증명서검증(a), 증명서다운로드(b), 검색(c)	'9' * '3' 값은 사용하지 않음 * 자체 연계 유형 정의 시 'g'~'z' 까지를 사용할 것
MessageType	요청메시지와 응답메시지의 구분 코드값	request(1), response(2)	'2'
MessageID	message의 ID	요청 : "req_" + 16byte random number를 16진수 string으로 변환한 값, 응답 : "res_" + 요청 메시지에 첨부된, 16진수 string 값으로 변환된 16byte random number	"res_0aa2c56e3bce534aefc3b23dec42fae3"
TimeStamp	메시지가 전송된 GMT 시각	"yyyymmddhhmiss" + "Z"	"20060918160959Z"
ResponseData	요청 내용 처리 결과	연계 유형별 응답 메시지 구조는 공인전자문서센터에서 자체적으로 정의하여 사용	

4.3 연계 유형별 요청 및 응답 메시지 구조

상기의 연계 메시지 구조에서 실제로 전달하고자 하는 내용 부분은 MessageBody 내의 RequestData와 ResponseData로서 각 서비스 유형에 따라 이름과 내부 구조가

달라지게 되는데, 해당 내부 구조에 대해서는 본 규격에서 제시하는 기본 요건을 준수하여 각 공인전자문서센터에서 자체적으로 정의하여 사용하도록 한다.

요청메시지 및 응답메시지에 포함되어 전달되는 파라미터에는 필수 파라미터와 선택 파라미터로 구분할 수 있는데, 필수 파라미터는 해당 연계 유형의 서비스가 수행되기 위하여 반드시 전달되어야 하는 인자이고, 선택 파라미터는 이용자와의 협약에 근거한 공인전자문서센터의 구현방식에 따라 전달될 수도 있고 전달되지 않을 수도 있는 인자를 의미한다.

선택 파라미터의 경우, 사전에 공인전자문서센터와 이용자 간 협의된 방식으로 처리가 이루어지며, 공인전자문서센터는 반드시 추후 부인방지를 위하여 협약의 근거를 유지·관리하여야 한다.

4.3.1 문서 등록 [SubmitDocument]

이용자가 전자문서를 공인전자문서센터에 등록할 때 이용하는 전자문서 등록 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

4.3.1.1 요청 [SubmitDocumentRequest]

전자문서 등록 요청 메시지는 공인전자문서센터에 보관할 이용자의 전자문서 및 관련 정보를 포함한다.

전자문서를 첨부하는 방식은 공인전자문서센터에서 자체적으로 정의할 수 있으나, 첨부되는 전자문서에 대한 기밀성 및 무결성 요건을 위반하는 방식은 불가하다. 참고로, 요건을 만족한다면 구버전의 패키지 규격 상 정의된 SIP 형식으로 문서등록을 위한 파라미터를 전달하는 것도 가능하다.

문서 등록 요청메시지 내에 복수개의 AIP를 생성할 수 있는 정보를 포함하여 전달하는 것도 가능하며, 이 경우 메시지 생성 규칙 상의 적절한 구분자를 이용하여 이용자의 의도가 오류 없이 공인전자문서센터에 전달될 수 있도록 한다.

구분	파라미터	비고
필수	- 전자문서	-
선택	- 최초등록증명서 발급여부 - 패키지 내용설명, 본제목, 보존만료일, 암호화 처리구분, 전자문서 생산자(소유자) 등	- AIP 생성을 위하여 이용자가 입력해야 하는 인자들

요청메시지에는 등록하고자 하는 전자문서를 필수 파라미터로 첨부하며, 최초등록증명서 발급여부 및 AIP 생성을 위하여 이용자 측에서 입력해야 하는 인자들의 경우

는, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 요청메시지에서 이를 생략할 수 있다.

이외에도 전자문서 관리에 필요한 다른 정보를 함께 전송할 수 있다.

주의할 점은 문서등록 요청메시지의 무결성 및 부인방지를 위하여 메시지에 전자서명을 수행 시, 반드시 전자문서가 아닌 전자문서의 해쉬값을 구하여 전자서명 대상에 포함시켜야 한다. 이것은 추후 부인방지를 위하여 공인전자문서센터에서 문서등록 요청메시지를 저장 시 전자문서를 저장하지 않도록 하기 위함으로써, 공인전자문서센터는 수신된 문서등록 요청메시지의 전자서명 및 전자문서 해쉬값에 대한 검증을 수행하여 전체 메시지의 무결성을 확인한 후, 추후 부인방지를 위하여 전자서명이 첨부된 메시지만 저장하고, 메시지에 첨부되었던 전자문서는 허용되지 않은 접근 등의 위협을 방지하기 위하여 별도로 저장하지 않는다.

4.3.1.2 응답 [SubmitDocumentResponse]

전자문서 등록 요청에 대한 응답 메시지는 이용자가 보관 요청한 전자문서에 대한 등록 처리 결과 및 관련 정보로서, 등록 작업의 처리 결과가 성공인 경우는 전자문서의 보관 정보 및 해당 등록 작업에 대한 증적 정보를 포함하며 실패인 경우는 해당 전자문서의 등록 처리 실패의 사유를 포함한다.

구분	파라미터	비고
필수	<ul style="list-style-type: none"> - 성공 : 결과코드, AIP ID - 실패 : 결과코드, 실패사유 	<ul style="list-style-type: none"> - 요청메시지 내에 복수개의 요청이 포함된 경우, 응답메시지에도 복수개의 처리 결과에 대한 파라미터가 포함되어야 함. 단 전체실패로 처리하는 경우는 제외 * 이하 연계유형별 응답 메시지 동일
선택	- 성공 : 최초등록증명서(또는 최초등록 증명서 획득 정보)	-

전자문서 등록 작업이 성공하였다면, 전자문서가 공인전자문서센터에 정상적으로 등록되었음을 확인할 수 있는 정보로서 AIP ID가 응답메시지에 포함되어 이용자시스템에 전송된다.

최초등록증명서의 경우는 응답메시지에 포함되거나, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 응답메시지에서 이를 생략할 수 있다.

4.3.2 문서 발급 [GetDocument]

이용자가 전자문서를 공인전자문서센터로부터 열람하거나 발급받을 때 이용하는 전자문서 발급 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

본 전자문서 발급 메시지와 관련하여, 패키지 규격 상 전자문서 발급 서비스는 원본 증명서가 첨부된 원본 전자문서를 DIP 형식으로 발급하는 것을 의미하며, 전자문서 열람 서비스는 원본증명서가 첨부되지 않은 원본 전자문서 또는 변환본(장기보존본 또는 업무활용본) 전자문서를 이용자에게 전달하는 것을 의미한다. 참고로 전자문서 열람 서비스는 기본적인 보안요건을 준수하는 범위 내에서, 본 전자문서 발급 메시지 이외에 다양한 방식의 서비스를 제공하는 것도 가능하다.

