


사설인증서 기반 통합인증 절차 및 규격

(2021.9., 금융보안원 마이데이터팀)

 **본 문서는 전자서명법상 인정받은 전자서명인증사업자*의 사설인증서비스에 기반한 통합인증 절차 및 규격에 해당**

* 전자서명법 제7조제2항에 따른 “운영기준” 준수사실을 인정받은 전자서명인증사업자

1 개 요

- **(목 적)** 정보주체의 통합인증수단 선택권 보장 및 편리한 서비스 이용을 위한 인정받은 전자서명인증사업자(이하 ‘인증기관’)* 기반 통합인증 절차 및 규격을 제시

* 통합인증 사업 참여 절차(별도 안내)에 따라 참여한 인정받은 전자서명인증사업자

- **(방 향)** 정보제공자 및 마이데이터사업자의 인증서비스 적용 비용 및 기간 최소화를 최우선 고려

2 공통 기준

- **(인증서 선정)** 마이데이터사업자는 사설인증서를 최소 1개 이상 도입하고, 정보제공자는 통합인증에 허용된 모든 인증서 허용

* 마이데이터겸 전자서명인증사업자의 경우 자체 인증서 외 타 인증서 적용 필수
(마이데이터사업자의 모·자회사가 인증사업자인 경우에는 해당 인증서도 자체 인증서에 포함)

- **(적용비용 최소화)** 추가 모듈 도입 없이도 전자서명을 생성 및 검증할 수 있는 인증 앱* 및 위임 검증** 방식 선정

* 인증 앱 이외 방식(웹 방식 등)은 개별 인증기관이 모듈 및 지원 등을 무상 제공

** 각 인증기관은 정보제공자가 필요시 자체 검증을 수행할 수 있도록 방안 제공

(예: 체인검증에 필요한 루트 및 중간 CA 인증서 제공 등)

□ **(신원확인)** 인증서 발급시, **실명확인 등 안전한 신원확인*** 기준

* 예시) 실명확인, 본인확인 + 계좌점유인증(1원 이체 등) 등

□ **(표준 API)** 인증기관 추가 등 확장성을 고려하여 **표준 API** 방식으로 인증기관과 정보제공자 및 마이데이터사업자 간의 요청·응답 처리

* 본 규격에서 정한 사항 이외에는 ‘금융분야 마이데이터 표준 API 규격’, ‘인증서 본인확인 기반 통합인증 절차 및 규격’ 준용

□ **(고객 단말 보호)** 고객 단말을 통한 인증정보 유출 등을 방지하기 위해 **안전한 방식***으로 인증서를 저장하고, 보안 키패드, 앱 위변조 탐지, 백신** 등의 **보호 대책** 적용

* H/W 및 S/W 기반의 안전한 방식(또는 이에 준하는 보안 수준)

** 고객 단말의 운영환경 등을 고려하여 적용

□ **(인증정보 보호)** 통신구간은 **TLS 암호화(mTLS)**를 적용하고, 인증정보 재전송 공격에 대한 대책(타임스탬프*, Nonce 등) 적용

* 전자서명 유효시간은 최대 1시간 이내에서 서버 및 네트워크 환경을 고려하여 설정(10분 내외 권장)

○ 인증기관→정보제공자 간 **CI** 제공시 관계기관 요구 등에 따라 추가 암호화가 필요한 경우, 인증기관이 **암호화(AES-256 등)** 하여 제공*

* 정보제공자가 암호화된 CI를 복호화하는데 필요한 암호 키는 각 인증기관이 클라이언트 자격증명(client_id, client_secret) 발급시 안전하게 제공

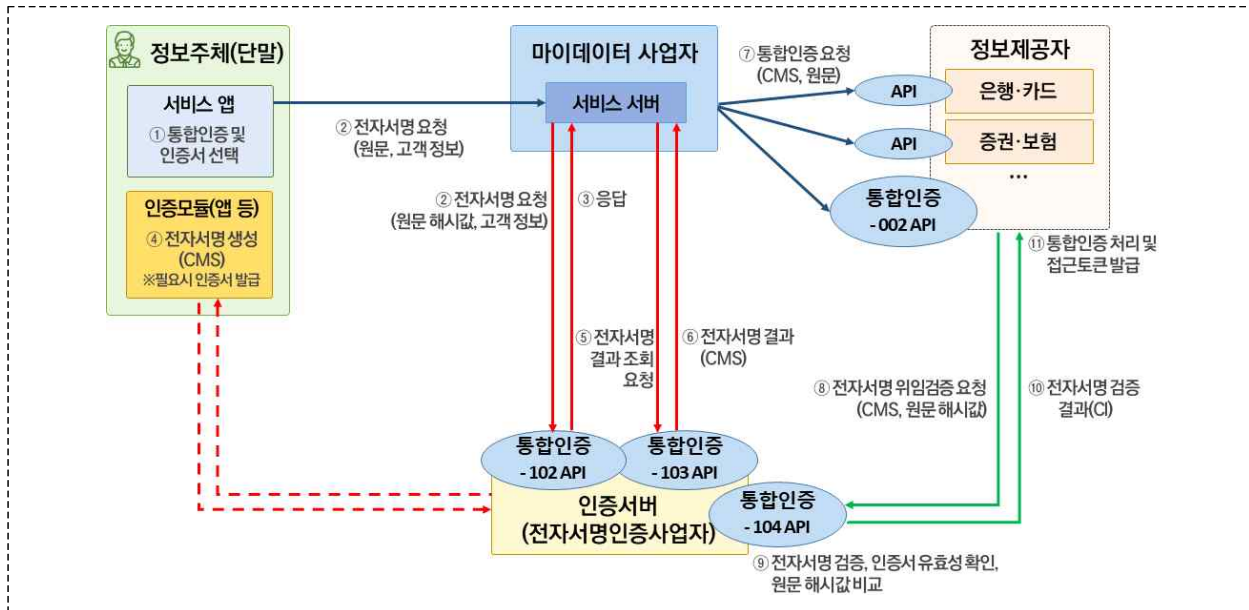
□ **(개인정보 보호)** 개인(신용)정보 유출 최소화를 위해 전송요구 내역의 **해시 값**을 대상으로 전자서명 생성 및 검증

