

인증서 본인확인 기반 통합인증 절차 및 규격

2021. 9.

금융보안원

| | |
|--|----|
| I. 개 요 | 1 |
| 1. 목적 및 범위 | |
| 2. 참여기관 역할 | |
| II. 공통 기준 | 3 |
| 1. 인증 수단 · 기관 | |
| 2. 인증 기준 · 규격 | |
| 3. 보안 대책 | |
| III. 통합인증 절차 및 규격 | 6 |
| 【첨부 1】 통합인증 준비 절차 | 9 |
| 【첨부 2】 통합 인증기관 및 모듈업체 현황 | 16 |
| 【첨부 3】 통합인증 상세 규격 및 API 명세 | 17 |
| 【첨부 4】 통합인증기관 및 인증서 식별정보 | 30 |
| 【첨부 5】 트랜잭션 ID 생성 규칙 | 31 |
| 【첨부 6】 전송요구내역 생성 및 전송 규격 | 32 |
| 【첨부 7】 전자서명 요청 및 응답 규격(샘플 데이터 포함) | 36 |
| 【첨부 8】 통합인증(인증서 본인확인) 이용약관 및 동의서 | 39 |
| 【첨부 9】 본인확인용(cpCode) 기관코드 발급 신청서(양식) | 41 |

I. 개 요

 본 문서는 정보통신망법상 인증서 본인확인서비스에 기반한 통합인증 절차 및 규격에 해당

※ 사설인증서 기반 통합인증 절차 및 규격은 <별첨 2> 참조

1 목적 및 범위

- (목 적) 마이데이터 서비스 이용시 정보주체의 안전하고 편리한 개인신용정보 전송요구를 위한 통합인증 절차 및 규격을 제시
※ '(참고1) 통합인증 필요성' 참고
- (범 위) 통합인증에 참여하는 정보제공자(중계기관 포함), 마이데이터 사업자, 인증기관을 대상으로 하며,
 - 각 기관은 역할에 따라 통합인증 기능 및 API를 구현

2 참여기관 역할

- (정보제공자) 정보주체의 통합인증 요청에 따라 고객을 인증
- (인증기관) 정보주체에게 통합 인증수단을 발급·관리하고, 인증수단 검증 등을 통해 고객 식별정보(CI 정보) 제공*
* 인증수단의 특성 등에 따라 인증기관이 관련 S/W를 제공·관리 가능
- (마이데이터 사업자) 고객에게 인증정보(전자서명) 생성을 요청하고 생성된 인증정보를 정보제공자에게 전달(통합인증 요청)
- (인증 지원기관) ①인증기준·규격 관리, ②인증기관 자격요건 확인·관리, ③인증절차 적합성 확인, ④업무규약 등 통합인증 관리체계 수립 및 운영(금융보안원)

《 (참고1) 통합인증 필요성 및 이용 예시 》

- **(현황 및 문제점)** 정보주체가 개인신용정보를 마이데이터 사업자에게 전송하도록 요구하기 위해서는 정보제공자별로 각기 다른 인증수단*을 이용하여 인증받아야 함

* (예) ID/PW 입력, 생체정보 입력, 휴대폰 인증, 공인인증서 활용 등

- 정보주체가 정보 전송을 요구하는 정보제공자의 수만큼 반복적으로, 인증을 수행함에 따라 이용 편의성이 크게 저하

- **(통합인증 필요성)** 정보주체가 안전하고 편리하게 1회 인증(지문, 비밀번호 등)만으로 다수 정보제공자에 인증하는 통합인증 방식을 도입 필요

《 통합인증 이용 예시(정보주체 관점) 》



※ 위 절차 이외에도 각 인증시 마다(②,③ 단계) 고객으로부터 동의(첨부8)를 받아야 함

Ⅱ. 공통 기준

1 인증 수단 · 기관

□ **(인증수단)** 인증 결과의 안전성 및 신뢰성 보장을 위해, 전자서명 인증서(PKI)를 통합 인증수단(‘통합인증서’)으로 선정

○ 인증서 본인확인수단을 통합인증서로 사용하며, 정보제공자 및 마이데이터사업자는 허용된 통합인증수단을 제공 필요

○ 정보주체(고객)는 참여 인증기관이 발급하는 통합인증서 중에서 기존 보유하고 있는 인증서를 이용하거나, 또는 신규로 발급*

* 통합인증서 신규 발급은 각 인증기관별 발급 절차를 따름

□ **(인증기관)** 정보통신망법상 지정받은 인증서 본인확인기관 총 5개 기관 중 4개 기관(참고2)이 인증서 본인확인 기반 통합인증기관으로 참여*

