하나금융그룹

하나아이앤에스 송수신연계모듈 “HIM” 소개

(Hanadocu Interface Module)

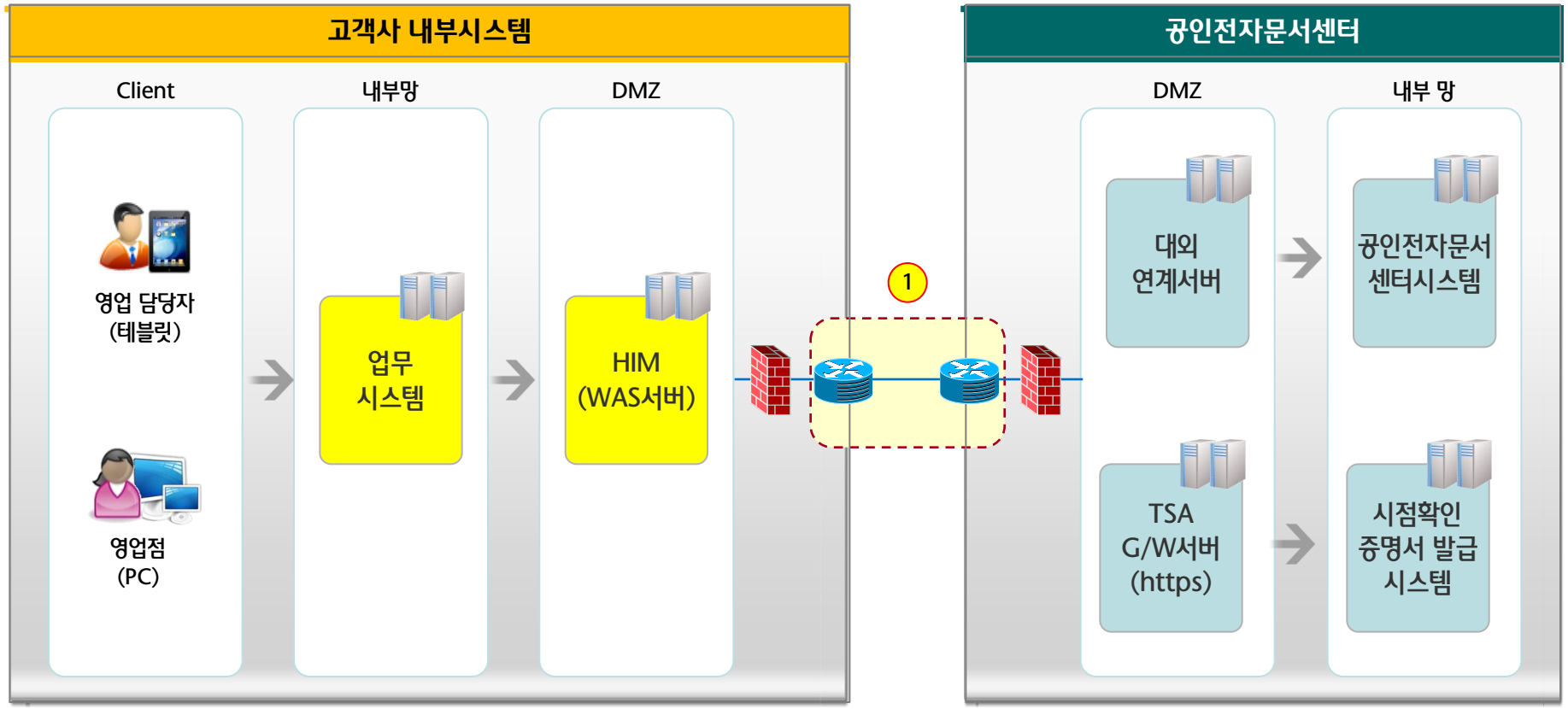
2016년 1월

하나아이앤에스

목차

1. 공인전자문서센터 대외 연계 방안 (물리적)
2. 공인전자문서센터 대외 연계 방안 (논리적)
3. 공인전자문서센터 연계 인터페이스 (구성도)
4. 공인전자문서센터 연계 인터페이스 (전문구성도)
5. 공인전자문서센터 연계 인터페이스 (메시지구조)
6. 공인전자문서센터 연계 인터페이스 (AIP구조)
7. 공인전자문서센터 연계 인터페이스 (DIP구조)
8. 공인전자문서센터 연계 인터페이스 (DIP구조)