□ **(기 타)** 각 인증기관은 통합인증을 위한 약관 및 동의서 등과 마이데이터서비스 등 기관 간 연동에 필요한 지원을 충실히 제공

※ 각 인증기관은 **통합인증서비스(상기 요건 포함)**를 전자서명법상 문제없이 제공 가능하도록 전자서명법상 평가·인정기관을 통해 확인 必

3 통합인증 절차 및 규격

《 통합인증 구성 및 절차 》



□ (절차) 0 사전준비 → 1 통합인증 요청 → 2 전자서명 검증 및 인증처리 단계에 따라 처리

0 (사전준비) 정보제공자는 고객 CI를 수집(일괄변환 등)하고, 정보주체는 인증서 발급(사전 미발급시에는 통합인증수행시 발급)

- 정보제공자 및 마이데이터사업자는 각 인증기관의 안내에 따라 클라이언트 자격증명(client_id, client_secret)을 발급
- 클라이언트 자격증명을 사용하여 인증기관으로부터 통합인증 API 요청에 필요한 접근토큰*을 발급(통합인증-101 API)

* 통합인증-102~104 API 요청용 접근토큰의 유효기간은 최장 1년(리프레시 토큰 미지원)

1 (통합인증 요청) ① 고객은 전송요구서 작성 및 인증서를 선택

②~③ 마이데이터사업자는 해당 인증기관에게 전송요구내역(해시 값)에 대한 전자서명을 요청(통합인증-102 API)

④ 고객 인증을 통해 전자서명 생성(재전송 공격 방지 대책 적용)

⑤~⑥ 마이데이터사업자는 인증기관에게 전자서명 결과를 요청
(통합인증-103 API)

⑦ 정보제공자에게 통합인증을 요청(통합인증-002 API)

※ (참고) 마이데이터 사업자가 인증 앱 이외 방식을 제공하는 인증기관을 선정 및 적용하는 경우에는 통합인증-101~103 API가 아닌 해당 인증기관의 규격에 따라 전자서명 요청 등을 처리 가능

2 (전자서명 검증 및 인증처리)

⑧ 정보제공자는 인증기관에게 전자서명 위임 검증을 요청
(통합인증-104 API)

⑨~⑩ 인증기관은 전자서명을 검증한 후, 해당 결과(CI 포함)를
정보제공자에게 제공하며,

⑪ 정보제공자는 인증처리 및 접근토큰을 발급

□ API 목록

API ID	API 명	URI			HTTP Method
		version	industry	resource	
통합인증-101	통합인증용 접근토큰 발급 요청 * 제공 : 인증기관 호출 : 마이데이터 정보제공자	해당 없음	해당 없음	/oauth/2.0/token	POST
통합인증-102	전자서명 요청 * 제공 : 인증기관 호출 : 마이데이터	v1	ca	/sign_request	POST
통합인증-103	전자서명 결과 조회 * 제공 : 인증기관 호출 : 마이데이터	v1		/sign_result	POST
통합인증-002	접근토큰 발급 요청(통합인증 요청) * 제공 : 정보제공자 호출 : 마이데이터	해당 없음	해당 없음	/oauth/2.0/token	POST
통합인증-104	전자서명 위임 검증 * 제공 : 인증기관 호출 : 정보제공자	v1	ca	/sign_verification	POST

※ [첨부 1] 사전 준비 및 상세 절차

※ [첨부 2] 사설인증서 기반 통합인증 API 명세

1. 사전 준비

□ (공통 준비사항) 마이데이터 생태계 참여를 위한 공통 준비사항

- 마이데이터사업자, 정보제공자, 통합인증기관은 각자의 역할에 따라, 마이데이터 생태계 참여를 위한 ‘기관정보 등록’, ‘서비스정보 등록’, ‘종합포털과 접속 채널 등 설정’ 수행*

* ‘금융분야 마이데이터 표준 API 규격’ - ‘3.1 사전준비’ 참고

□ (통합인증 준비사항) 사설인증 기반 통합인증 준비사항

가. 참여기관 공통

- ‘통합인증 공동업무규약’ 참가

- 정보제공자(중계기관), 마이데이터사업자, 인증기관은 ‘통합인증 공동업무규약’ 참가

* 필요시 공동업무규약과 동일한 효력을 갖는 계약(약관 등)으로 대체 가능

- 마이데이터사업자는 인증서 선정과 관련하여 필요시 인증기관과 별도의 계약 등 체결

나. 정보제공자 및 중계기관

① 고객 CI 정보 수집(全 정보제공자)

- 정보제공자는 고객에게 본인확인서비스(예: 휴대폰/인증서/신용카드 본인확인)를 요구하거나, 또는 CI 일괄변환*을 통해 고객 CI 정보를 수집

* 안전한 CI 저장·관리를 위해, 주민번호와 CI 분리저장(필수), CI 저장시 암호화(권고) 필요(세부 기준은 보안수준 등을 고려하여 자체 판단)

☞ (지원 담당) 아이핀 본인확인기관(NICE평가정보, KCB, SCI평가정보)

② 통합인증 개발(API 직접구축 정보제공자, 중계기관)

— 통합인증-101, 통합인증-104 API 호출 개발(첨부2)

☞ (지원 담당) 인증기관, 마이데이터 지원기관(신용정보원, 금융보안원)

③ 인증기관과 연동 준비(API 직접구축 정보제공자, 중계기관)

— 기관정보 조회 API(지원-002)를 통해 인증기관의 정보*를 수집

* 기관코드(org_code), API 도메인(IP 및 서비스 포트 포함) 정보

— 인증기관 정보를 시스템 및 방화벽 등에 적용하고 연동 테스트 수행

— 인증기관을 통해 클라이언트 자격증명(client_id, client_secret)을 발급받고, 통합인증-101을 호출하여 통합인증-104 API 호출용 접근토큰 발급

☞ (지원 담당) 인증기관

다. 마이데이터 사업자

① 고객 CI 정보 수집

- 서비스 회원 가입시 고객에게 본인확인서비스를 요구하여 고객 CI 정보를 수집

③ 통합인증 개발

- 통합인증-101, 통합인증-102, 통합인증-103 API 호출 개발(첨부2)