* 인증기관 참여 절차 등은 별도 안내

《 (참고2) 참여 인증기관 및 인증수단 》

| 참여 인증기관 | 인증수단 |
|---------|--------------|
| 금융결제원 | 범용/은행용 공동인증서 |
| 코스콤 | 범용/증권용 공동인증서 |
| 한국정보인증 | 범용/은행용 공동인증서 |
| 한국전자인증 | 범용 공동인증서 |

※ 상기 인증서 이외에 인증기관이 발급 중인 인증서는 본인확인제도 소관 부처의 확인 등을 거쳐 통합인증수단에 추가 가능

2 인증 기준 · 규격

□ **(신원확인)** 인증기관은 **통합인증서 발급**시에 직접 또는 등록 기관(RA)을 통한 **실명확인**을 통해 정보주체의 신원을 확인

□ **(인증 규격)** 통합인증 규격은 다음을 준수하고 그 외 범위는 인증기관별로 자율적으로 규격을 마련 · 적용

○ **(데이터 형식)** 인증 요청 · 응답 데이터의 형식 등은 KISA의 '공인인증서를 이용한 본인확인 서비스 가이드라인*'을 준용

* 공인인증서를 이용한 본인확인 서비스(UCPID) 가이드라인 부속서(v1.3) 포함

○ **(전송 방식)** 인증 데이터의 전송은 전송구간*에 따라 표준 API, 또는 본인확인 서비스 가이드라인의 전송 규격을 적용

* (마이데이터사업자↔정보제공자) 표준 API, (정보제공자↔인증기관) UCPID 규격

○ **(기 타)** 기타 인증 규격은 다음을 참고(참고3)

《 (참고3) 기타 인증 규격 》

○ **(규 격)** X.509 v3, CMS(RFC 2630) 등 표준규격 준용

* 인증서 정보, DN 체계 등 세부 규격은 인증기관별 규격·체계를 준용. 다만, 상세 기술검토 등을 통해 인증서 필수 포함 정보를 추가 가능

○ **(암호 수준)** 암호 알고리즘 및 키 길이 등은 KISA 등의 암호 지침 준용

○ **(인증서 저장)** 통합인증서는 타 이용자 접근 및 악성코드 등으로부터 안전한 방식*으로 저장 및 접근통제

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

○ **(고객 접근통제)** 생체인증, PIN, 패스워드 입력 등 안전성이 확보된 방식을 통해 고객이 확인된 경우에만 전자서명을 생성

□ **(S/W 제공 및 연동)** 통합인증서 관련 인증 S/W 모듈(전자서명 생성·검증 등)은 각 정보제공자 및 마이데이터사업자가 구비*

* 인증모듈업체, 또는 인증기관이 제공(인증 모듈을 직접 개발하고자 하는 정보제공자 및 마이데이터사업자는 인증기관 및 지원기관과 개별 협의)

3 보안 대책

- **(고객 단말 보호)** 고객 단말을 통한 인증정보 유출 등을 방지하기 위해 보안 키패드, 앱 위변조 탐지, 백신* 등의 보호 대책 적용

* 고객 단말의 운영환경 등을 고려하여 적용

- **(기관 간 인증)** 표준 API 구간에는 TLS 기반 상호인증 적용*, 그 외 구간에는 본인확인 서비스 가이드라인**을 준용

* TLS 상호인증 세부 방식은 ‘금융분야 마이데이터 표준 API 규격’ 참고

** 서버용 공동인증서 기반의 기관 인증

- **(통신구간 보호)** 표준 API 구간은 TLS 인증서 기반 암호화 통신, 그 외 구간은 본인확인 서비스 가이드라인*을 준용

* 서버용 공동인증서 기반의 암호화 통신 적용(인터넷망 이외에 전용선 및 VPN 등을 이용하고자 하는 정보제공자는 인증기관과 개별 협의)