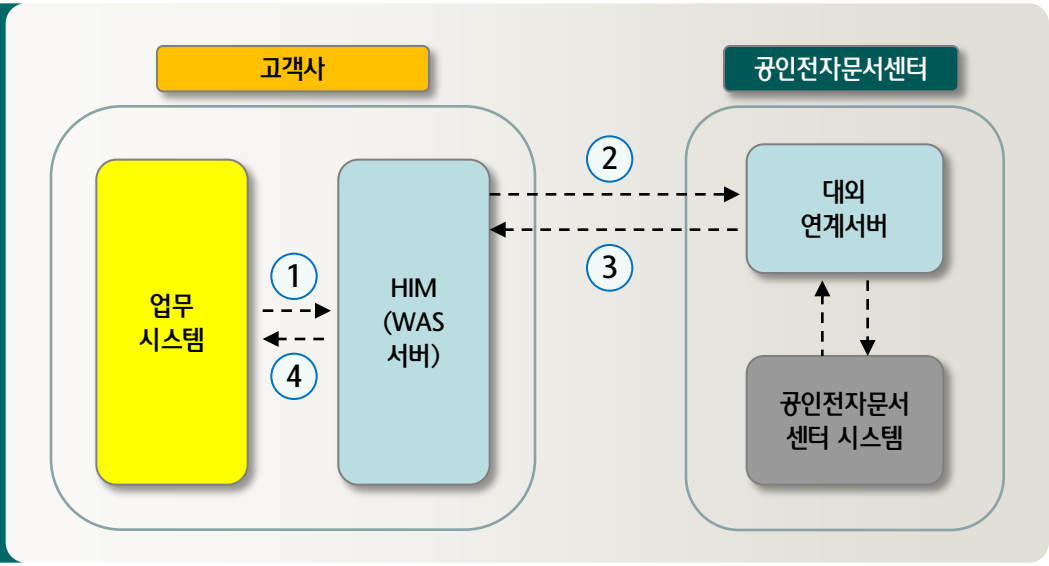
1. 공인전자문서센터 대외 연계방안 (물리적)



	구분	데이터 암호화 전송 방법	상세 내역	구축사례
1 센터간 물리적 회선 연계 방안	전용회선	SSL S/W 이용	HIM의 구간암호화 사용	- 현대카드: HIM (2015.12 적용) - KEB하나은행 : SSL S/W - 구.외환은행 : IPSec + SSL S/W
		라우터 간 IPSec 적용	Cisco 라우터 사용 시 적용 가능	
	인터넷	SSL S/W 이용	HIM의 구간암호화 사용	- 카카오페이: SSL S/W - 메리츠증권: SSL S/W - 현대,기아 자동차 : SSL S/W - 에이스손해보험 : HIM (2015.07 적용)

2. 공인전자문서센터 대외 연계방안 (논리적)

전자문서 공인전자문서센터 등록



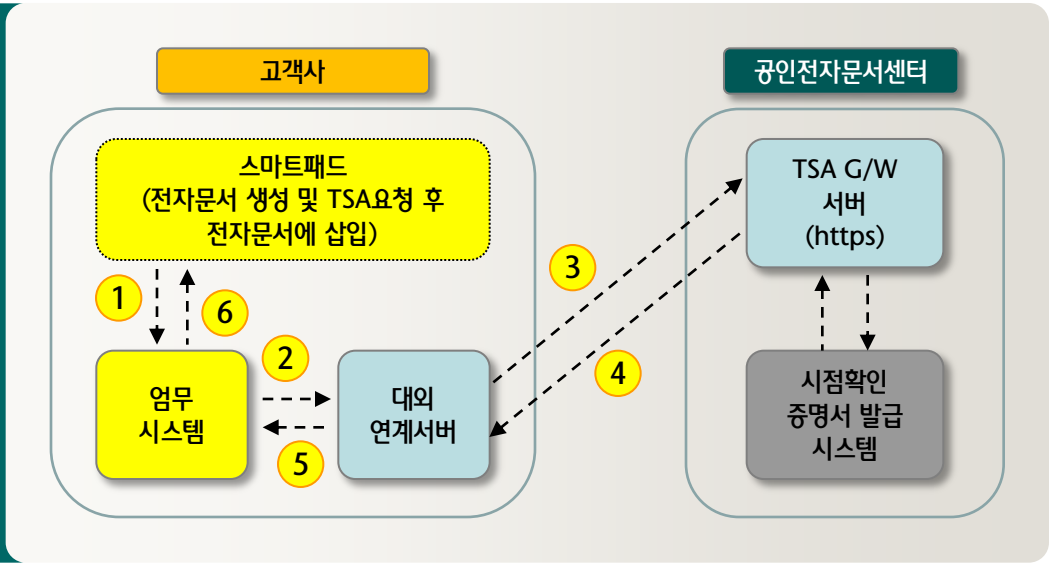
① TSA삽입된 전자문서의 등록을 대외 연계서버를 통해 진행

② 전용선 구간으로 필요 시 IPSec을 통해 전송구간을 암호화

③ ④ 등록결과 전송

※ ② ③ 구간에 전송구간 암호화는 연계 클라이언트 (HIM)의 구간암호화 기능으로 대체 가능함.

