제5장. 인증 API 명세

5.1 개별인증 API

5.1.1 인가코드 발급 요청

ㅇ 기본 정보

API ID	개별인증-001	HTTP Method	GET
API 제공자	정보제공자	API 요청자	마이데이터사업자
API 명 (URI)	/oauth/2.0/authorize		
설명	정보주체(고객)가 마이데이터사업자 앱을 통해 개별인증수단(정보제공자가 제공)을 이용하여 인증 및 전송요구를 수행한 후 인가코드를 발급 • 정보제공자는 개별인증을 위한 인증화면 및 전송요구를 위한 자산선택 화면을 웹뷰 등으로 제공, 해당 화면을 통해 개별인증 및 전송요구 수행 • 인가코드 발급 후 정보제공자는 redirect_uri (Callback URL)로 인가코드 등을 리다이렉트		
기준시점	현재 시점		
Content-Type (요청)	-	Content-Type (응답)	- 또는 application/json; charset=UTF-8

ㅇ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-user-ci	정보주체 식별값	Y	B64 (100)	정보주체 식별을 위한 연계정보 (Connection Information) • 개별인증을 요청하는 정보주체의 CI값(마이데이터사업자 회원가입 시 수집)으로, 정보제공자는 개별인증 수행 시 정보제공자가 보유한 CI값과 마이데이터사업자가 전달한 CI값(x-user-ci)를 비교·검증해야 함
	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Parameter	org_code	기관코드	Y	aN (10)	정보제공자 기관코드 • 지원 API로부터 배포
	response_type	타입	Y	a (4)	정보주체가 인증 및 전송요구 시 인가코드가 반환됨을 의미 • 'code' 고정값
	client_id	클라이언트 ID	Y	aN (50)	종합포털에 마이데이터 서비스 등록 시 발급받은 클라이언트 식별값

	redirect_uri	Callback URL	Y	aNS (100)	정보주체가 전송요구 후 응답이 전달(redirect)될 마이데이터 서비스 URI(종합포털에 마이데이터 서비스 등록 시 입력한 주소와 동일해야 함) • URL 인코딩 필요 (정보제공자는 디코딩 후 검증)
	app_scheme	마이데이터서비스 앱 URL 스킴	Y	aNS (100)	정보주체가 현재 실행중인 마이데이터서비스 앱의 앱스킴 (일부기관의 경우, 동일 마이데이터서비스를 복수 개의 앱으로 제공하기 때문에 특정 필요) • 정보제공자가 앱방식 개별인증 제공 시, 인증완료 후 다시 마이데이터서비스 앱으로 전환하기 위해 필요 • 마이데이터사업자는 사전에 본인의 앱스킴(복수 개 가능)을 종합포털에 등록 필요 (지원-003 API 통해 배포) • URL 인코딩 필요 (정보제공자는 디코딩 후 검증)
	state	상태값	Y	aN (40)	CSRF 보안위협에 대응하기 위해 임의 설정하는 값(일반적으로 마이데이터 서비스 서버 및 앱 간 세션값으로 설정)

○ 응답메시지 명세 (HTTP 응답코드 : 302)

- 마이데이터사업자의 Callback URL(redirect_uri)로 리다이렉트

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Parameter	code	인가코드	Y	aNS (128)	발급한 인가코드(Authorization code) • 인가코드 유효시간은 최대 10분 권고(RFC 6749)
	state	상태값	Y	aN (40)	요청 Parameter로 전달받은 'state'와 동일한 값 설정
	api_tran_id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조) • 요청시 전달받은 거래고유번호 헤더값(x-api-tran-id)과 동일한 값 • 본 API는 결과를 Callback URL로 리다이렉트하지만 헤더값은 redirect되지 않기 때문에 다른 API들과는 달리 parameter로 거래고유번호를 회신

회신 예시

```
HTTP/1.1 302 Found
Location: https://마이데이터사업자_Callback_URL?code=인가코드&state=상태값&api_tran_id=거래고유번호
```

ㅇ 에러메시지 명세 (RFC 6749 준용)

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Parameter	error	에러코드	Y	aNS (30)	에러코드 • [첨부1]-① 참조
	error_description	에러메시지	N	AH (450)	에러메시지 • [첨부1]-① 참조
	state	상태값	Y	aN (40)	요청 Parameter로 전달받은 'state'와 동일한 값 설정
	api_tran_id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조) • 요청시 전달받은 거래고유번호 헤더값 (x-api-tran-id)과 동일한 값 • 본 API는 결과를 Callback URL로 리다이렉트하지만 헤더값은 redirect되지 않기 때문에 다른 API들과는 달리 parameter로 거래고유번호를 회신

① 요청메시지 내 client_id 또는 redirect_uri 가 유효하지 않은 경우 등

- JSON으로 회신 (응답메시지 Content-Type : application/json; charset=UTF-8)
- HTTP 응답코드 : 400, 405 (상세 응답코드 및 응답메시지는 첨부1 참조)

회신 예시

```
{
  "error": 에러코드,
  "error_description: 에러메시지,
  "state": 상태값,
  "api_tran_id": 거래고유번호
}
```