- **(CI 보호)** CI는 인증기관(본인확인기관)이 본인확인을 요청한 정보제공자에게만 안전하게 제공 및 활용

4 기 타

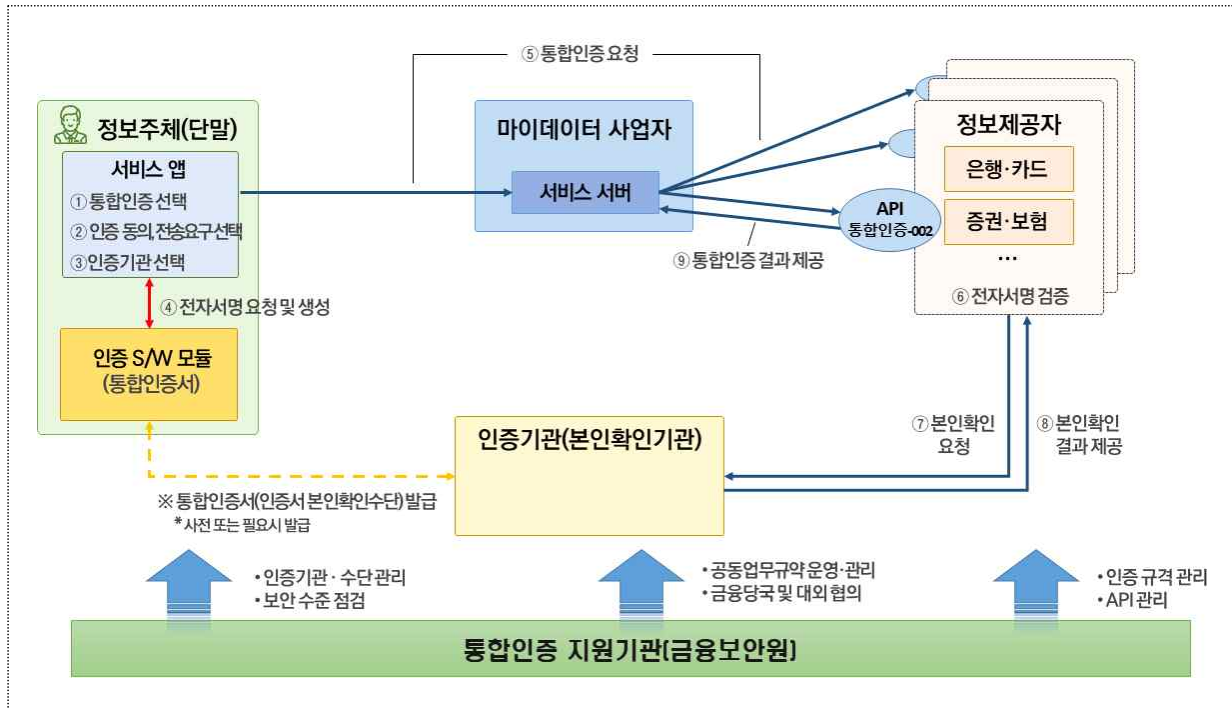
- ‘통합인증 공동업무규약’을 통해 참여기관별 역할 및 관계, 책임소재 등을 규정

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

Ⅲ. 통합인증 절차 · 규격

- ※ 통합인증 절차에 앞서 “(첨부 1) 통합인증 준비 절차” 를 사전 수행 필요
- ※ 상세 규격 및 API는 “(첨부 2) 통합인증 상세 규격 및 API 명세” 참고

《 (그림 1) 통합인증 절차 개요 》



- ① (통합인증 선택) 고객(정보주체)은 인증방식으로 통합인증을 선택
- ② (인증 동의 및 전송요구 선택) 고객은 서비스 앱을 통해 통합인증(본인확인서비스)을 위한 이용약관 및 동의서*를 확인(동의)하고, 개인신용정보 전송요구 내역**을 선택