TSA 공인전자문서센터 연계



① 생성된 전자문서의 hash값 등의 정보를 업무시스템에 전달

② 전자문서의 TSA발급 요청을 위해 대외연계서버로 hash값 등의 정보를 전달

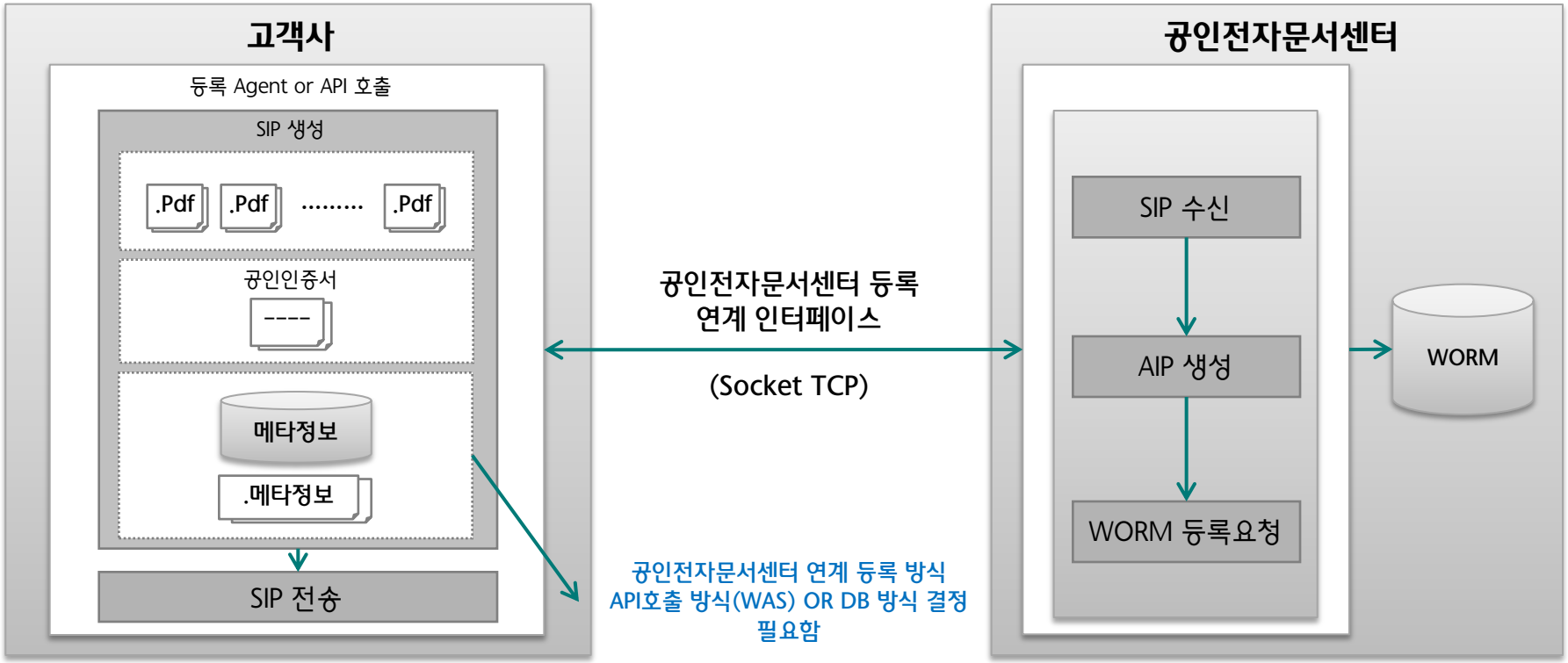
③ 공인전자문서센터에 시점확인요청 전문을 발송(https)

④ ⑤ ⑥ 시점확인증명서 발급

※ 전자문서 TSA 삽입을 업무시스템에서 수행하는 경우도 있음

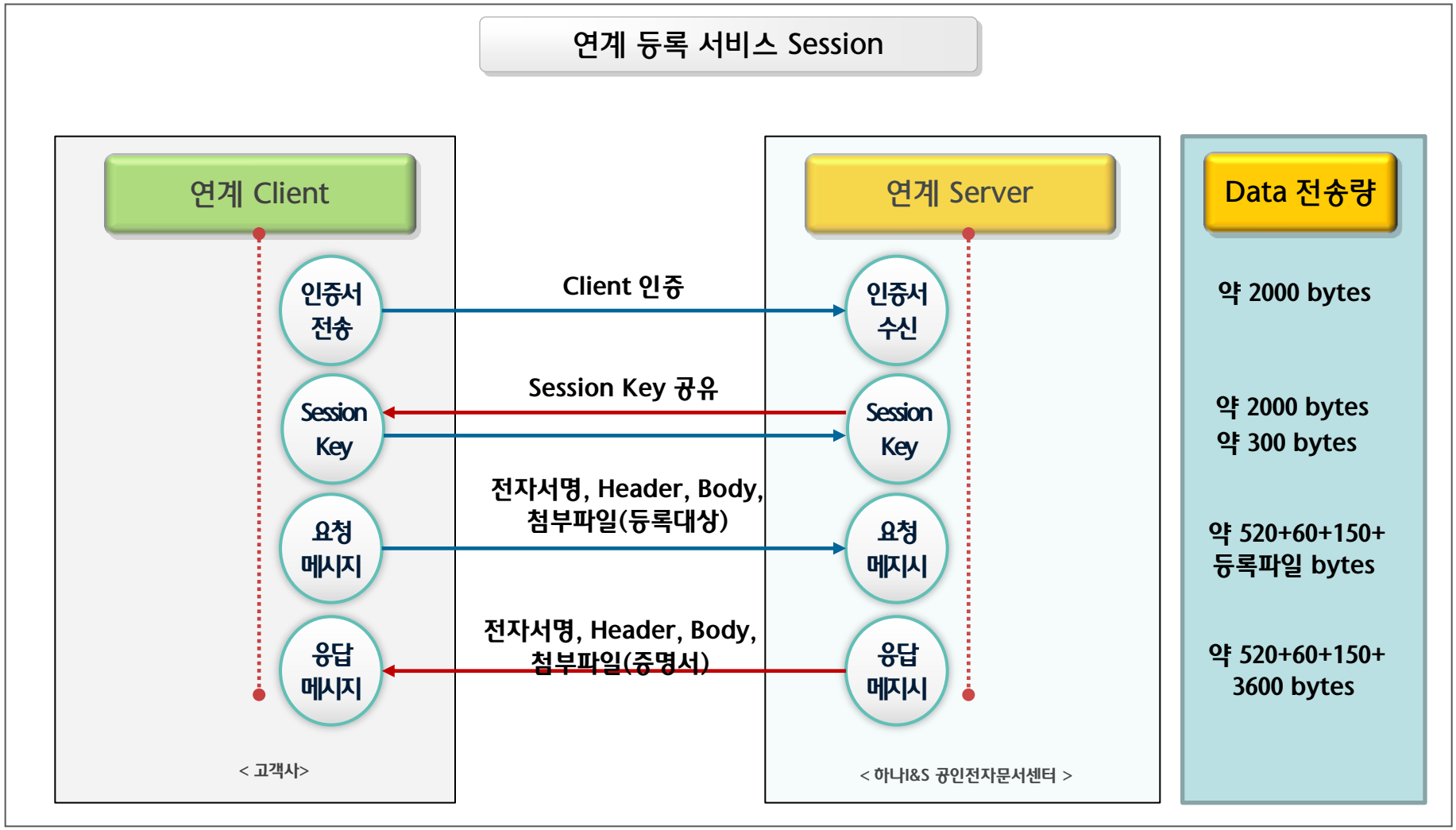
3. 공인전자문서센터 연계 인터페이스 (구성도)