4.3.2.1 요청 [GetDocumentRequest]

전자문서 발급 요청 메시지는 공인전자문서센터에 보관 중인 전자문서를 발급받기 위한 정보를 포함한다.

구분	파라미터	비고
필수	<ul style="list-style-type: none"> - AIP ID - 원본증명서 발급을 위한 증명요청서 (DIP 발급 요청 시) - 불변경증명서 발급을 위한 증명요청서 (열람용 변환본에 대한 불변경증명서 발급 요청 시) 	<ul style="list-style-type: none"> - 전자문서 발급요청(DIP 발급)인 경우는 원본증명서 발급을 위한 증명요청서를 첨부해야 함. 미 첨부 시 열람 서비스로 간주됨 - 변환본 전자문서 열람 시 변환본 전자문서에 대한 불변경증명서를 발급받고자 한다면 불변경증명서 발급을 위한 증명요청서를 첨부
선택	<ul style="list-style-type: none"> - AIP 내 전자문서 식별정보 - 암호화 발급 여부 및 암호화 인증서 또는 패스워드 - 수신 방법 및 수신주소 	-

요청메시지에는 발급받을 전자문서를 식별하기 위한 정보로서 추후 부인방지를 위하여 패키지 규격상의 AIP ID를 포함하여야 하며, 열람이 아닌 발급이라면 DIP에 첨부될 원본증명서 발급을 위한 증명요청서가 포함되어야 한다. 만약 발급 요청 메시지에 원본증명서 발급을 위한 증명요청서가 첨부되지 않았다면, 공인전자문서센터는 열람 서비스를 제공하도록 한다.

열람 서비스인 경우, 만약 이용자가 변환본 전자문서에 대하여 불변경증명서를 발급받고자 한다면 요청메시지에 불변경증명서 발급을 위한 증명요청서를 포함해야 한다.

추가적으로 AIP 내 전자문서 식별정보, 암호화 발급정보, 수신정보 등이 요청메시지에 포함되거나, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된

경우 요청메시지에서 이를 생략할 수 있다.

AIP 내에는 공인전자문서센터의 정책 및 이용자의 요청에 의하여 원본 이외에도 변환본(장기보존본 또는 업무활용본) 전자문서가 포함되어 있을 수 있으며, 이 가운데 어떤 문서를 발급 또는 열람할 것인가에 대한 정보가 요청 메시지에 포함될 수 있다.

패키지 규격 상 업무활용본의 경우는, 전자문서 등록 과정이 아닌 발급 과정에서 공인전자문서센터가 변환작업을 수행하여 이용자에게 내려줄 수 있다. 따라서 공인전자문서센터 변환정책 및 열람정책에 따라, 이용자는 현재 AIP 내에 업무활용본이 포함되어 있지 않은 경우에도 업무활용본에 대한 열람을 요청할 수 있으며, 이에 공인전자문서센터는 변환작업을 수행하여 생성된 업무활용본을 응답메시지에 포함시켜 이용자에게 전달하도록 한다.

이용자는 수신한 전자문서를 특정인에게만 배포할 목적으로 전자문서를 암호화하여 발급해 줄 것을 요청할 수 있으며, 이 경우 암호화에 사용할 특정인의 인증서 또는 패스워드를 요청 메시지에 포함하여 전송하도록 한다. 인증서를 사용하여 암호화 요청하는 경우, 발급 요청자가 문서의 내용을 열람해야 할 필요가 있을 때는 특정인의 인증서 리스트에 발급 요청자의 인증서도 포함시켜야 한다.

전자문서를 암호화하기 위하여 패스워드를 사용하는 경우는 반드시 공인전자문서센터의 인증서를 사용하여 해당 패스워드를 암호화한 후 요청메시지의 파라미터 값으로 설정하여야 한다. 이것은 송·수신 메시지의 기밀성 유지를 위한 네트워크 암호화 구간이 종료된 이후, 암호화된 전자문서에 대한 공격을 차단하는 한편, 이용자의 개인 정보를 보호하기 위해서이다.

이용자는 발급된 전자문서를 응답메시지를 통하여 직접 수신하는 방법 이외에 공인전자문서센터가 제공하는 다른 방식으로 수신할 수도 있으며, 이를 위하여 전자문서를 수신하는 방법 및 수신주소를 요청메시지에 파라미터로 포함시킬 수 있다.

이외에도 전자문서 발급을 위하여 필요한 다른 정보를 함께 전송할 수 있다.

4.3.2.2 응답 [GetDocumentResponse]

전자문서 발급 요청에 대한 응답 메시지는, 해당 전자문서에 대한 발급 작업의 처리 결과가 성공인 경우는 발급된 전자문서 또는 발급된 전자문서와 관련된 정보를 포함하며, 실패인 경우는 해당 전자문서의 발급 처리 실패의 사유를 포함한다.

구분	파라미터	비고
필수	- 성공 : 결과코드, DIP 또는 전자문서 (또는 DIP 및 전자문서 획득 정보), 불변경증명서(이용자 요청시)	- 요청메시지에 원본증명요청서가 포함된 경우는 DIP를, 포함되지 않은 경우는 원본 또는 변환본 전자문서 파일을 첨부

	- 실패 : 결과코드, 실패사유	- 전자문서 열람 서비스 시, 요청메시지에 불변경증명요청서가 포함된 경우는 불변경증명서 첨부
선택	-	-

처리 결과가 성공인 경우, 발급된 전자문서는 응답 메시지에 직접 첨부되어 이용자에게 전달될 수도 있고, 공인전자문서센터와 이용자 간에 미리 협의된 별도의 방식으로 이용자 또는 인가된 제 3자에게 전달할 수도 있다. 즉, 전자문서 수신자의 Email 전송, HTTP 또는 FTP를 이용한 다운로드 등의 온라인 방식이나, CD, TAPE, 대용량 저장장치 등의 저장매체를 이용한 오프라인 방식도 가능하다. 단, 어떤 방식으로 전달되더라도 인증, 기밀성, 무결성, 부인방지 등의 기본적인 보안 요건은 만족되어야 한다.

주의할 점은 문서발급 응답메시지를 포함하여 별도의 방식으로 이용자에게 전자문서를 전달하는 경우 해당 메시지의 무결성 및 부인방지를 위하여 메시지에 전자서명을 수행 시, 반드시 전자문서가 아닌 전자문서의 해쉬값을 구하여 전자서명 대상에 포함시켜야 한다. 이것은 추후 부인방지를 위하여 공인전자문서센터에서 해당 메시지를 저장 시 전자문서를 저장하지 않도록 하기 위함으로써, 공인전자문서센터는 메시지 송신 후, 추후 부인방지를 위하여 전자서명이 첨부된 메시지만 저장하고, 메시지에 첨부되었던 전자문서는 허용되지 않은 접근 등의 위협을 방지하기 위하여 별도로 저장하지 않는다.