* 이용약관 및 동의서 - 각 마이데이터 사업자는 서비스 앱을 통해 고객이 통합인증에 필요한 이용약관 및 동의서를 확인 및 동의할 수 있도록 화면 구성·제공

※ [첨부8] 통합인증(인증서 본인확인) 이용약관 및 동의서

** 개인신용정보 전송요구 내역 선택 - 마이데이터 사업자는 고객이 전송요구 내역을 선택할 수 있도록 화면을 구성·제공

③ (인증기관 선택) 고객은 서비스 앱을 통해 선호하는 인증기관(수단)을 선택

※ ①,②,③ 단계 순서는 마이데이터 사업자가 자율적으로 변경 가능

④ (전자서명 요청 및 생성) 서비스 앱은 고객이 선택한 인증기관(전자서명 생성 모듈 등)에 전자서명을 요청하고, 인증기관은 전자서명 결과 값을 생성하여 서비스 앱에 응답

《 전자서명 요청·응답 개요 》

| | |
|---------|---|
| 개 요 | 통합인증을 위해 인증기관에게 정보제공자(N개)별 전자서명 생성을 요청 |
| 전자서명 요청 | [정보제공자 A 기관 코드 : 동의 내역 : 전송요구내역], ... [정보제공자 N 기관 코드 : 동의 내역 : 전송요구내역] |
| 전자서명 응답 | [정보제공자 A 기관 코드 : 전자서명(동의 내역) : 전자서명(전송요구내역)], ... [정보제공자 N 기관 코드 : 전자서명(동의 내역) : 전자서명(전송요구내역)] |

⑤ (통합인증 요청) 마이데이터 서버는 통합인증 요청을 위해, 정보제공자별로 전자서명 결과 값을 전송(API: 통합인증-002)

《 통합인증-002 : 통합인증 요청 API 》

| | |
|------------------|--|
| API 명 (HTTP URD) | /oauth/2.0/token |
| API 설명 | 정보제공자에게 통합인증(접근토큰) 요청 |
| API 제공자 / 이용자 | 정보제공자(중계기관) / 마이데이터 서버 |
| 요청정보 | 서비스 자격증명, 전자서명(동의내역), 전자서명(전송요구내역), CI 등 |
| 응답정보 | 접근토큰, scope 등 |

- ⑥ (전자서명 검증) 각 정보제공자는 전자서명 검증 모듈을 이용하여 전송요구내역 및 동의 내역에 대한 전자서명을 검증
- ⑦ (본인확인 요청) 정보제공자는 고객 본인확인을 위해 본인 확인 요청 모듈을 이용하여 본인확인 요청 메시지를 생성 및 고객 인증서를 발급한 인증기관(본인확인기관)에 요청*
- * 본인확인 서비스 가이드라인 상의 UCPIIDRequest 전송
- ⑧ (본인확인 결과 제공) 인증기관은 본인확인 요청을 처리하고 결과(CI, 인증서 유효성 등)를 정보제공자에게 제공(⑦ 단계의 응답)
- ⑨ (통합인증 결과 제공) 정보제공자는 ⑥,⑧ 결과를 통해 고객을 인증하고, 그 결과로 정보제공 API 요청시 필요한 접근토큰을 마이데이터 서버에게 전송(통합인증-002의 응답)

《 (참고4) 중계기관 이용시 고려사항 》

- 정보제공자가 중계기관을 이용하는 경우에는 상기 절차상에서 정보 제공자 역할은 중계기관이 수행하나, CI 기반의 고객식별 등 중계기관이 직접 수행 불가능한 과정은 정보제공자가 직접 수행할 필요
- 통합인증 절차 및 규격에서는 중계기관 및 이를 이용하는 정보제공자 간의 세부 절차 및 규격은 다루지 않으며, 해당 중계기관 및 정보제공자 간의 방침에 따름

- **(공통 준비사항)** 마이데이터 생태계 참여를 위한 공통 준비사항
 - 마이데이터사업자, 정보제공자, 통합인증기관은 각자의 역할에 따라, 마이데이터 생태계 참여를 위한 ‘기관정보 등록’, ‘서비스 정보 등록’, ‘종합포털과 접속 채널 등 설정’ 수행*