- SIP – 입수 정보 패키지 (Submission Information Package)
- AIP – 보존 정보 패키지 (Archive Information Package)
- DIP – 배부 정보 패키지 (Dissemination Information Package)
- WORM (Write Once Read Many) – 한번 쓰면 지울 수 없는 없다는 개념을 구현한 솔루션으로 넷앱 의 웜 스토리지 사용을 시작으로 EMC Centera, Hitachi Hcap 순으로 증설 하였고 해당 제품에 대한 변경심사 완료
- 증명 (DCA, DVCS) 서버 – 신뢰된 기관에 증명서를 보관함으로써 문서이용자가 전자문서의 진본 여부를 확인 할 수 있도록 증명서를 생성하고 확인하게 하는 서버
- 연계 서버 – 외부와 공인전자문서센터 내의 서버들과 연결이 가능하게 하는 서버



4. 공인전자문서센터 연계 인터페이스 (전문구성도)

- TCP Socket Connection less 방식으로 하나의 연결된 session에서 내부적으로 정의된 protocol 로 Data 처리



5. 공인전자문서센터 연계 인터페이스 (메시지구조 1/3)

가. 요청메시지

메시지 필드 명					type (크기)
Message	MessageHeader (1..1)	Version			char (3byte)
		OperationType (1..1)			char (1byte)
		MessageType (1..1)			char (1byte)
		MessageID (1..1)			string (36byte)
		TimeStamp (1..1)			string (15byte)
	MessageBody (1..1)	RequestHeader (1..1)	TotalCount (1..1)		long (4byte)
		RequestBody (1..1)	RequestDataList (1..1)	RequestData (1..∞)	structure
			SlotList (0..1)	Slot (1..∞)	structure

메시지 필드 명			type (크기)	설명
SlotList (0..1)	Slot (1..∞)	Name (1..1)	string (50byte이내)	Slot을 식별하기 위한 Slot의 이름으로서, 사용하기 위해서 정의되어 있어야 함
		Value (1..1)	defined by Name	정의된 형식을 따름

5. 공인전자문서센터 연계 인터페이스 (메시지구조 2/3)

나. 응답메시지

메시지 필드 명						type (크기)
Message	MessageHeader (1..1)	Version				char (3byte)
		OperationType (1..1)				char (1byte)
		MessageType (1..1)				char (1byte)
		MessageID (1..1)				string (36byte)
		TimeStamp (1..1)				string (15byte)
	MessageBody (1..1)	ResponseHeader (1..1)	TotalResultCode (1..1)			char (1byte)
			TotalCount (1..1)			long (4byte)
			SuccessCount (1..1)			long (4byte)
			FailCount (1..1)			long (4byte)
		ResponseBody (1..1)	ResponseResult (1..1)	ResponseDataList (choice1)	ResponseData (1..∞)	structure
				FailReason (choice2)		string (500byte이내)
			SlotList (0..1)	Slot (1..∞)		structure