※ (참고) 인증 앱 이외 방식을 적용하는 경우에는 통합인증-101~103 API가 아닌 해당 인증기관의 규격에 따라 필요 기능 개발

- 필요시 인증앱과의 앱 to 앱 호출을 위한 앱 URL(app scheme URL 등) 등록 등을 수행

☞ (지원 담당) 인증기관, 마이데이터 지원기관

② 인증기관과 연동 준비

- 기관정보 조회 API(지원-002)를 통해 인증기관의 정보*를 수집

* 기관코드(org_code), API 도메인(IP 및 서비스 포트 포함) 정보

- 인증기관 정보를 시스템 및 방화벽 등에 적용하고 연동 테스트 수행

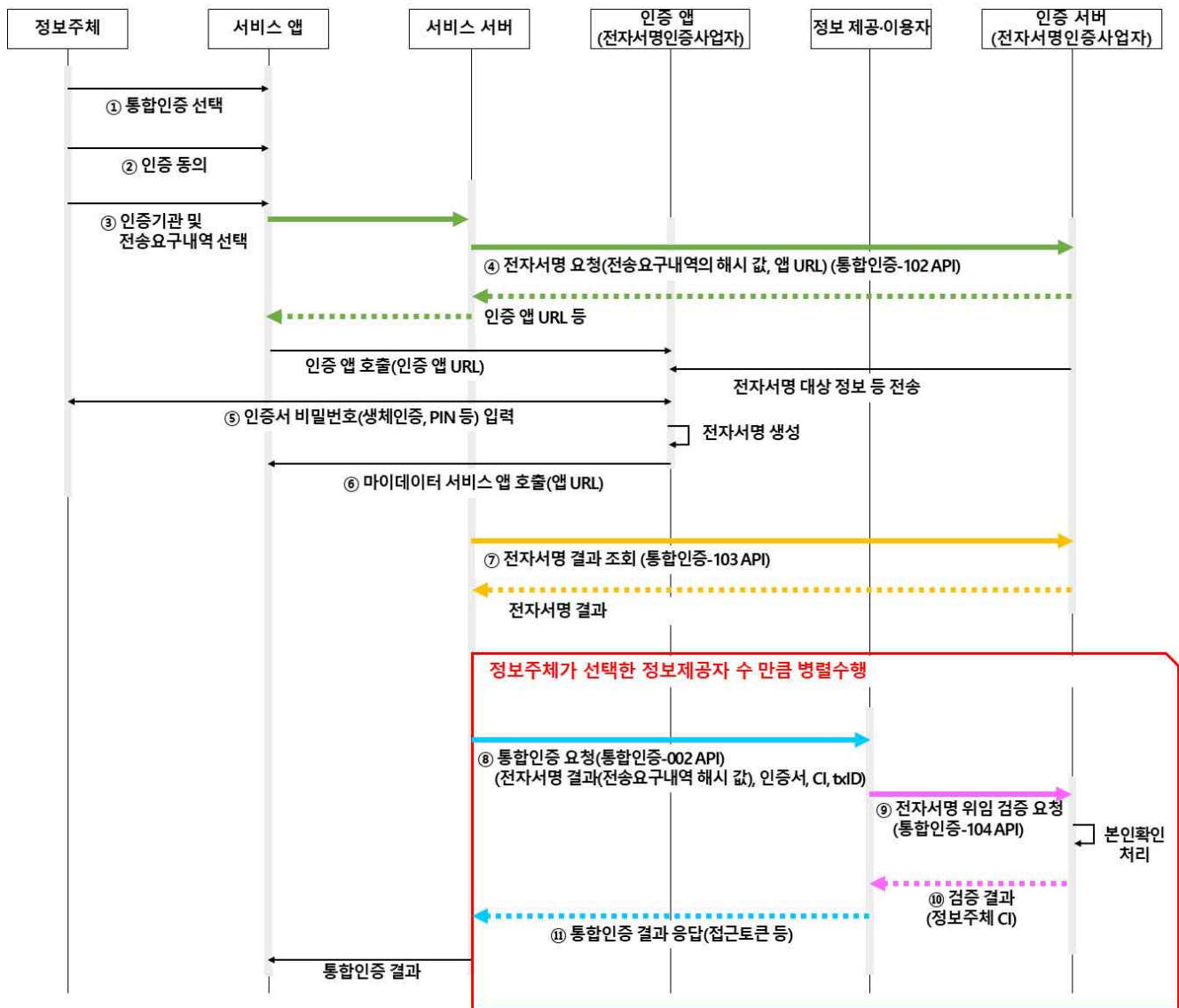
- 인증기관을 통해 클라이언트 자격증명(client_id, client_secret)을 발급받고, 통합인증-101 API를 호출하여 통합인증-102, 통합인증-103 API 호출용 접근토큰 발급

☞ (지원 담당) 인증기관, 마이데이터 지원기관

라. 인증기관

- 통합인증 API 호출을 위한 클라이언트 자격증명(client_id, client_secret) 발급 방안 및 통합인증-101~104 API 구축
 - 종합포털(신용정보원)에 통합인증에 필요한 기관정보* 등록
 - * 기관코드(org_code), API 도메인(IP 및 서비스 포트 포함) 정보
 - 기관정보 조회 API(지원-002)를 통해 정보제공자 및 마이데이터 사업자의 정보를 수집*
 - * 기관코드(org_code), IP 주소, TLS 인증서 시리얼번호 등
 - 정보제공자 및 중계기관, 마이데이터사업자 정보를 시스템 및 방화벽 등에 적용하고 연동 테스트 수행
- ☞ (지원 담당) 마이데이터 지원기관

2. 상세 절차



- ① **(정보주체)** 마이데이터 서비스 회원가입 후 해당 서비스 앱에 로그인하여 인증방식으로 통합인증을 선택
- ② **(정보주체)** 마이데이터 서비스 앱을 통해 통합인증을 위해 필요한 동의문을 확인 및 동의
- ③ **(정보주체)** 마이데이터 서비스 앱을 통해 전송요구할 대상 정보제공자를 선택 및 전송요구 내역을 특정하고, 인증기관(인증서)을 선택