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

- **(통합인증 준비사항)** 통합인증 참여 및 이용을 위한 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

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 기관정보 등록(API 직접구축 정보제공자, 중계기관)

— 인증기관과의 **본인확인** 요청·응답시 필요한 **기관코드(cpCode)***와 **서버용 공동인증서****를 인증기관으로부터 **발급*****

* 본인확인용 기관코드(cpCode) - 본인확인 요청 메시지 내에 포함하여야 하는 정보이며, 서비스별 이용자 중복가입 확인정보(DI) 생성에 활용

** 서버용 공동인증서 - 본인확인 응답 메시지 암호화 등에 사용

*** 서버용 공동인증서는 참여 인증기관으로부터 발급(인증서를 발급받은 인증기관 외 타 인증기관에도 사용 가능)

— **기존** 발급받은 서버용 공동인증서가 존재하는 경우 **그대로 사용 가능하며**(신규 발급 X), 본인확인용 **기관코드(cpCode)**는 **신규 발급***을 권장

* 정보제공자는 기존 서비스와 구분을 위해 본인확인용 기관코드(cpCode)는 신규 발급받는 것을 권장(타 본인확인서비스 및 기관을 통해 기 발급받은 본인확인용 기관코드도 원칙상 사용 가능)

** 중계기관은 중계기관의 본인확인용 기관코드(cpCode)를 발급받아야 하며, 중계 이용기관(정보제공자)의 본인확인용 기관코드(cpCode)도 발급·관리 필요

※ “[첨부9] 본인확인용 기관코드(cpCode) 발급 신청서” 참고(중계 이용기관은 중계기관을 통해 일괄적으로 신청 접수)

☞ (지원 담당) 인증기관

《 (참고) 본인확인용 기관코드(cpCode) 규격 》

○ (cpCode) 12자리 문자열(숫자 및 알파벳 구성, 첫 번째 자리는 발급기관코드)

< cpCode 예시 >

| | | | | | | | | | | | |
|----|---|---|---|---|---|---|---|---|---|---|---|
| A* | a | 0 | 1 | 2 | 0 | 1 | 2 | 1 | 2 | C | V |
|----|---|---|---|---|---|---|---|---|---|---|---|

* 발급기관코드 : 발급기관별로 기 부여된 코드(알파벳 대문자)

** 예시) 금융결제원 - ‘Y’, 코스콤 - ‘C’, 한국정보인증 - ‘A’ 등

- **종합포털(신용정보원)에 기관정보 등록시, 본인확인용 기관 코드(cpCode)와 서버용 공동인증서 정보***를 등록

* 서버용 공동인증서의 issuer DN, subject DN 값 등록

** 중계기관은 중계기관의 본인확인용 기관코드(cpCode) 및 서버용 공동인증서 정보를 등록하여야 하며, 중계 이용기관(정보제공자)은 이용기관의 본인확인용 기관코드(cpCode)를 등록 필요(서버용 공동인증서 정보 등록 X)

☞ (지원 담당) 인증기관, 마이데이터 지원기관

③ 인증기관과 연동 준비(API 직접구축 정보제공자, 중계기관)

- 기관정보 조회 API(지원-002)를 통해 인증기관의 정보*를 수집하고 허용되는 인증기관 및 수단을 확인

* 기관코드(org_code), IP 주소(또는 도메인) 및 서비스 포트 정보, 각 인증기관 식별값(고객 인증서 issuer DN의 o 값), 허용 인증서 종류의 식별값(고객 인증서 OID 값)

※ "[첨부4] 통합인증기관 및 인증서 식별정보" 참고

- 인증기관 정보를 시스템 및 방화벽 등에 적용하고 연동 테스트 수행

☞ (지원 담당) 인증기관, 인증모듈업체(첨부2)

④ 통합인증 개발(API 직접구축 정보제공자, 중계기관)

- 마이데이터사업자로부터 전송받은 전송요구내역 전자서명과 본인확인 전자서명을 검증하기 위한 전자서명 검증 모듈* 설치 및 관련 기능 개발

* 전자서명 검증모듈을 보유한 경우, 이를 활용 가능(다만, 각 인증모듈업체를 통해 호환성 등 확인 필요)