하나아이앤에스

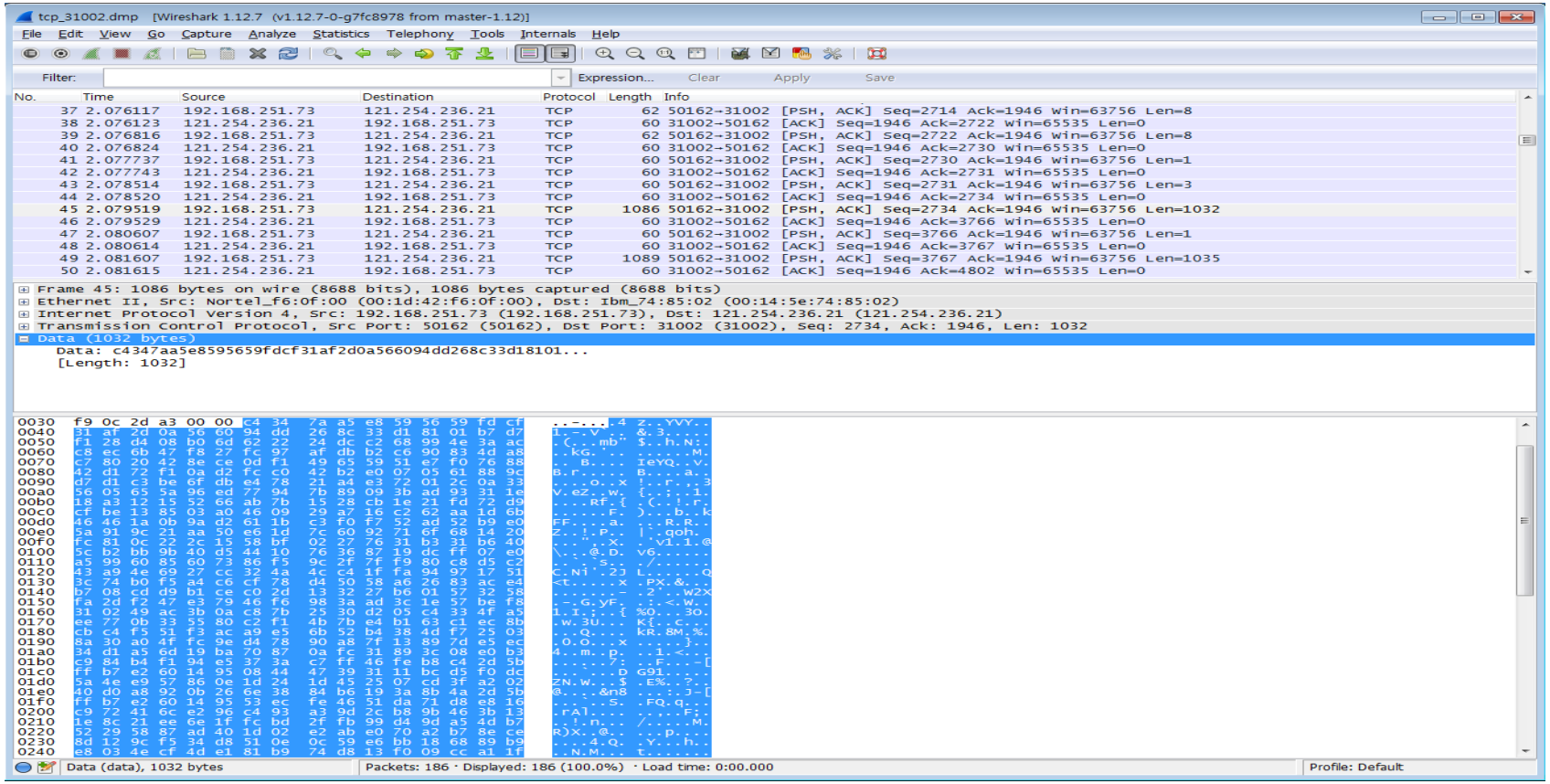
5. 공인전자문서센터 연계 인터페이스 (메시지구조 3/3)

다. 필드설명

필드명	설명	생성규칙	예
Version	연계 인터페이스 메시지 스키마의 버전	본 규격을 준용한 연계 인터페이스 메시지의 버전은 “2.0”로 설정	“2.0”
OperationType	각 작업에 대한 코드값	문서등록(1), 문서발급(2), 3자발급(3), 증명서를 사용한 문서발급(4), 문서이관(5), 문서폐기(6), 증명서발급(8), 증명서갱신발급(9), 증명서검증(a), 증명서다운로드(b), 검색(c)	‘9’ * '7'값은 사용하지 않음
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 GMT시각	"yyyymmddhhmiss" +"Z"	"20060918160959Z"
TotalResultCode	전체작업의 성공/실패 여부로서 성공이면 ResponseDataList를 처리하고 실패면 FailReason을 처리함. 전체작업에 대한 성공/실패의 판단은 보관소 정책을 따름.	성공(1), 실패(2)	‘1’
TotalCount	ResponseDataList 하위의 ResponseData의 수	TotalResultCode의 값이 실패인 경우 0	3212
SuccessCount	처리 성공한 ResponseData의 수	TotalResultCode의 값이 실패인 경우 0	3000
FailCount	처리 실패한 ResponseData의 수	TotalResultCode의 값이 실패인 경우 0	212
ResponseData	응답 작업에 필요한 인자들로 구성된 구조체	연계 유형별 응답 메시지 구조에서 정의됨	
FailReason (choice2)	string (500byte이내)	전체 작업에 대한 처리 실패 사유	보관소 시스템의 오류 메시지 형식을 따름

5. 공인전자문서센터 연계 인터페이스 (메시지 내용캡쳐)