- 마이데이터사업자는 서비스앱을 통해 신용정보법 제33조의2제5항에 의거, 정보주체가 전송요구내역을 특정할 수 있도록 화면을 구성 및 제공 필요
- 정보주체가 특정한 사항을 규격에 따라 전송요구내역*으로 생성
- * “인증서 본인확인 기반 통합인증 절차 및 규격”의 [첨부6] 참고

《 보유 자산의 수가 매우 많은 고객에 대한 처리 》

- (이슈) 일부 은행 고객 등은 보유 계좌(여·수신, IRP 계좌 등)의 수가 수백, 수천개에 달해, 전송요구내역의 크기가 API를 통해 전송 가능한 크기를 초과하여 전송이 불가능
 - * 현재, 통합인증 API 규격상 전송요구내역의 전송 크기는 7,000 Byte이므로, 보유 계좌 수가 약 234개를 초과하는 경우에는 전송요구내역 전송이 불가(계좌 번호 길이를 30Byte로 가정, $30 \times 234 = 7020(7000 \text{ 초과})$)
- (처리 방법) **고객이 다수 계좌를 선택하여** 상기 이슈로 인해 해당 정보제공자를 대상으로 전송요구가 불가능한 경우에 한하여, “전송을 요구하는 개인신용정보”에 대한 전송 메시지 생성시 자산 목록을 모두 열거하지 않고, 전체 자산(“all_asset”)으로 명시하여 생성([첨부6] 참고)
 - “전체 자산”은 해당 전송요구 시점에 고객이 보유한 전체 자산을 의미하며, 향후 신규 추가된 자산은 포함되지 않음(신규 전송요구 필요)
 - 해당 고객에게는 해당 정보제공자 대상으로는 전송을 요구할 자산을 선택할 수 없으며, 전체 자산의 전송요구만 가능함을 안내
 - **고객이 최초 전송요구(all_asset) 후에 추가 계좌 개설을 하고, 이후 일부 전송요구내역을 변경하고자 전송요구를 다시 하게되는 경우, 추가 계좌도 전송요구에 포함됨을 고객에게 안내**

- ④ (마이데이터사업자) 고객이 한번에 다수 정보제공자별 전송요구내역에 대하여 정보주체가 통합인증서를 이용하여 전자서명을 생성할 수 있도록 인증기관에 전자서명 생성을 요청(통합인증-102 API)
- 통합인증-102 API 호출시 전자서명 대상 값으로 전송요구내역의 원문이 아닌 해시 값(SHA-256)을 제공하고,
 - 고객이 이용중인 단말(device_code) 및 서비스 형태(device_browser)와 함께, 고객이 모바일 앱을 이용 중인 경우에는 해당 앱의 앱 URL(return_app_scheme_url)을 함께 제공

- 고객이 모바일 앱을 이용 중인 경우에는 통합인증-102 API 호출 결과로 인증 앱의 앱 URL(sign_ios_app_scheme_url, sign_aos_app_scheme_url)이 반환되므로, 이를 이용하여 인증 앱을 호출
 - * 고객이 PC, 테블릿, 모바일 웹 브라우저 등을 이용 중인 경우에는 인증 기관에서 PUSH 방식으로 인증 앱을 호출
- ⑤ **(정보주체)** 인증 앱을 통해 전송요구내역의 요약 정보 등을 확인하고 전자서명 생성을 위한 인증정보(생체, PIN 등)를 입력
- ⑥ **(인증기관)** 전자서명 생성 완료 후, 고객이 모바일 앱을 이용 중인 경우, 인증 앱에서 마이데이터 서비스 앱을 호출(return_app_scheme_url 호출)
- * 고객이 PC, 테블릿, 모바일 웹 브라우저 등을 이용 중인 경우에는 고객이 마이데이터 서비스에서 '인증 완료' 버튼을 클릭
- ⑦ **(마이데이터사업자)** 인증기관에 전자서명 생성 결과 조회를 요청(통합인증-013 API)하여, 생성된 전자서명을 수신
- ※ (참고) 인증 앱 이외 방식을 적용하는 경우에는 상기 절차(④~⑦, 통합인증-102 및 103 API)가 아닌 해당 인증기관의 규격에 따라 전자서명 요청 등을 처리 가능
- ⑧ **(마이데이터사업자)** 전자서명과 종합포털로부터 발급받은 "서비스 자격증명"(client_id, client_secret) 등을 이용하여 각 정보제공자에게 병렬적으로 접근토큰을 요청(통합인증-002 API)
- API를 통해, 고객 CI, 전송요구내역에 대한 전자서명(password), 전송요구내역 원문(cosent), 트랜잭션 ID(tx_id), 인증기관 기관코드(ca_code)를 전송
- ⑨ **(정보제공자)** 전송요구내역에 대한 전자서명*을 다음 절차에 따라 검증(순서 보장)
- * 전자서명은 전송내역 보관 기준(기술 가이드라인)에 따라 저장·관리 필요

1) (고객 여부 확인) API를 통해 전송받은 CI를 이용하여 자사 고객 중에서 CI가 일치하는 고객이 있는지 여부를 확인(CI 일치 고객이 없는 경우 거부*)

* 자사고객이 아닌 경우에는 2) 전자서명 위임 검증을 수행하지 않고 즉시 에러 반환

2) (전자서명 위임 검증) 통합인증-002 API를 통해 전송받은 전송요구내역의 전자서명(password)에 대해 해당 인증서 발급기관(인증기관)으로 전자서명 위임 검증을 요청(통합인증-104 API)

- 위임 검증을 위해, 통합인증-002 API를 통해 전송받은 전송요구내역 원문(consent)*의 해시 값(SHA-256)을 생성하여 함께 제공

* 통합인증-002 API를 통해 전송받은 consent는 UTF-8 인코딩된 상태이며, 인코딩된 상태에서 해시 값 생성

⑩ (인증기관) 통합인증-104 API를 통해 전송받은 전자서명(signed_consent)을 검증 및 전송요구내역 원문의 해시 값(consent)과 동일 여부를 검증하고, 인증서 유효성 확인 등을 수행하여, 위임 검증 결과(CI 포함)를 정보제공자에게 제공