변환본 전자문서에 대한 열람 서비스 시, 이용자가 변환본 전자문서에 대한 불변경증명서를 요청한 경우, 공인전자문서센터는 불변경증명서를 발급한 후 열람 서비스 제공방식에 따라 이용자에게 전달하도록 한다.

4.3.3 증명서를 사용한 문서 발급 (GetDocumentByCert)

이용자가 자신의 전자문서에 대한 발급권한(또는 열람권한)을 수입자에게 위임하여 수입자가 이용자의 전자문서를 발급받을 수 있도록 하는, 증명서를 사용한 전자문서 발급 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

이용자는 자신의 전자문서에 대한 발급권한을 타 이용자 또는 공인전자문서센터의 이용자로 등록되지 않은 제3자에게 위임할 수 있는데, 공인전자문서센터의 타 이용자에게 위임하는 경우는 공인전자문서센터의 권한 관리 기능을 사용하여 이용자의 승인하에 손쉽게 발급권한의 위임이 가능하지만 공인전자문서센터의 이용자가 아닌 경우는 해당 방법의 적용이 불가능하기 때문에, 본 증명서를 사용한 전자문서 발급 서비스 기능을 이용하여 공인전자문서센터의 이용자가 아닌 경우에도 이용자의 전자문서를 발급받을 수 있게 된다.

이용자는 먼저 제3자에게 발급권한을 위임하기 위하여, 제3자가 발급받고자 하는 전자문서의 등록증명서에 제3자의 정보를 수임자(nominee)로 설정하여 발급 후 수임자에게 전달해야 한다.

수임자는 해당 등록증명서 및 자신의 인증서를 사용하여 자신이 전자문서에 대한 정당한 수임자임을 증명하게 된다.

등록증명서의 수임자 정보 설정에 대한 상세한 내용은 증명서 규격을 참조하도록 한다.

증명서를 사용한 문서 발급 기능에 대한 구현은 공인전자문서센터의 정책상 선택적으로 구현 가능한 기능이며, 구현 시에는 본 규격을 준용하여야 한다.

4.3.3.1 요청 [GetDocumentByCertRequest]

수임자는 자신이 전자문서에 대한 발급권한을 위임받은 자임을 증명하기 위하여, 등록증명서, 자신의 인증서 및 전자서명값, 그리고 등록증명서에 기재된 수임자와 인증서의 소유자가 동일인임을 확인할 수 있는 자신의 실명, 식별번호, 그리고 인증서 VID값 생성시 사용된 Random Number를 공인전자문서센터에 전송하여야 한다.

구분	파라미터	비고
필수	<ul style="list-style-type: none"> - 등록증명서 - 인증서, 전자서명값 - 수임자 실명 및 식별번호 - Random Number(수임자 정보가 실명 및 식별번호로 생성된 경우) - 원본증명서 발급을 위한 증명요청서 (DIP(원본 전자문서) 발급 요청 시) - 불변경증명서 발급을 위한 증명요청서 (열람용 변환본에 대한 불변경증명서 발급 요청 시) 	<ul style="list-style-type: none"> - Random Number는 인증서의 VID값 생성 시 사용된 값으로서, 등록증명서에 설정된 수임자 정보가 실명 및 식별번호를 사용하여 생성된 경우에만 전달함에 주의할 것 - 수임자의 권한이 전자문서 발급인 경우는 원본증명서 발급을 위한 증명요청서가 포함되며, 수임자의 권한이 열람인 경우는 포함되지 않아야 함 - 변환본 전자문서 열람 시 변환본 전자문서에 대한 불변경증명서를 발급받고자 한다면 불변경증명서 발급을 위한 증명요청서를 첨부
선택	<ul style="list-style-type: none"> - AIP 내 전자문서 식별정보 - 암호화 발급 여부 및 암호화 인증서 또는 패스워드 - 수신 방법 및 수신주소 	-

전자문서를 발급 또는 열람하기 위해 필요한 등록증명서, 인증서, 전자서명값, 수임

자 실명, 식별번호, Random Number, 원본증명요청서 등은 필수 인자로 포함된다.

그리고 열람 서비스인 경우, 만약 이용자가 변환본 전자문서에 대하여 불변경증명서를 발급받고자 한다면 요청메시지에 불변경증명서 발급을 위한 증명요청서를 포함해야 한다.

첨부되는 등록증명서 내에는 발급 또는 열람하고자 하는 전자문서의 정보 및 권한을 위임받은 수임자의 정보가 명시되어 있다.

인증서의 소유자임을 증명하기 위한 전자서명값은 메시지 무결성 및 부인방지 등을 위하여 메시지에 첨부되는 기본 전자서명값을 그대로 사용하도록 하고, 인증서 또한 메시지 전자서명 구조 상 인증서를 포함하는 구조라면 해당 인증서를 사용하도록 한다.

증명서 규격 상 등록증명서에 수임자 정보를 설정하는 방법은 수임자의 실명 및 식별번호를 수임자 정보로 설정하거나, 수임자 인증서 식별정보를 수임자 정보로 설정하는 2가지 방법이 있다.

이 중 수임자의 실명 및 식별번호가 등록증명서의 수임자 정보로 설정되었다면, 해당 수임자와 함께 전송된 인증서의 소유자가 동일인임을 확인하기 위한 정보로서 수임자 실명 및 식별번호, 그리고 인증서의 VID 값 생성 시 사용된 Random Number가 전송되어야 한다.

만약 수임자 인증서 식별정보가 등록증명서의 수임자 정보로 설정되었다면, 함께 전송된 인증서 내에 포함된 인증서 식별정보를 사용하여 수임자와 인증서 소유자가 동일인임을 확인할 수 있으므로, 이를 확인하기 위한 정보로서 수임자 실명 및 식별번호, 그리고 Random Number는 필요없게 된다.

하지만 수임자의 실명 및 식별번호는 전자문서 발급 증적 생성 시 서비스 요청자 정보를 생성할 때에도 사용되기 때문에 수임자 인증서 식별정보가 등록증명서의 수임자 정보로 설정된 경우라도 공인전자문서센터에 전달해야 함에 주의한다.

등록증명서의 수임자 정보 검증에 대한 상세한 내용은 증명서 규격을 참조하도록 한다.