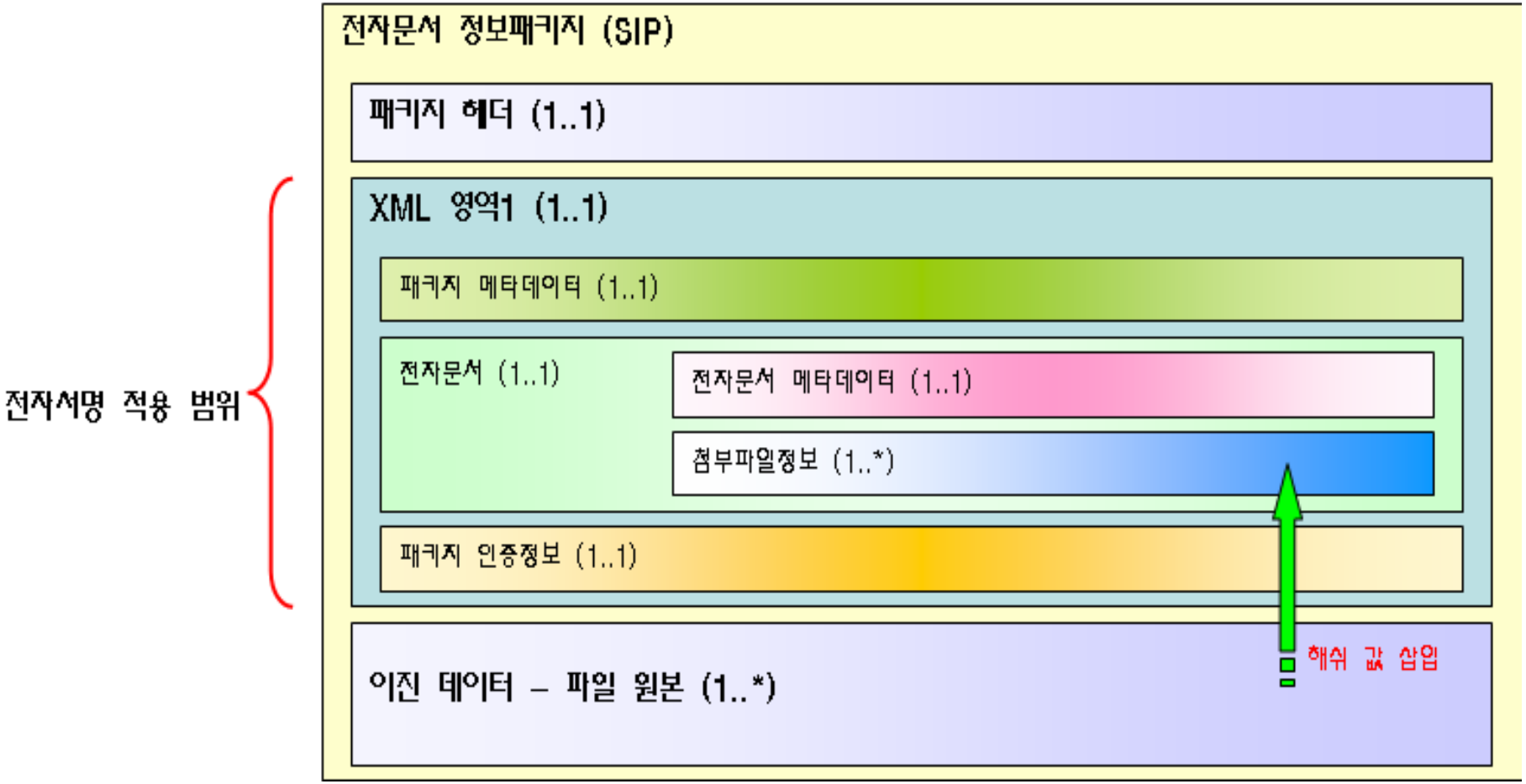
- 암호화 방식 – 대칭키 암호화 방식을 사용합니다.(키공유는 전자서명을 통해 안전하게 공유하고 있습니다.)
  암호화 대상은 요청메시지, 응답메시지, 첨부파일 입니다
- 암호화 알고리즘 – 3DES(Triple DES) 알고리즘입니다.(공인전자문서센터 연계규격 알고리즘입니다.)
- 전문구조(전문에 고객정보 유무 확인용) – 고객정보에 대한 I/F 받지 않고 있으며, 연계 전문내용 또한
  고객메타정보는 없고 등록할 content자체 data만 해당 됩니다.