⑪ (정보제공자) 위임 검증 결과 등을 토대로 정보주체를 인증(CI 활용)한 후, 접근토큰을 발급하여 마이데이터 사업자에게 제공(⑧에 대한 응답)

⑫ (마이데이터사업자) 통합인증 결과를 고객에게 안내 및 접근토큰을 이용하여 개인신용정보를 요청·수집

* 통합인증을 요청한 다수 정보제공자 중에서 일부 정보제공자에서 인증이 실패한 경우에는 해당 기관에서만 통합인증이 재요청되도록 처리

첨부 2

사실인증서 기반 통합인증 API 명세

□ (통합인증-101) 통합인증용 접근토큰 발급 요청

○ 기본 정보

API ID	통합인증-101	HTTP Method	POST
API 제공자	인증기관(전자서명인증사업자)	API 요청자	마이데이터사업자, 정보제공자
API 명 (URI)	/oauth/2.0/token		
설명	각 인증기관이 사전에 발급한 통합인증 API용 자격증명을 이용하여 접근토큰 발급 • 중계기관을 이용하는 기관의 경우, 중계기관이 본 API를 호출하여 접근토큰을 대표로 발급 받음		
기준시점	현재 시점		
Content-Type (요청)	application/x-www-form-urlencoded	Content-Type (응답)	application/json; charset=UTF-8

○ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
	grant_type	권한부여 방식	Y	aNS (18)	권한부여 방식('client_credentials' 고정값)
Body	client_id	클라이언트 ID	Y	aN (50)	각 인증기관이 발급한 클라이언트 ID 값
	client_secret	클라이언트 Secret	Y	aN (50)	각 인증기관이 발급한 클라이언트 Secret 값
	scope	권한 범위	Y	a (6)	고정값: 'ca'

○ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
	token_type	접근토큰 유형	Y	a (6)	접근토큰 유형('Bearer' 고정값)
Body	access_token	접근토큰	Y	aNS (900)	발급된 접근토큰
	expires_in	접근토큰 유효기간	Y	N (9)	접근토큰 유효기간(단위: 초)
	scope	권한 범위	Y	a (6)	고정값 : 'ca'

○ 에러메시지 명세 (RFC 6749 준용)

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	error	에러코드	Y	aNS (30)	에러코드 • 표준API 규격 [첨부1]-[2] 참조
	error_description	에러메시지	N	AH (450)	에러메시지 • 표준API 규격 [첨부1]-[2] 참조

□ (통합인증-102) 전자서명 요청

○ 기본 정보

API ID	통합인증-102	HTTP Method	POST
API 제공자	인증기관	API 요청자	마이데이터사업자
API 명 (URI)	/ca/sign_request		
설명	마이데이터사업자가 인증기관에게 전송요구내역에 대한 전자서명을 요청		
기준시점	현재 시점		
Content-Type (요청)	application/json; charset=UTF-8	Content-Type (응답)	application/json; charset=UTF-8

○ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	Authorization	접근토큰	Y	aNS (1500)	발급된 접근토큰 • 접근토큰 유형(Bearer)을 명시 예) Authorization: Bearer 접근토큰
	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	sign_tx_id	서명 요청 트랜잭션 ID	Y	aNS (49)	마이데이터 사업자가 생성 '마이데이터사업자 기관코드(10)_' '인증기관 기관코드(10)_' '전자서명 요청 시간'(YYYYMM DDHHMMSS)(14)_' '일련번호(12)'
	user_ci	정보주체 식별값	Y	B64 (100)	정보주체 식별을 위한 연계정보 (Connection Information)
	real_name	정보주체 이름	N	AH (30)	정보주체 식별을 위한 이름
	phone_num	정보주체 휴대폰 번호	N	aNS (15)	정보주체 식별을 위한 휴대폰 번호 (E.164 표준 준용, 예시: '+821034959954')
	request_title	인증요청 제목	N	AH (120)	인증요청 제목 / 인증앱에서 사용자에게 노출
	device_code	디바이스 코드	Y	AN (2)	• PC : PC • TB : Tablet • MO : Mobile(기본값) • WB : 웹브라우저
	device_browser	브라우저	Y	AN (2)	• NA : Native App(기본값) • HY : Hybrid App
	return_app_schem e_url	마이데이터 서비스의 app scheme URL	N	AH (1000)	device_code가 'MO'이고, device_browser : 'NA' 또는 'HY'인 경우에만 세팅 인증앱에서 인증 완료 후 이동할 마이데이터 서비스 앱의 app scheme URL (화이트리스 트로 관리 해야함)
	consent_type	전자서명 유형	Y	aN (1)	• 전송요구내역 원문에 서명 : 0 • 전송요구내역 해시값에 서명 : 1 (기본값)
	consent_cnt	전송요구내역 개수	Y	N (4)	전자서명을 요청하는 전송요구내역의 개수

	consent_list	전송요구내역 목록	Y	<object>	'순서를 보장해야 한다.' 통합인증-103 API를 통한 전자서명 결과 조회시 본 순서와 동일한 순서로 결과 응답
	-- consent_len	consent 항목 길이	Y	N (5)	전송요구내역 원문의 길이
	-- consent_title	각 원문의 타이틀	N	AH (120)	인증앱에서 각 전송요구에 대해 표시할 요약 정보
	-- consent	전송요구내역	Y	AH (7000)	전자서명 대상 원문 consent_type이 0인 경우 : 전송요구내역 원문 (UTF-8 인코딩) consent_type이 1인 경우 : 전송요구내역 원문 (UTF-8 인코딩)의 해시값(SHA-256) ※ 전송요구내역 규격은 '인증서 본인확인 기반 통합인증 절차 및 규격'의 [첨부6] 준용
	-- tx_id	전송요구내역 트랜잭션 ID	Y	aNS(74)	마이데이터 사업자가 생성 'MD'_'마이데이터사업자 기관코드(10)_'정보 제공자 기관코드(10)_'중계기관 기관코드 (10)_'인증기관 기관코드(10)_'전자서명 요청 시간(YYYYMMDDHHMMSS)(14)_'일련번호(12)' ※ 트랜잭션 ID 규격은 '인증서 본인확인 기반 통합인증 절차 및 규격'의 [첨부5] 준용

○ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	rsp_code	세부 응답코드	Y	aN (5)	표준API 규격 - [별첨1]-③ 참조
	rsp_msg	세부 응답메시지	N	AH (450)	표준API 규격 - [별첨1]-③ 참조
	sign_ios_app_scheme_url	iOS 인증앱의 app scheme	N	AH (1000)	iOS 단말에서 마이데이터 서비스 앱이 호출할 인증앱 Custom Scheme Url
	sign_aos_app_scheme_url	AOS 인증앱의 app scheme	N	AH (1000)	AOS(안드로이드) 단말에서 마이데이터 서비스 앱이 실행할 인증앱 Scheme Url (인증기관에 따라 intent 형태의 scheme Url로 제공 가능)
	sign_web_url	인증 웹의 url	N	AH (1000)	마이데이터 서비스 앱에서 실행할 인증 웹 Url
	cert_tx_id	인증기관 트랜잭션 ID	Y	aNS (40)	전자서명 결과 조회시 사용할 트랜잭션 ID

※ (참고) 인증기관은 device_code, device_browser 값을 활용하여, App To App 방식 또는 인증앱에 Push를 보내 고객이 인증앱을 통해 전자서명을 할 수 있도록 제공. App To App 방식의 경우, 인증기관은 sign_ios_app_scheme_url(iOS), sign_aos_app_scheme_url(Android) 값을 채워 마이데이터사업자에게 응답하고, 해당 마이데이터사업자는 전송받은 scheme_url 중에 고객 단말 환경을 고려 및 선택하여 호출.

□ (통합인증-103) 전자서명 결과 조회

○ 기본 정보

API ID	통합인증-103	HTTP Method	POST
API 제공자	인증기관	API 요청자	마이데이터사업자
API 명 (URI)	/ca/sign_result		
설명	마이데이터사업자가 인증기관에게 전자서명 결과를 요청		
기준시점	현재 시점		
Content-Type (요청)	application/json; charset=UTF-8	Content-Type (응답)	application/json; charset=UTF-8

○ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	Authorization	접근토큰	Y	aNS (1500)	발급된 접근토큰 • 접근토큰 유형(Bearer)을 명시 예) Authorization: Bearer 접근토큰
	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	cert_tx_id	인증기관 트랜잭션 ID	Y	aNS (40)	전자서명 요청 응답으로 받은 cert_tx_id
	sign_tx_id	서명 요청 트랜잭션 ID	Y	aNS (49)	전자서명 요청 시 사용했던 sign_tx_id

○ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	rsp_code	세부 응답코드	Y	aN (5)	표준API 규격 - [별첨1]-[3] 참조
	rsp_msg	세부 응답메시지	N	AH (450)	표준API 규격 - [별첨1]-[3] 참조
	signed_consent_cnt	signed_consent 개수	Y	N (4)	전자서명 결과의 개수
	signed_consent_list	signed_consent 목록	Y	<object>	'순서를 보장해야 한다.'
	-- signed_consent_len	signed_consent 항목 길이	Y	N (5)	전자서명 결과의 길이
	-- signed_consent	전송요구내역 전자서명 (signedConse nt)	Y	aNS (10000)	전송요구내역 전자서명(CMS SignedData, Base64 url-safe 인코딩)
	-- tx_id	전송요구내역 트랜잭션 ID	Y	aNS(74)	마이데이터 사업자가 생성했던 tx_id 전자서명 위임 검증 시 사용

□ (통합인증-002) 통합인증 요청(API 접근토큰 발급 요청)

○ 기본 정보

API ID	통합인증-002	HTTP Method	POST
API 제공자	정보제공자, 중계기관	API 요청자	마이데이터사업자
API 명 (URI)	/oauth/2.0/token		
설명	<p>마이데이터사업자는 고객이 선택한 정보제공자를 대상으로 통합인증을 요청(전자서명 전송)</p> <ul style="list-style-type: none"> 마이데이터 서버는 1개 이상의 정보제공자에게 해당 기관을 대상으로 하는 전자서명을 각각 전송 요청메시지 내 auth_type, consent_type 항목 설정 방식 <ul style="list-style-type: none"> 공동인증서(인증서 본인확인) 기반 통합인증 : auth_type : 0, consent_type : 0 사실인증서(전자서명인증사업자) 기반 통합인증 : auth_type : 1, consent_type : 1 		
Content-Type (요청)	application/x-www-form-urlencoded	Content-Type (응답)	application/json; charset=UTF-8

○ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	tx_id	전송요구내역 트랜잭션 ID	Y	aNS (74)	마이데이터 사업자가 생성 'MD'_마이데이터사업자 기관코드(10)_'정보제공자 기관코드(10)_'중계기관 기관코드(10)_'인증기관 기관코드(10)_'통합인증 요청 시간/전자서명 요청 시간(YYYYMMDDHHMMSS)(14)_'일련번호(12)'
	org_code	기관코드	Y	aN (10)	통합인증을 수행할 정보제공자 코드 (종합포털에 기관 등록시 할당된 코드)
	grant_type	권한부여 방식	Y	aN (8)	권한부여 방식 • 'password' 고정값
	client_id	클라이언트 ID	Y	aN (50)	종합포털에 마이데이터 서비스 등록 시 발급받은 클라이언트 식별값
	client_secret	클라이언트 Secret	Y	aN (50)	종합포털에 마이데이터 서비스 등록 시 발급받은 클라이언트 Secret 값(보안을 강화하기 위해 추가 확인하기 위한 코드)
	ca_code	통합인증기관 코드	Y	aN (10)	통합인증수단을 발급한 통합인증기관 기관코드 (종합포털에 등록시 할당된 기관코드(org_code))
	username	고객 CI 정보	Y	B64 (100)	고객 CI 정보
	request_type	전송요구 타입	Y	aN (1)	<ul style="list-style-type: none"> 자산목록조회 전송요구(1차) : 0 전송요구내역의 scope에 xxx.list만 존재하는 경우 고객선택자산에 대한 세부 전송요구(2차) : 1