등록증명서에는 수임자에게 위임된 권한이 명시되어 있는데, 이에 따라 발급을 의미하는 downloadDocument인 경우는 요청메시지의 파라미터로 원본증명서 발급을 위한 증명요청서를 첨부하여 공인전자문서센터에 원본증명서가 첨부된 DIP의 형식의 전자문서 발급을 요청해야 하고, 열람을 의미하는 readDocument인 경우는 원본증명서 발급을 위한 증명요청서를 첨부하지 않은 열람 요청메시지를 전송하여야 한다.

만약 downloadDocument와 readDocument가 둘 다 설정되어 있다면, 수임자는 발급 또는 열람을 선택하여 요청할 수 있다. 이 경우, 요청메시지에 원본증명서 발급을 위한 증명요청서가 포함되어 있다면 전자문서 발급이며, 미포함되어 있다면 전자문서 열람으로 간주한다.

이용자가 변환본 전자문서에 대하여 열람 서비스를 제공받는 경우, 이용자는 해당 변환본 전자문서에 대한 불변경증명서 발급을 요청할 수 있으며 이를 위하여 요청 메시지에 불변경증명서 발급을 위한 증명요청서를 포함시켜야 한다.

이외에 공인전자문서센터 정책에 따라 전자문서 발급 시와 동일하게 선택 파라미터를 설정할 수 있다.

4.3.3.2 응답 [GetDocumentByCertResponse]

증명서를 사용한 전자문서 발급 요청에 대한 응답 메시지는, 전자문서 발급 요청에 대한 응답 메시지와 동일한 형식이다.

구분	파라미터	비고
필수	<ul style="list-style-type: none"> - 성공 : 결과코드, DIP 또는 전자문서 (또는 DIP 및 전자문서 획득 정보), 불변경증명서(이용자 요청시) - 실패 : 결과코드, 실패사유 	<ul style="list-style-type: none"> - 요청메시지에 원본증명요청서가 포함된 경우는 DIP를, 포함되지 않은 경우는 원본 또는 변환본 전자문서 파일을 첨부 - 전자문서 열람 서비스 시, 요청메시지에 불변경증명요청서가 포함된 경우는 불변경증명서 첨부
선택	-	-

4.3.4 문서 이관 [TransferDocument]

공인전자문서센터에 보관 중인 전자문서를 타 공인전자문서센터에 이관할 것을 요청할 때 이용하는 전자문서 이관 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

4.3.4.1 요청 [TransferDocumentRequest]

전자문서 이관 요청 메시지는 이관 대상 전자문서 정보 및 수관 공인전자문서센터의 정보를 포함한다.

구분	파라미터	비고
필수	- 이관 대상 전자문서 정보	- AIP ID, 2013년 8월 28일 등록된 문서 전체, 등록된 모든 문서 등
선택	- 수관 공인전자문서센터 정보	-

요청메시지에는 이관하고자 하는 전자문서 정보를 필수 파라미터로 첨부하며, 수관 공인전자문서센터 정보는 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 요청메시지에서 이를 생략할 수 있다.

일반적으로 타 공인전자문서센터로의 전자문서 이관은 대량의 전자문서에 대하여 발생하므로, 이관 대상 전자문서 정보로는 AIP ID 이외에도 공인전자문서센터에서 이관 대상 전자문서를 명확하게 식별(구분)할 수 있는 정보면 무엇이든 가능하며, 추후 부인방지 정보로서 사용될 수 있어야 한다.

4.3.4.2 응답 [TransferDocumentResponse]

일반적으로 공인전자문서센터가 전자문서를 수관 공인전자문서센터에 이관하는 작업은 이관 요청 및 응답 작업 시점과 비동기적으로 이루어지기 때문에, 전자문서 이관 요청에 대한 응답 메시지에는 해당 전자문서에 대한 이관 가능 여부의 확인 결과도 포함되며, 전자문서 이관 작업을 완료한 후, 공인전자문서센터는 작업의 결과 및 실패 시 오류 내용을 반드시 이관 요청자에게 전달하여야 한다.

만약 이관 요청 시 동기적으로 이관 작업이 이루어진다면 이관 응답메시지에는 이관 작업의 결과 및 실패 시 오류 내용을 포함하도록 한다.

구분	파라미터	비고
필수	<ul style="list-style-type: none"> - 성공 : 결과코드, 이관 가능 여부 확인 결과(또는 이관 작업 결과) - 실패 : 결과코드, 실패사유 	<ul style="list-style-type: none"> - 이관작업이 비동기적으로 발생하는 경우는 이관 가능 여부 확인 결과가 전달되며, 동기적으로 발생하는 경우는 이관 작업 결과가 전달됨
선택	-	-

4.3.5 문서 폐기 [DeleteDocument]

공인전자문서센터에 보관 중인 전자문서를 폐기 요청할 때 이용하는 전자문서 폐기 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

이용자는 전자문서의 보관 만료일 전에 공인전자문서센터에 보관중인 전자문서를 폐기해 줄 것을 요청할 수 있고, 공인전자문서센터는 이에 대한 응답으로 전자문서를 폐기한 후, 이용자의 요청이 있을 시 원본 전자문서를 이용자에게 전송한다.

4.3.5.1 요청 [DeleteDocumentRequest]

전자문서 폐기 요청 메시지는 폐기하고자 하는 전자문서가 속한 AIP 패키지 식별자를 포함한다.

구분	파라미터	비고
필수	- AIP ID	-
선택	- 원본 전자문서 수신 여부 - 수신 시 수신 방법 및 수신주소	-

요청메시지에는 폐기하고자 하는 전자문서의 AIP ID를 필수 파라미터로 첨부하며, 원본 전자문서 수신과 관련된 정보의 경우는, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 요청메시지에서 이를 생략할 수 있다.

공인전자문서센터는 이용자 전자문서를 폐기 시 이용자의 요청이 있는 경우 이용자에게 원본 전자문서를 전송하여야 한다. 이용자가 원본 전자문서를 돌려받고자 하는 경우, 원본 전자문서 수신 여부와 수신 시 수신 방법 및 수신 주소 등을 요청메시지에 포함하여야 하며, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 요청메시지에서 이를 생략할 수도 있다.

4.3.5.2 응답 [DeleteDocumentResponse]

전자문서 폐기 요청에 대한 응답 메시지는 폐기 작업의 처리 결과를 포함하며, 실패인 경우는 실패의 사유를 포함한다.

구분	파라미터	비고
필수	- 성공 : 결과코드 - 실패 : 결과코드, 실패사유	-
선택	- 원본 전자문서(또는 전자문서 획득과 관련된 정보)	-

원본 전자문서의 경우는 응답메시지에 포함되거나, 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 응답메시지에서 이를 생략할 수 있다.