하나아이앤에스

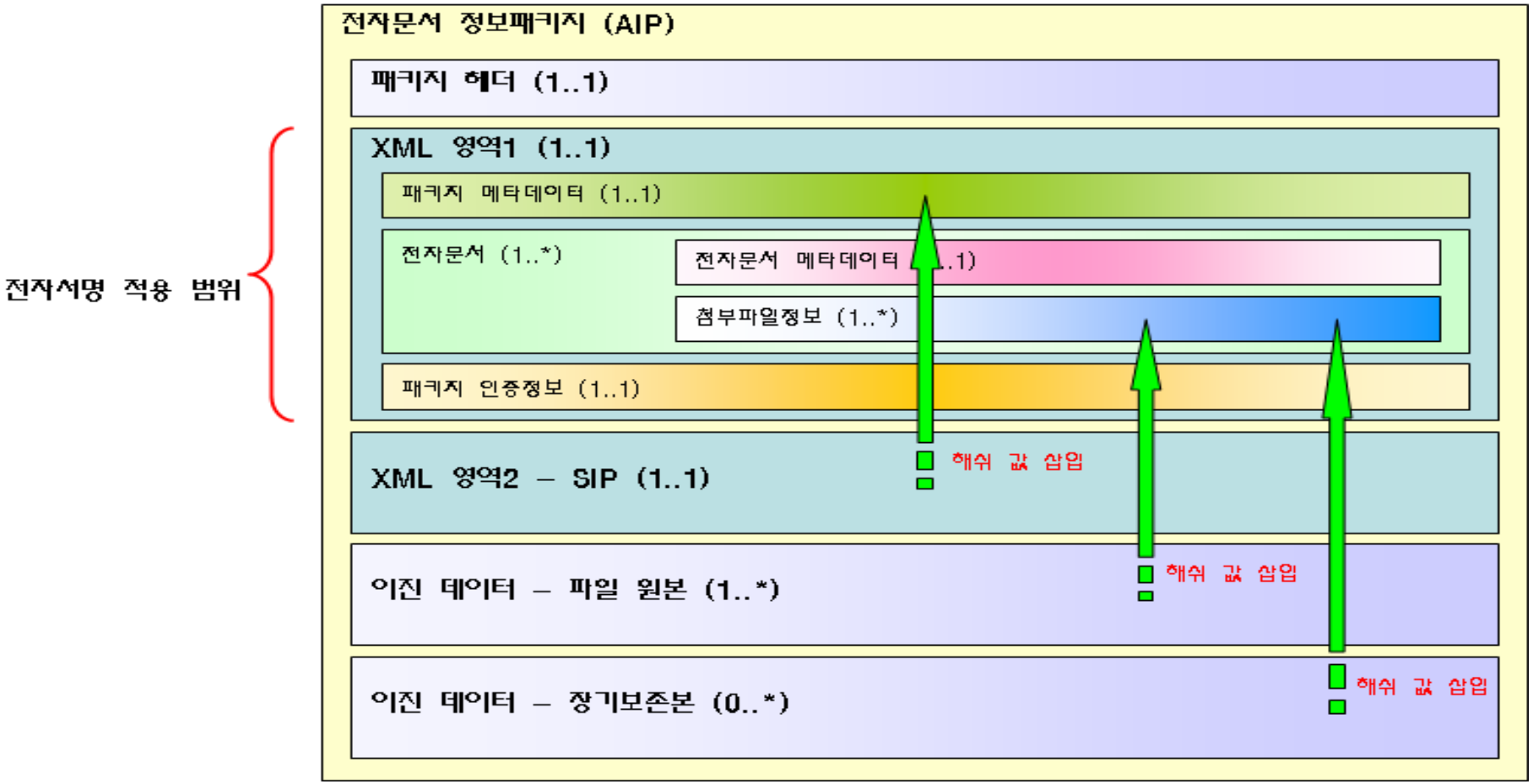
6. 공인전자문서센터 연계 인터페이스 (SIP구조)

입수 정보패키지(SIP; Submission Information Package)는 이용자의 프로그램에서 제출하여 입수되는 문서의 개념 모형을 말한다. 기본적으로 전자문서와 관련 메타데이터, 이용자의 인증정보로 구성된다.



7. 공인전자문서센터 연계 인터페이스 (AIP구조)

보존 정보패키지(AIP; Archive Information Package)는 보관소 시스템에 등록되어 적절한 관리조치를 통해 안정적으로 보관되는 전자문서의 개념 모형을 말한다. 입수 정보패키지를 보관소 시스템에 등록하는 시점에서 보존 정보패키지를 생산하게 되며, 보관소 시스템 내에서 유일한 식별자를 부여하여 관리하게 된다.



8. 공인전자문서센터 연계 인터페이스 (DIP구조)