password_len	password 항목 길이	Y	N (5)	전송요구내역 전자서명(signedData) 길이
password	전송요구내역 전자서명 (signedConsent)	Y	aNS (10000)	전송요구내역 전자서명(CMS SignedData, Base64 url-safe 인코딩) ※ 항목명 password는 OAuth 표준 준용함
auth_type	본인확인 이용 여부	Y	aN (1)	• 인증서 본인확인기관 이용 : 0 • 전자서명인증사업자 이용 : 1
consent_type	전자서명 유형	Y	aN (1)	• 전송요구내역 원문에 서명 : 0 (인증서 본인 확인기관 기본값) • 전송요구내역 해시값에 서명 : 1 (전자서명인증 사업자 기본값)
consent_len	consent 항목 길이	N	N (5)	consent_type이 1인 경우에만 세팅 전송요구내역 원문의 길이
consent	전송요구내역	N	AH (7000)	consent_type이 1인 경우에만 세팅 전송요구내역 원문(UTF-8 인코딩)
signed_person_info_req_len	본인확인 이용동의 전자서명 항목 길이 (signedPersonInfoReq의 길이)	N	N (5)	auth_type가 0인 경우에만 세팅 signed_person_info_req의 길이 적용
signed_person_info_req	본인확인 이용동의 전자서명 (signedPersonInfoReq)	N	aNS (10000)	auth_type가 0인 경우에만 세팅 본인확인 이용동의 전자서명(CMS SignedData, Base64 url-safe 인코딩) ※ UCPID 가이드라인의 signedPersonInfoReq
consent_nonce	재전송공격 방지정보 1 (consentNonce)	N	aNS (30)	auth_type가 0인 경우에만 세팅 전송요구내역 전자서명(signedConsent)에 포함된 Nonce 값(Base64 url-safe 인코딩)
ucpid_nonce	재전송공격 방지정보 2 (ucpidNonce)	N	aNS (30)	auth_type가 0인 경우에만 세팅 본인확인 이용 동의내역 전자서명(signedPersonInfoReq)에 포함된 Nonce 값(Base64 url-safe 인코딩)
cert_tx_id	인증사업자 트랜잭션 아이디	N	aNS (40)	auth_type가 1인 경우에만 세팅 전자서명 요청 응답으로 받은 cert_tx_id
service_id	서비스번호	N	AN (22)	“금융분야 개인신용정보 전송요구 표준API규격”에 따른 기관 간 전송요구시에만 세팅 정보수신자가 종합포털에 서비스 등록 시 발급 받은 서비스번호 • 기관코드(10자리) + 등록일자(8자리) + 순번(4자리) • 예시) ORG00000001202105200001

* '공인인증서를 이용한 본인확인 서비스 가이드라인' 및 동 가이드라인의 부속서(v1.3)

○ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 문서의 별첨14 참조)
Body	tx_id	전송요구내역 트랜잭션 ID	Y	aNS (74)	API 요청시 포함되어 있던 tx_id
	token_type	접근토큰 유형	Y	aN (6)	접근토큰 유형 • 'Bearer' 고정값
	access_token	접근토큰	Y	aNS (1500)	발급된 접근토큰
	expires_in	접근토큰 유효기간	Y	N (9)	접근토큰 유효기간(단위: 초)
	refresh_token	리프레시 토큰	Y	aNS (1500)	접근토큰 갱신을 위한 토큰
	refresh_token_expires_in	리프레시 토큰 유효기간	Y	N (9)	리프레시 토큰 유효기간(단위: 초)
	scope	권한 범위	Y	aNS (128)	접근토큰 권한 범위 (다중 scope 가능) • 2.2-③ 참조

○ 에러메시지 명세 (RFC 6749 준용)

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 문서의 별첨14 참조)
Body	tx_id	전송요구내역 트랜잭션 ID	Y	aN (74)	API 요청시 포함되어 있던 tx_id
	error	에러코드	Y	aNS (30)	에러코드 • 표준API 규격 - [별첨1]-② 참조
	error_description	에러메시지	N	AH (450)	에러메시지 • 표준API 규격 - [별첨1]-② 참조 • 통합인증 관련 에러 발생 시에는 아래 "통합인증 응답코드 및 응답메시지"를 적용 • 인증과 관련 없는 기타 API 요청 항목에 문제가 있는 경우에는 각 기관이 자율적으로 에러메시지 명시

《 통합인증 응답코드 및 응답메시지 》

HTTP 응답 코드	에러코드 (error)	에러메시지 (error_description)	상세설명	비고	
400 (Bad Request)	invalid_request	UCPID_001	잘못된 요청입니다.	본인확인 전자서명 처리과정에서 발생한 에러	인증기관에서 발생한 에러
		UCPID_002	서버에 요청이 너무 많습니다. 잠시후에 다시 시도하십시오		
		UCPID_003	알수없는 에러 입니다.		
		UCPID_020	잘못된 메시지 구조입니다.		
		UCPID_021	지원하지 않는 버전의 메시지 구조입니다.		