4.3.6 문서 보관 연장 [ExtendRetention]

공인전자문서센터에 보관 중인 전자문서의 보관 기간을 연장 요청할 때 이용하는 전자문서 보관 연장 서비스에 대한 요청 및 응답 메시지를 정의한다.

참고로, 보관 연장 서비스는 AIP에 설정된 보존만료일을 연장하는 서비스가 아니며, AIP에 설정된 보존만료일이 경과되지 않은 상태에서 문서보관 시스템에 설정된 실제 보관 기간을 연장하고자 할 때 이용되는 서비스이기 때문에, 본 서비스의 대상이

되는 전자문서는 반드시 AIP에 설정된 보존만료일이 경과되지 않은 상태이어야 한다.

이용자의 전자문서 보관기간 연장 요청에 대하여 공인전자문서센터는 서비스 구현 방식에 따라 동기적으로 처리하여 즉시 응답을 주거나, 처리 가능 여부에 대한 응답만을 먼저 이용자에게 보낸 후 보관기간 연장 작업을 수행한 최종 결과를 비동기적으로 이용자에게 전송할 수 있다.

문서 보관 연장 기능에 대한 구현은 공인전자문서센터의 정책상 선택적으로 구현 가능한 기능이다.

4.3.6.1 요청 [ExtendRetentionRequest]

전자문서 보관 연장 요청 메시지는 대상 전자문서 정보와 보관 만료일 정보를 포함한다.

구분	파라미터	비고
필수	- 보관기간 연장 대상 전자문서 정보	- AIP ID, 2013년 8월 28일 등록된 문서 전체, 등록된 모든 문서 등
선택	- 보관 만료일 정보	- 연장할 보관만료일을 명시하거나 현재 보관만료일에 추가될 연장기간 등

요청메시지에는 보관기간을 연장하고자 하는 전자문서 정보를 필수 파라미터로 첨부하며, 보관 만료일 정보는 사전에 공인전자문서센터와 이용자 간 해당 내용에 대한 협의가 된 경우 요청메시지에서 이를 생략할 수 있다.

일반적으로 타 공인전자문서센터로의 전자문서 보관기간 연장은 대량의 전자문서에 대하여 발생할 것이므로, 보관기간 연장 대상 전자문서 정보로는 AIP ID 이외에도 공인전자문서센터에서 연장 대상 전자문서를 명확하게 식별(구분)할 수 있는 정보면 무엇이든 가능하며, 추후 부인방지 정보로서 사용될 수 있어야 한다.

보관 만료일 정보를 설정하는 경우, 연장할 보관만료일을 명확하게 설정하거나, 현재의 보관만료일에 더해질 연장기간을 설정하도록 한다. 보관만료일을 설정한다면 GMT 또는 LocalTime 여부를 명확하게 하도록 한다.

4.3.6.2 응답 [ExtendRetentionResponse]

이용자의 보관 기간 연장 요청에 대한 보관기간 연장 가능 여부 확인 결과 또는 보관기간 연장 작업 수행결과가 포함된다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 보관기간 연장 가능	- 보관기간 연장 작업이 비동기적으로

	여부 확인 결과(또는 보관기간 연장 작업 결과) - 실패 : 결과코드, 실패사유	발생하는 경우는 보관기간 연장 가능 여부 확인 결과가 전달되며, 동기적으로 발생하는 경우는 보관기간 연장 작업 결과가 전달됨
선택	-	-

4.3.7 증명서 발급 (IssueCert)

공인전자문서센터가 수행한 전자문서 등록, 전자문서 발급, 전자문서 이관, 전자문서 폐기 서비스를 수행한 사실을 증명하는 제 증명서 및 시점확인증명서를 발급받기 위하여 이용하는 증명서 발급 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

4.3.7.1 요청 (IssueCertRequest)

증명서 발급 요청 메시지는 증명서를 발급받기 위한 증명요청서가 포함된다.

구분	파라미터	비고
필수	- 증명요청서 - 난수값(증명서 요청자가 개인인 경우)	- 증명서 요청자가 개인인 경우 요청자 정보 생성 시 사용한 난수값
선택	-	-

증명서 요청자가 개인이라면 반드시 증명요청서의 증명서 요청자 정보를 생성할 때 사용한 난수값(랜덤 넘버)을 증명요청서와 함께 공인전자문서센터에 전달해야 한다. 단, 증명서 요청자 정보를 생성하지 않은 시점확인증명요청서인 경우는 요청메시지에 난수값을 포함하지 않는다.

난수값에 대한 자세한 내용은 증명서 규격의 “4.2.1.2 requester 증명서 요청자” 및 “부록 2.1 IdentifyData의 생성” 부분을 참조한다.

4.3.7.2 응답 (IssueCertResponse)

증명서 발급 요청에 대한 응답 메시지는, 해당 증적에 대한 증명서 발급 작업의 처리 결과가 성공인 경우는 증명서에 대한 정보를 포함하며, 실패인 경우는 실패의 사유를 포함한다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 증명서	-

	- 실패 : 결과코드, 실패사유	
선택	-	-

4.3.8 증명서 갱신 (UpdateCert)

발급된 증명서가 효력 만기일 내에 있으나, 증명서에 서명한 공인전자문서센터 인증서의 유효기간이 곧 만료되거나 이미 만료되어 더 이상 증명서의 유효성을 보증하지 못하는 경우에, 이용자는 증명서의 갱신을 공인전자문서센터에 요청할 수 있고, 공인전자문서센터는 이에 대하여 갱신된 공인전자문서센터의 인증서를 사용하여 증명서를 갱신하여야 한다.

갱신된 증명서의 내용은 갱신 전 증명서의 내용과 동일하며, 다만 증명서의 이전 서명 정보를, 갱신된 공인전자문서센터의 인증서를 사용하여 생성된 새로운 서명으로 교체하여 발급하도록 한다.

4.3.8.1 요청 (UpdateCertRequest)

증명서 갱신은 새로운 증명서를 발급받는 것이 아니라 증명서의 서명정보만을 교체하는 것이므로, 요청 메시지에 증적이나 증명요청서가 포함되는 대신, 갱신 대상인 증명서의 정보가 포함된다.

구분	파라미터	비고
필수	- 증명서	-
선택	-	-

공인전자문서센터는 증명서가 해당 공인전자문서센터에서 발급된 증명서임을 확인한 후 갱신 작업을 수행하여야 한다.