《 (참고) 전자서명 검증 관련 주요 기능 》

- (재전송 공격 탐지) 2개 전자서명 값에 각각 포함된 Nonce값과 마이데이터 사업자가 전송(통합인증-002 API)한 2개 Nonce값이 동일한지 여부를 비교·검증하는 기능(동일한 경우 정상)
- (인증서 비교) 전송요구내역 및 본인확인 전자서명 값에 각각 사용된 정보주체(고객)의 인증서가 동일한지 비교·검증하는 기능
- ※ 세부 내용은 “[첨부3] 통합인증 상세 절차·규격 및 API 명세” 참고

☞ (지원 담당) 인증모듈업체

— 마이데이터 사업자로부터 전송받은 본인확인 전자서명 값을 이용하여 인증기관에 본인확인을 요청하기 위한 **본인확인 요청·응답 메시지*** 처리 모듈**을 설치 및 관련 기능 개발

* 본인확인 요청 메시지(UCPIDRequest) 생성 및 본인확인 응답 메시지(UCPIDResponse) 처리

** 통합인증 기능 및 상호호환성이 확인된 인증모듈업체를 통해 확보

☞ (지원 담당) 인증모듈업체, 인증기관

다. 마이데이터 사업자

① 고객 CI 정보 수집

- 서비스 회원 가입시 고객에게 본인확인서비스를 요구하여 고객 CI 정보를 수집

② 인증기관 정보 수집

- 기관정보 조회 API(지원-002)를 통해 인증기관의 정보*를 수집하고 허용되는 인증기관 및 수단을 확인

* 기관코드(org_code), 각 인증기관 식별값(고객 인증서 issuer DN의 o 값), 허용 인증서 종류의 식별값(고객 인증서 OID 값)

※ "[첨부4] 통합인증기관 및 인증서 식별정보" 참고

☞ (지원 담당) 마이데이터 지원기관(신용정보원, 금융보안원)

③ 통합인증 개발

- 전송요구내역 및 본인확인 메시지에 대한 전자서명 생성 모듈*을 서비스 내에 설치 및 관련 기능** 개발

* 전자서명 생성 기능 이외에도 본인확인 메시지(signedPersonInfoReq) 생성(전자서명) 기능 포함

** 멀티서명 기능, 허용 인증기관 및 인증서 식별, 재전송공격 방지정보(Nonce) 제공, 고객 단말 보호(보안 키패드, 앱 위변조 탐지, 백신) 등

☞ (지원 담당) 인증모듈업체

- 통합인증 시, 관련 분쟁해결 및 과금 등 **본인확인** 요청의 추적성을 위해 필요한 **트랜잭션 ID(tx_id)*** 생성 기능 개발

* 통합인증 요청(통합인증-002 API)시 정보제공자에게 제공하며, 정보 제공자는 본인확인 요청 메시지(UCPIDRequest) 생성시 활용 (cpRequestNumber에 적용)

※ “[첨부5] 트랜잭션 ID 생성 규칙” 참고

④ 인증모듈정보 제출

- 마이데이터서비스 보안취약점 점검*을 수행하고 점검결과를 금융보안원 앞으로 통지 시, “③ 통합인증 개발”에서의 전자서명 생성 모듈의 정보**를 포함하여 통지

* 마이데이터 서비스에 전자서명 생성 모듈을 포함하여 개발완료된 상태에서 취약점 점검을 수행

** 밴더사명, 모듈명, 버전정보(Major.Minor.Build.Revision)

※ 인증모듈을 직접 개발하고자 하는 기관은 지원기관 및 인증기관과 개별 협의가 필요하며, 인증모듈 관리 방안은 향후 변경 가능

☞ (지원 담당) 인증모듈업체, 마이데이터 지원기관

《 (참고) 인증모듈 정보 생성 규칙 》

○ 인증모듈정보는 다음 규격에 따라 생성

| 구 분 | 허용 문자 | 길이(최대) |
|--|-------------|--------|
| 밴더사명 (인증모듈 개발사) | 알파벳 | 20 |
| 모듈명* | 숫자 및 알파벳 | 40 |
| 버전정보** (Major.Minor.Build.Revision) | 숫자(구분자 ".") | 30 |