② 그 외

- 마이데이터사업자의 Callback URL(redirect_uri)로 리다이렉트
- HTTP 응답코드 : 302 (상세 응답코드 및 응답메시지는 첨부1 참조)

회신 예시

```
HTTP/1.1 302 Found
Location: https://마이데이터사업자_Callback_URL?error=에러코드&error_description=에러메시지&state=상태값
    &api_tran_id=거래고유번호
```

5.1.2 접근토큰 발급 요청

ㅇ 기본 정보

API ID	개별인증-002	HTTP Method	POST
API 제공자	정보제공자	API 요청자	마이데이터사업자
API 명 (URI)	/oauth/2.0/token		
설명	인가코드 발급 API(개별인증-001)를 통해 획득한 인가코드(Authorization code)를 이용하여 접근토큰을 발급		
기준시점	현재 시점		
Content-Type (요청)	application/x-www-form-urlencoded	Content-Type (응답)	application/json; charset=UTF-8

ㅇ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	org_code	기관코드	Y	aN (10)	정보제공자 기관코드 • 지원 API로부터 배포
	grant_type	권한부여 방식	Y	aNS (18)	권한부여 방식 • 'authorization_code' 고정값
	code	인가코드	Y	aNS (128)	인가코드 발급 API(개별인증-001)를 통해 획득한 인가코드(Authorization code)
	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)
	redirect_uri	Callback URL	Y	aNS (100)	마이데이터 서비스 URI • 인가코드 발급 요청 시 요청했던 Callback URL과 동일해야 함

ㅇ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	token_type	접근토큰 유형	Y	a (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	Y	aNS (1500)	접근토큰 갱신을 위한 토큰

		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

ㅇ 에러메시지 명세 (RFC 6749 준용)

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

5.1.3 접근토큰 갱신

ㅇ 기본 정보

API ID	개별인증-003	HTTP Method	POST
API 제공자	정보제공자	API 요청자	마이데이터사업자
API 명 (URI)	/oauth/2.0/token		
설명	접근토큰 발급 시 수신한 리프레시 토큰(refresh_token)을 이용하여 새로운 접근토큰을 발급		
기준시점	현재 시점		
Content-Type (요청)	application/x-www-form-urlencoded	Content-Type (응답)	application/json; charset=UTF-8

ㅇ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	org_code	기관코드	Y	aN (10)	정보제공자 기관코드 • 지원 API로부터 배포
	grant_type	권한부여 방식	Y	aNS (13)	권한부여 방식 • 'refresh_token' 고정값
	refresh_token	리프레시 토큰	Y	aNS (1500)	접근토큰 갱신을 위한 토큰
	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)

ㅇ 응답메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	token_type	접근토큰 유형	Y	a (6)	접근토큰 유형 • 'Bearer' 고정값
	access_token	접근토큰	Y	aNS (1500)	발급된 접근토큰
	expires_in	접근토큰 유효기간	Y	N (9)	접근토큰 유효기간(단위: 초)

ㅇ 에러메시지 명세 (RFC 6749 준용)

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

5.1.4 접근토큰 폐기

ㅇ 기본 정보

API ID	개별인증-004	HTTP Method	POST
API 제공자	정보제공자	API 요청자	마이데이터사업자
API 명 (URI)	/oauth/2.0/revoke		
설명	접근토큰 및 리프레시토큰 폐기 • 개별인증 또는 통합인증을 통해 발급된 접근토큰 및 리프레시토큰을 유효기간 만료 전 폐기(고객이 전송요구 철회 시)하기 위한 API • 접근토큰(요청메시지 내 token)뿐만 아니라, 리프레시토큰도 함께 폐기		
기준시점	현재 시점		
Content-Type (요청)	application/x-www-form-urlencoded	Content-Type (응답)	application/json; charset=UTF-8

ㅇ 요청메시지 명세

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	org_code	기관코드	Y	aN (10)	정보제공자 기관코드 • 지원 API로부터 배포
	token	폐기하고자 하는 토큰	Y	aNS (1500)	폐기하고자 하는 접근토큰
	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)

ㅇ 응답메시지 명세

- ①접근토큰 및 리프레시토큰을 정상적으로 폐기한 경우, ②요청메시지의 접근토큰(token)이 유효하지 않은 경우 모두 HTTP 응답코드 200 회신 (RFC 7009를 준용하여 ②의 경우도 에러로 회신하지 않음)

HTTP	항목명	항목설명	필수	타입(길이)	설명 (비고)
Header	x-api-tran-id	거래고유번호	Y	AN (25)	거래고유번호 (첨부14 참조)
Body	rsp_code	세부 응답코드	Y	aN (5)	'00000' : 접근토큰 및 리프레시토큰 폐기 성공 '99999' : 폐기하고자하는 토큰이 유효하지 않은 경우
	rsp_msg	세부 응답메시지	Y	AH (450)	

ㅇ 에러메시지 명세 (RFC 7009 준용)

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

5.2 통합인증 API

※ 통합인증 API 상세 규격은 “ “[별첨1] 인증서 본인확인 기반 통합인증 절차 및 규격”, “[별첨2] 사설인증서 기반 통합인증 절차 및 규격” 참조