4.3.8.2 응답 (UpdateCertResponse)

공인전자문서센터는 요청메시지에 포함된 증명서 정보에 대하여 공인전자문서센터가 발급한 증명서인가의 여부를 포함한 확인과정을 수행한 후, 증명서의 서명을 교체하여 이용자에게 전송한다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 갱신된 증명서 - 실패 : 결과코드, 실패사유	-
선택	-	-

4.3.9 증명서 검증 (VerifyCert)

이용자가 증명서 검증 과정의 한 단계로서 공인전자문서센터에 증명서의 폐지 여부에 대한 검증을 요청할 때 이용하는 증명서 검증 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

공인전자문서센터는 검증 대상 증명서에 대하여 폐지 여부를 확인한 후, 이용자에게 검증 결과를 전송해야 한다.

4.3.9.1 요청 (VerifyCertRequest)

증명서 검증 요청 메시지는 대상 증명서와 증명서 발급 시 증명서 요청자 개인인 경우에 생성하여 공인전자문서센터가 보관 중인 난수값에 대한 요청 여부를 포함한다.

구분	파라미터	비고
필수	- 증명서 - 난수값 요청여부(이용자 시스템에서 증명서 내의 증명서 요청자 검증 시)	- 증명서 요청자가 개인인 경우 요청자 정보 생성 시 사용한 난수값
선택	-	-

난수값은 증명서 검증 과정 중에 증명서 요청자에 대한 검증을 수행할 경우에만 요청하도록 하며, 자세한 사항은 증명서 규격의 “6. 증명서 검증” 부분을 참조하도록 한다.

공인전자문서센터는 증명서가 해당 공인전자문서센터에서 발급된 증명서임을 확인한 후 폐지 여부 확인 작업을 수행하여야 한다.

4.3.9.2 응답 (VerifyCertResponse)

증명서 검증 요청에 대한 응답 메시지에는, 해당 증명서의 폐지 여부에 대한 검증 작업의 결과가 포함된다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 난수값(요청메시지에서 난수값 요청한 경우) - 실패 : 결과코드, 실패사유	- 증명서 요청자가 개인인 경우 요청자 정보 생성 시 사용한 난수값
선택	- 성공 : 난수값	-

증명서 검증 작업 결과가 성공인 경우, 요청메시지에 난수값을 요청하였다면 응답 메시지에 난수값을 포함하고 있어야 하나, 증명서 요청자가 법인인 경우는 공인전자 문서센터에 난수값이 보관되어 있지 않기 때문에 요청메시지에 난수값을 요청하였더라도 응답메시지에 난수값이 포함되지 않음에 주의한다.

4.3.10 증명서 다운로드 (GetCert)

공인전자문서센터가 이미 발급한 증명서에 대하여 이용자가 다운로드를 요청할 때 이용하는 증명서 다운로드 서비스에 대한 요청 및 응답 메시지의 요건을 정의한다.

유효기간 만료 전인 증명서를 분실한 경우나 기타 사유에 의해서 과거에 발급된 증명서를 다운로드할 필요가 있을 때, 이용자는 공인전자문서센터에 기 발급된 증명서를 요청할 수 있고, 공인전자문서센터는 해당 증명서를 검색하여 이용자에게 전송한다.

4.3.10.1 요청 (GetCertRequest)

증명서 다운로드 요청 메시지는 다운로드하고자 하는 증명서의 식별자를 포함한다.

이용자가 증명서 다운로드 요청을 하기 위해서는 미리 증명서의 식별자를 검색하여, 요청 메시지에 해당 식별자를 설정하여야 한다.

구분	파라미터	비고
필수	- 증명서 일련번호	-
선택	-	-

4.3.10.2 응답 (GetCertResponse)

증명서 다운로드 요청에 대한 응답 메시지는, 해당 증명서에 대한 검색 작업 등의 처리 결과가 성공인 경우는 증명서를 포함하며, 실패인 경우는 실패의 사유를 포함한다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 증명서 - 실패 : 결과코드, 실패사유	-
선택	-	-

4.3.11 검색 [Search]

이용자가 공인전자문서센터 내의 전자문서, 증적 데이터, 증명서 등을 검색할 때 이용하는 검색 서비스에 대한 요청 및 응답 메시지를 정의한다.

이용자는 전자문서 발급, 전자문서 이관, 전자문서 폐기, 증명서 발급, 증명서 다운로드 등의 서비스를 요청하기 전에, 대상 전자문서의 식별자, 대상 증적의 식별자, 대상 증명서의 식별자 등을 검색하여야 하며, 이외에도 이용자가 공인전자문서센터 내의 기타 데이터에 대한 검색 및 조회 서비스를 요청할 필요가 있을 경우 본 검색 요청 및 응답 메시지 구조를 사용하도록 한다.

4.3.11.1 요청 [SearchRequest]

검색 요청메시지에는 전자문서, 증적, 증명서, 이용자 정보 등을 검색하기 위해 필요한 다양한 파라미터를 설정하도록 한다.

구분	파라미터	비고
필수	- 검색 조건	- 전자문서, 증적, 증명서, 이용자 정보 등 검색 대상에 따른 검색 조건 설정
선택	-	-

4.3.11.2 응답 [SearchResponse]

검색 응답 메시지에는 검색 결과 또는 오류 메시지가 리턴된다.

구분	파라미터	비고
필수	- 성공 : 결과코드, 검색 결과 - 실패 : 결과코드, 실패사유	-
선택	-	-

5. 보안 및 메시지 검증

5.1 개요

본 장에서는 안전하고 신뢰성 있는 메시지 송·수신을 위한 연계 인터페이스의 기본적인 보안 요건을 정의한다.

이용자시스템 및 공인전자문서센터의 연계 인터페이스는 본 장에서 제시하는 보안 요건을 반드시 준수하여야 하며, 이는 온라인 서비스의 동기식 처리 및 비동기식 처리의 전 구간은 물론, 모든 오프라인 서비스에서도 준수되어야 한다.

또한 본 규격에 제시된 연계 유형 이외에 공인전자문서센터와 이용자 시스템 간 송·수신되는 메시지의 경우도 본 장에서 제시하는 기본적인 보안 요건을 준수하여야 한다.

연계 인터페이스가 준수하여야 할 기본적인 보안요건으로는 인증, 기밀성, 무결성, 부인방지가 있다.

5.2 인증

공인전자문서센터는 공인전자문서 서비스 요청자가 해당 서비스를 이용할 수 있는 정당한 이용자인가를 먼저 확인한 후 서비스를 제공하여야 한다. 즉, 본 기술규격에서 제시하고 있는 기본적인 공인전자문서센터 서비스인 전자문서 등록, 발급, 이관, 폐기, 증명서 발급, 검증, 갱신을 비롯하여 기타 부가적인 공인전자문서 서비스 제공 시, 그리고 이용자의 개인정보 송·수신 시에는 반드시 해당 이용자가 공인전자문서센터의 이용자로 등록되어 있거나 또는 권한을 위임받은 자임을 확인하여야 한다.