* 인증모듈업체(기존 본인확인모듈 공급 업체)는 기존 본인확인모듈의 모듈명과 상이한 모듈명을 지정 필요

** 버전정보 중 build, revision은 옵션 항목이므로 선택적으로 적용 가능

라. 인증기관

- 종합포털(신용정보원)에 통합인증에 필요한 기관정보* 등록

* IP 주소(또는 도메인) 및 서비스 포트, 인증기관 식별값(고객 인증서 issuer DN의 o 값), 허용 인증서 종류의 식별값(고객 인증서 OID 값)

- 기관정보 조회 API(지원-006)를 통해 정보제공자* 및 마이데이터 사업자**의 정보를 수집

* 정보제공자 기관코드(org_code), IP 주소(또는 도메인), 본인확인용 기관 코드(cpCode) 및 서버용 공동인증서 정보(issuer DN, subject DN 등)

** 마이데이터사업자의 기관코드(org_code)

- 금융보안원을 통해 마이데이터 사업자의 전자서명 생성 모듈 정보*를 수집

* 밴더사명, 모듈명, 버전정보(Major.Minor.Build.Revision)

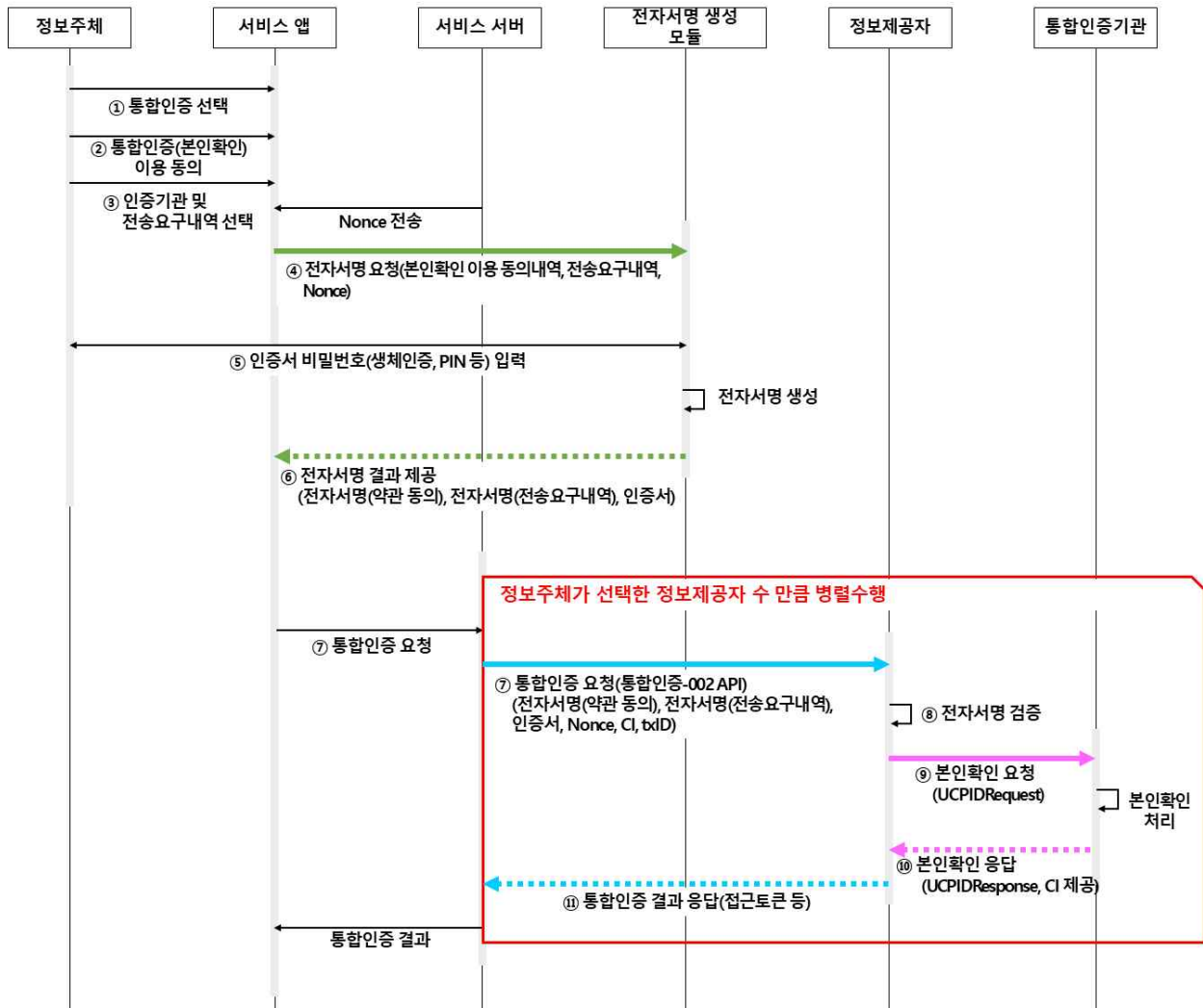
☞ (지원 담당) 마이데이터 지원기관

첨부 2

통합 인증기관 및 모듈업체 현황

| 구분 | 기관명 | 이메일 | 연락처 | 모듈제공 현황 | |
|------------|---------------|---|---|---------------|---------------|
| | | | | 전자서명 생성·검증 | 본인확인 요청·응답 |
| 통합인증 기관 | 금융결제원 | (사업) yeskeycert@kftc.or.kr (개발) yeskey.dev@kftc.or.kr | (사업) 02-531-3172 02-531-3162 (개발) 02-531-3183 | X | X |
| | 코스콤 | (영업) hschoi@koscom.co.kr bkkim@koscom.co.kr (개발) csh1man@koscom.co.kr | (영업) 02-767-7228 02-767-7213 (개발) 02-767-7396 | ○ | ○ |
| | 한국정보인증 | jhkim@signgate.com sym1031@signgate.com | (정) 02-360-3084 (부) 02-360-3060 | ○ | ○ |