		UCPID_022	디코딩에 실패하였습니다.	정보제공 자에서 발생한 에러
		UCPID_030	올바르지 않은 서명값입니다.	
		UCPID_031	권한이 없습니다. (등록되지 않은 기관 요청시)	
		UCPID_032	지원되지 않은 서명 알고리즘입니다.	
		UCPID_033	서명값이 올바르지 않습니다.	
		UCPID_040	UCPID 서버에 문제가 발생하였습니다. 관리자에게 문의하십시오	
		UCPID_041	유효하지 않은 인증서입니다.	
		UCPID_042	UCPID 서비스 제공기관 내 UCPID 이용 제한된 사용자(혹은 인증서)입니다. (FDS 시스템에 의한 사용이 제한 된 사용자의 요청인 경우)	
		UCPID_043	CI생성기관 측 사유로 정보 제공이 제한된 사용자(허무인 등).	
		UCPID_050	허용하지 않는 인증 모듈 정보 (등록되지 않은 인증모듈 요청)	
		UCPID_100	전자서명 검증에 실패하였습니다.	
		UCPID_101	전자서명 메시지 디코딩에 실패하였습니다.	
		UCPID_110	인증서 경로 검증에 실패하였습니다.	
		UCPID_111	인증서가 만료되었습니다.	
		UCPID_112	인증서 유효기간 시작일시 미도래	
		UCPID_113	인증서가 폐지되었습니다.	
		UCPID_114	인증서가 효력이 정지되었습니다.	
		UCPID_115	인증서 검증에 실패하였습니다. (UCPID 110~114에 해당하지 않는 경우)	
		UCPID_120	통합인증에 허용된 인증서가 아닙니다.	
		UCPID_121	서명시간이 유효시간 범위를 초과하였습니다.	
		UCPID_122	NONCE 검증에 실패하였습니다.	
		SIGN_001	존재하지 않는 고객입니다.	정보제공자의 전송요구내역 전자서명 처리(또는 인증기관의 위임 검증) 과정에서 발생한 에러
		SIGN_002	고객 CI가 일치하지 않습니다.	
		SIGN_100	전자서명 검증에 실패하였습니다.	
		SIGN_101	전자서명 메시지 디코딩에 실패하였습니다.	
		SIGN_102	전자서명 원문 비교에 실패하였습니다.	
		SIGN_110	인증서 경로 검증에 실패하였습니다.	
		SIGN_111	인증서가 만료되었습니다.	
		SIGN_112	인증서 유효기간 시작일시 미도래	
		SIGN_113	인증서가 폐지되었습니다.	
		SIGN_114	인증서가 효력이 정지되었습니다.	
		SIGN_115	인증서 검증에 실패하였습니다. (SIGN 110~114에 해당하지 않는 경우)	
		SIGN_120	통합인증에 허용된 인증서가 아닙니다.	
		SIGN_121	서명시간이 유효시간 범위를 초과하였습니다.	
		SIGN_122	NONCE 검증에 실패하였습니다.	
		SIGN_130	본인확인 전자서명과 전송요구내역 전자서명에 사용된 인증서가 상이합니다.	

※ 접근토큰 재발급 및 폐기(전송요구 철회)를 위한 API는 개별인증 API와 동일(표준 API 규격의 '개별인증-003', '개별인증-004' 참고)

□ (통합인증-104) 전자서명 위임 검증

○ 기본 정보

API ID	통합인증-104	HTTP Method	POST
API 제공자	인증기관	API 요청자	정보제공자, 중계기관
API 명 (URI)	/ca/sign_verification		
설명	정보제공자가 전자서명인증사업자에게 전자서명 검증을 요청(위임 검증)		
기준시점	현재 시점		
Content-Type (요청)	application/json; charset=UTF-8	Content-Type (응답)	application/json; charset=UTF-8

○ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	Authorization	접근토큰	Y	aNS (1500)	발급된 접근토큰 • 접근토큰 유형(Bearer)을 명시 예) Authorization: Bearer 접근토큰
	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	cert_tx_id	인증기관 트랜잭션 ID	Y	aNS(40)	전자서명 요청 응답으로 받은 cert_tx_id
	tx_id	전송요구내역 트랜잭션 ID	Y	aNS(74)	마이데이터 사업자가 통합인증-002 API를 통해 제공한 tx_id
	signed_consent_len	signed_consent 항목 길이	Y	N (5)	전자서명 결과의 길이
	signed_consent	전송요구내역 전자서명 (signedConsent)	Y	aNS (10000)	전송요구내역 전자서명(CMS SignedData, Base64 url-safe 인코딩)
	consent_type	전자서명 유형	Y	aN (1)	• 전송요구내역 원문에 서명 : 0 • 전송요구내역 해시값에 서명 : 1 (기본값)
	consent_len	consent 항목 길이	N	N (5)	서명 검증할 전송요구내역 원문의 길이
	consent	전송요구내역	Y	AH (7000)	전송요구내역 원문(UTF-8 인코딩) consent_type이 0인 경우 : 전송요구내역 원문 consent_type이 1인 경우 : 전송요구내역 해시값 (UTF-8 인코딩된 상태에서 SHA-256 해시값 생성)

○ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (표준 API 규격 [첨부14] 참조)
Body	tx_id	전송요구내역 트랜잭션 ID	Y	aNS (74)	API 요청시 포함되어 있던 tx_id
	rsp_code	세부 응답코드	Y	aN (5)	표준API 규격 - [별첨1]-③ 참조
	rsp_msg	세부 응답메시지	Y	AH (450)	표준API 규격 - [별첨1]-③ 참조 • 전자서명 및 인증서 검증 과정에서 발생한 에러는 아래 "위임검증 응답코드 및 응답 메시지"를 적용 • 인증과 관련 없는 API 처리 관련 에러 발생시, 각 기관이 자율적으로 에러메시지 명시
	result	전자서명 검증결과 (인증서 확인 및 원문 비교 포함)	Y	Boolean	true = 전자서명 검증 성공 false = 전자서명 검증 실패 ※ 정보제공자의 명확한 결과 인지를 위해 실패시에도 본 항목을 포함하여 응답 ※ 인증 실패 및 기타 API 처리 관련 에러 발생시 모두 false 응답
	user_ci	정보주체 식별값	Y	B64 (100)	result가 true인 경우에만 제공 정보주체 식별을 위한 연계정보 (CI, Connection Information)

《 위임검증 응답코드 및 응답메시지 》

HTTP 응답 코드	세부응답 코드 (rsp_code)	세부응답 메시지 (rsp_msg)	상세설명	비고
400 (Bad Request)	40001	SIGN_100	전자서명 검증에 실패하였습니다.	인증기관(전자서명인 증사업자)의 전자서명 위임 검증 과정에서 발생한 에러
		SIGN_101	전자서명 메시지 디코딩에 실패하였습니다.	
		SIGN_102	전자서명 원문 비교에 실패하였습니다.	
		SIGN_110	인증서 경로 검증에 실패하였습니다.	
		SIGN_111	인증서가 만료되었습니다.	
		SIGN_112	인증서 유효기간 시작일시 미도래	
		SIGN_113	인증서가 폐지되었습니다.	
		SIGN_114	인증서가 효력이 정지되었습니다.	
		SIGN_115	인증서 검증에 실패하였습니다. (SIGN 110~114에 해당하지 않는 경우)	
		SIGN_120	통합인증에 허용된 인증서가 아닙니다.	
		SIGN_121	서명시간이 유효시간 범위를 초과하였습니다.	
		SIGN_122	NONCE 검증에 실패하였습니다.	
		SIGN_123	전자서명을 완료하지 않았습니다.	