반대로, 이용자도 공인전자문서 서비스를 제공받기 위하여 접속한 공인전자문서센터가 자신이 신뢰하는 공인전자문서센터인가를 확인한 후 서비스를 요청하여야 하며, 공인전자문서센터로부터 응답메시지를 수신하였을 때도 해당 응답메시지가 신뢰하는 공인전자문서센터로부터 생성된 것인가를 반드시 확인하여야 한다.

온라인 상에서는 일반적으로 이용자시스템과 공인전자문서센터 간 기밀성 유지를 위한 암호화 세션을 맺는 과정에서 1차적으로 상대의 신원을 확인하며, 수신된 상대의 메시지를 검증하는 과정 중에 메시지에 첨부된 전자서명을 검증하면서 메시지의 생성 주체를 확인하는데, 각 인증 과정은 각각 다른 의미를 가지고 있기 때문에 하나를 생략할 수 없다.

오프라인 상에서는 대면확인을 통하여 상대의 신원을 확인하도록 하며, 이에 대한 근거를 유지하여야 한다.

5.3 기밀성

온라인 상에서 이용자가 공인전자문서 서비스를 이용하는 과정 중에, 인가되지 않은 제 3자가 이용자시스템과 공인전자문서센터 간 송·수신되는 메시지 및 메시지에 포함된 데이터의 내용을 열람할 수 없어야 하며, 이를 위하여 이용자 시스템이 공인전자문서센터 시스템에 접속 시, 가장 먼저 이용자 시스템과 공인전자문서센터 간 암호화 세션이 생성되어야 한다.

암호화 세션을 생성하는 방법으로 SSL(Secure Socket Layer)V3.0을 권고하며, 이외에도 동일한 수준의 안전성이 보장된 다른 기술 방식도 가능하다.

이용자시스템과 공인전자문서센터 간 생성되는 암호화 세션은 상호인증을 기반으로 하여야 하는데, 예를 들어 SSL V3.0의 경우 해당 표준에서는 클라이언트와 서버간 암호화 세션을 맺는 과정(핸드셰이크) 중에 서로 상대의 신원을 확인하는 상호인증의 단계를 제시하고 있다.

SSL 핸드셰이크의 상호인증 시 주의할 점은 상대의 신원을 확인하는 방법으로 Peer 인증서의 유효성 확인과 더불어 신뢰하는 Peer임을 확인하여야 하는데, 이를 위하여 SSL 세션 핸드셰이크 중에 획득한 Peer의 인증서가 신뢰목록에 포함되어있는가를 확인하는 방식 이외에 접속할 수 있는 Peer의 IP를 통제하는 방식 등도 가능하다.

연계 인터페이스에서 이용자시스템과 공인전자문서센터 간 상호 신뢰하는 Peer임을 확인하는 방법으로 하기의 방식을 적용하도록 한다.

○ 웹(HTTP/S)을 이용한 송·수신 인터페이스

- ◆ 이용자의 공인전자문서센터 인증 : 웹브라우저상의 공인전자문서센터 인증서 육안 확인

○ 연계 송·수신 인터페이스

- ◆ 클라이언트의 서버 인증: 신뢰하는 서버 인증서임을 확인하거나 서버의 IP를 확인
- ◆ 서버의 클라이언트 인증 : 신뢰하는 클라이언트 인증서임을 확인하거나 클라이언트의 IP를 확인

구축된 연계 인터페이스의 종류에 따라 SSL이나 VPN과 같이 송·수신 구간 전체를 암호화하기 어려운 경우 구현된 연계 인터페이스에 적합한 암호화 처리 방식을 적용하는 것도 가능하다.

예를 들면, 온라인 서비스의 비동기 처리 방식 내 비동기 구간이나 오프라인 서비스의 경우는 기밀성을 보장하기 위한 세션 암호화가 불가능하기 때문에 각 구현 방식에

적합한 암호화 처리를 함으로써 기밀성 유지를 할 수 있어야 한다.

오프라인에서도 온라인에서와 마찬가지로 전달되는 데이터의 기밀성을 유지하기 위한 암호화를 기본적으로 적용하여야 하나, 만약 공인전자문서센터와 이용자 간 미리 협의가 된 경우, 이동 저장매체에 대한 물리적인 시건장치 및 봉인 등을 사용하여 이를 대신할 수 있다. 이 경우 공인전자문서센터는 추후 이와 관련된 분쟁이 발생하지 않도록 이용자에게 기밀성 및 암호화와 관련된 내용을 충분히 숙지시킨 후 이에 대한 근거를 유지하여야 한다.

5.4 무결성

온라인 상에서 이용자 시스템과 공인전자문서센터 간 송·수신되는 전자문서 등록, 발급, 이관, 폐기, 증명서 발급, 검증, 갱신 메시지를 비롯하여 기타 부가적인 공인전자문서 서비스 메시지 및 이용자의 개인정보 송·수신 메시지는 메시지 전송 도중 메시지의 무결성을 보장하기 위한 전자서명이 첨부되어 있어야 한다.

메시지의 무결성을 보장한다는 것은 송신자가 보낸 메시지가 수신자에게 도달하는 동안 위조 또는 변조(일부 누락 포함) 등의 보안적인 위협이 발생한 경우 이를 탐지할 수 있음을 의미한다.

전자서명의 구조 또는 전자서명이 적용되는 메시지의 구조는 각 공인전자문서센터에서 자체적인 구현이 가능하나, 전체 메시지에 대한 무결성 침해 여부를 탐지할 수 있어야 한다. (전체 메시지에 대하여 전자서명을 직접 수행할 것인지, 메시지를 몇 개의 단위로 구분하여 각 단위에 대한 해쉬값을 계산한 후 전자서명 대상에 포함시킬 것인지, 널리 알려진 표준 서명 구조를 준용할 것인지, 자체 개발한 서명 구조를 준용할 것인지 등)

즉, 메시지에 첨부된 송신자의 전자서명을 수신자가 검증함으로써, 해당 메시지의 송신자가 정당한 송신자임을 확인(위조 확인)할 수 있어야 하고, 또한 메시지가 전달되는 과정 중에 메시지의 내용이 변경되거나 일부가 누락되지 않았음을 확인(변조 확인)할 수 있어야 한다.

오프라인 상에서도 전달되는 데이터의 무결성을 유지하기 위한 전자서명을 기본적으로 적용하여야 하나, 만약 공인전자문서센터와 이용자 간 미리 협의가 된 경우, 권한 및 책임있는 담당자의 데이터 확인 후 상호 서명된 인수인계서 등을 작성하는 방식으로 이를 대신할 수 있다. 이 경우 공인전자문서센터는 추후 이와 관련된 분쟁이 발생하지 않도록 이용자에게 무결성과 관련된 내용을 충분히 숙지시킨 후 이에 대한 근거를 유지하여야 한다.