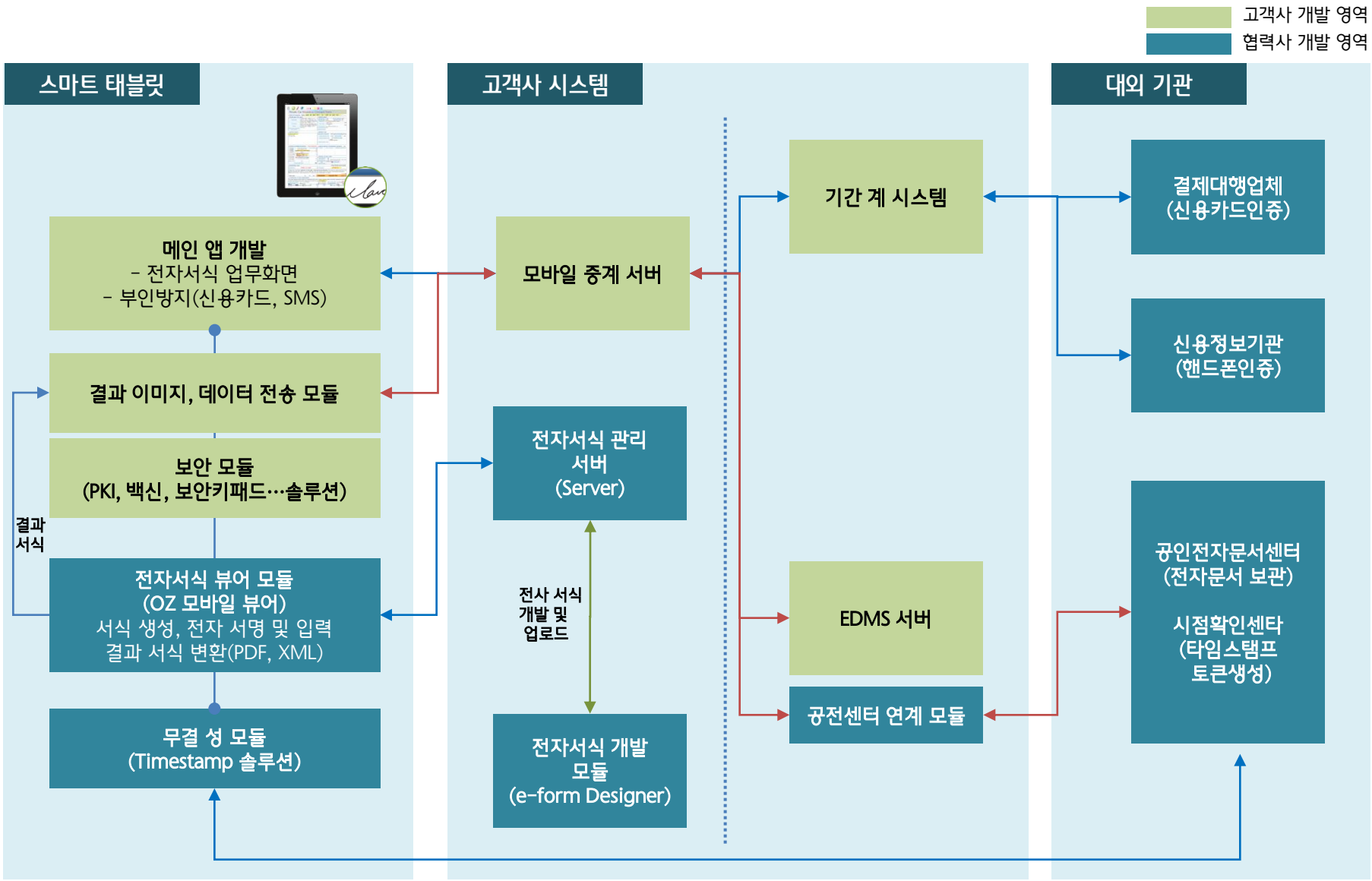
배부 정보패키지(DIP; Dissemination Information Package)는 이용자의 요청에 따라 원본 전자문서를 이용자에게 발급하거나 또는 변환본 전자문서를 이용하여 열람 서비스를 제공할 때 구성되는 전자문서 패키지 모형을 말한다. 특별히 이용자가 열람하고자 하는 변환본 전자문서가 장기보존본이 아닌 업무활용본 전자문서인 경우는 보존 정보패키지에 미리 변환되어 포함되지 않고, 배부 정보패키지 생성 시 업무활용본 전자문서 포맷으로 변환하여 포함시키는 것도 가능하다.

목차

별첨.1 전자청약시스템 개요

별첨.2 하나공인전자문서센터 연계시 필요사항 및 정보

별첨1. 전자청약시스템 개요



별첨2. 하나공인전자문서센터 연계시 필요사항 및 정보

하나공인전자문서센터 연계시 필요사항

항목	설명	비고
네트워크 구간	VPN 전용선 + HIM , 인터넷 + HIM	
고객범용인증서(서명용,암호용)	하나I&S 공인전자문서용 용도제한 인증서 발급가능 http://www.tradesign.net/ra/hanadocu.jsp	
연계이용 등록 방식	SYNC방식 연계 등록 API 샘플 소스 제공 , AGENT 방식 제공	
문서발급	http://www.hanadocu.com 이용하여 문서 발급 가능합니다.	

하나공인전자문서센터 전자문서 연계시 필요한 정보

항목	설명	비고
연계시 사용할 서버종류	AIX, HP-UX, Window 등등	
연계시 사용할 서버대수		
JDK버전 정보		
IP정보	ANY정책으로 연계 불가(TSA 서비스는 ANY정책 사용가능)	
연계 문서 종류	PDF,DOC..	
연계 문서 필요한 파라미터	문서제목,보존연한,문서ID(발급시 필요한 KEY값), 검색어, 첨부파일 설명, 문서위치,문서명 정의 필요함	

대외 연계 구축 사례 예시 (ex. 대외 시스템(EAI,FEP)을 통하지 않고 WAS서버에서 공전소 연계서버 통신)

고객사	연계등록방식	구현방식
현대카드	전용선 + HIM	API 이용 BATCH방식(샘플 소스 제공)
에이스손해보험	인터넷 + HIM	API 이용 BATCH방식(샘플 소스 제공)
현대.기아자동차	인터넷 , SSL S/W + 연계클라이언트	API 이용 WAS 서블릿방식 호출
메리츠증권	인터넷 , SSL S/W + 연계클라이언트	API 이용 BATCH방식(샘플 소스 제공)
카카오페이	인터넷 , SSL S/W + 연계클라이언트	DB 폴링 방식 AGENT

End of Documents.