5.5 부인방지

이용자가 공인전자문서 서비스를 요청하면, 공인전자문서센터는 요청에 대한 작업 수행 후 작업 결과를 이용자에게 전달한다.

공인전자문서 서비스가 발생한 이후, 만약 이용자가 공인전자문서 서비스 요청 사실을 부인하거나, 반대로 공인전자문서센터가 해당 서비스 제공 사실을 부인하는 경우 이를 입증할 수 있어야 하는데, 이것은 요청메시지 및 응답메시지에 첨부된 전자서명을 검증함으로써 가능하게 된다.

부인방지를 위하여 메시지의 전자서명을 검증하는 방법은 무결성 검증을 위하여 전자서명을 검증하는 방식과 동일하다. 즉, 검증자는 메시지에 대한 위조 및 변조 여부를 탐지하여 이상없음을 확인해야 하며, 이를 통하여 메시지를 생성한 주체 또는 메시지의 내용에 대하여 부인하려는 시도를 차단할 수 있다.

일반적으로 송·수신된 메시지를 이용자 시스템에서 지속적으로 유지·관리하는 것은 어렵기 때문에, 공인전자문서센터는 TTP로서 모든 요청메시지 및 응답메시지를 요구되는 일정 기간 동안 유지·관리하여, 추후 부인방지를 위한 검증을 수행할 수 있어야 한다.

오프라인 상에서는 메시지(또는 데이터)에 전자서명이 적용되어 있는 경우 해당 전자서명을 유지하고 검증함으로써 온라인에서와 동일한 방식으로 부인방지를 수행하도록 하며, 만약 공인전자문서센터와 이용자 간 협의에 의하여 전자서명 대신 메시지(또는 데이터) 인수인계서가 작성되었다면 해당 서류를 근거로 부인방지를 수행하도록 한다.

5.6 전자서명 검증 시 고려사항

연계 인터페이스 메시지의 인증 및 무결성 검증을 위하여 전자서명을 검증 시에는 반드시 메시지의 전자서명에 사용된 인증서의 유효성 확인 작업도 수행되어야 한다.

인증서 유효성 확인 작업은 공인인증체계의 “공인인증서 경로검증 기술규격 [KCAC.TS.CERTVAL]”을 준용하여 검증한다.

연계 인터페이스 메시지의 생성과 검증은 거의 실시간으로 이루어지기 때문에, 생성 시에는 서명 인증서가 유효하지만, 검증 시에는 서명 인증서가 유효하지 않을 수 있는 경우는 거의 발생하지 않을 것이나, 추후 부인 방지 등을 위하여 보관 중이었던 과거의 연계 인터페이스 메시지에 대하여 현재에 검증을 수행하는 경우라면 충분히 서명 인증서의 유효기간이 만료되어 유효하지 않은 경우가 발생할 가능성이 있다.

부인방지 시 서명 인증서의 유효기간이 만료되었지만, 전자서명 장기검증 기술이 적용되었고 해당 검증 기술에 따라 검증하여 성공하였다면, 서명 인증서의 유효성 검증의 결과와는 관계없이 연계 인터페이스 메시지의 전자서명 검증에 성공한 것으로 처리한다.

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

메시지에 대한 전자서명 검증 시에는 메시지 서명자에 대한 인증 과정을 통하여 반드시 메시지 서명자가 적법한 통신 상대임을 확인하여야 한다.

메시지 서명자에 대한 인증은, 전자서명 검증에 사용된 서명자의 인증서가 통신 상대 신뢰 목록 내에 있음을 확인함으로써 이루어진다.

물론 통신 상대 신뢰 목록은 메시지 검증 시스템이 안전하게 관리하여야 한다.

메시지 서명자에 대한 인증은 이용자와 공인전자문서센터 양측에서 모두 수행되어야 한다.

만약 상대 시스템과의 통신하는 과정 중에 상대 메시지에 대한 서명검증이 실패한다면, 검증 시스템은 해당 오류의 원인을 출력하도록 하고, 상대 시스템과의 연결을 종료하도록 한다.

규 격 연 혁

버전	제 · 개정일	제 · 개정내역
v1.00	2006년 11월 28일	· 제정
v1.10	2007년 8월 27일	<ul style="list-style-type: none"> · 메시지헤더에 버전필드 추가 · 연계인터페이스 메시지 검증절차 추가 · 공인전자문서센터의 비동기식 응답에 대한 내용 추가 · 필드(엘리먼트)의 길이를 관련 규격에 맞추거나 합리적인 길이로 수정 · 오류가 있거나 규격본문과 스키마가 일치하지 않는 부분 보완
v1.11	2007년 11월 14일	<ul style="list-style-type: none"> · 목차 오류 수정 · 증명서검색응답메시지의 Nominee 필드 반복수 오류 수정
v1.20	2009년 11월 4일	<ul style="list-style-type: none"> · 증명서를 사용한 전자문서 발급 시 장기보존본이 없는 경우 원본전자문서를 발급한다는 내용 추가 · 증명서를 사용한 전자문서 발급 시, 수임자 검증을 위한 랜덤값 추가 · 증적 및 증명서 검색 시, 응답메시지의 FileIDList 옵션처리 · SSL세션 생성 과정 중 클라이언트 인증의 방법으로 IP 통제 등의 방법도 가능하도록 보완 · 보안요건 및 메시지 제약조건 등을 포함한 필수요건을 제외하고 SOAP 메시지 프로토콜에 대해서는 권고사항으로 완화
v2.00	2011년 12월 30일	<ul style="list-style-type: none"> · 전자문서 등록 시 최초등록증명서를 선택적으로 발급할 수 있도록 구조 보완 · 전자문서 발급 시 패스워드 암호화 방식 추가 · 전자문서 3자 발급 시 비암호화 방식과 패스워드 암호화 방식 추가, 전자문서 수신지로 전자메일 이외에 다른 주소도 허용 · 증명서를 사용한 전자문서 발급 요청메시지의 인

		자 중, Random Number에 대한 잘못된 설명 보완 · 패키지 규격 상 변환본이 열람용으로만 발급됨에 따라, 관련 내용 보완 · 전자문서 폐기 시 원본전자문서 발급요청 플래그 값 변경 · 문서 보관 연장 메시지 삭제
v2.10	2013년 6월 20일	· 규격 용어 현행화
v3.00	2014년 1월 1일	· 메시지 요건 완화 · 전자문서 3자 발급 삭제 · 규격 외 서비스 유형 허용 · SOAP 메시지 예시 삭제