| | 한국전자인증 | (영업) hjlee@crosscert.com (기술) dylee1@crosscert.com | (영업) 010-4240-4436 (기술) 02-3470-3821 | ○ | ○ |
| 인증모듈 업체 | 드림시큐리티 | sskim@dreamsecurity.com yjkim@dreamsecurity.com | (정) 010-7353-5025 (부) 010-6816-6840 | ○ | ○ |
| | 라온시큐어 | sjpark@raonsecure.com | (정) 010-2042-8472 (부) 010-8637-6639 | ○ | ○ |
| | 예티소프트 | (영업) c.park@yettiesoft.com (기술) river88@yettiesoft.com | (영업) 010-6210-0782 (기술) 010-8940-6682 | ○ | ○ |
| | 위즈베라 | sschoi@wizvera.com jeonghun.kim@wizvera.com | (정) 010-6282-3847 (부) 010-7282-7585 | ○ | ○ |
| | 이니텍 | sec_sale1@initech.com | (정) 02-6445-7139 (부) 02-6445-7148 | ○ | ○ |
| | 펜타시큐리티 시스템 | (영업) heehoshin@pentasecurity.com (기술) mclim@pentasecurity.com | (영업) 010-3263-2225 (기술) 010-3782-9034 | ○ | ○ |
| | 한컴위드 | (영업) wonjae@hancomwith.com donghwan@hancomwith.com (기술) dongjo@hancomwith.com | (영업) 010-3438-3213 010-3750-9385 (기술) 010-2223-9213 | ○ | ○ |

1. 통합인증 상세 절차



① (정보주체) 마이데이터 서비스 회원가입 후 해당 서비스 앱에 로그인하여 인증방식으로 통합인증을 선택

② (정보주체) 마이데이터 서비스앱을 통해 통합인증을 위해 필요한 본인확인 이용약관 및 동의서*를 확인 및 동의

* 정보통신망법 상 인증서 본인확인 이용을 위해 필요하며, **세부 사항은 “[첨부8] 통합인증(인증서 본인확인) 이용약관 및 동의서” 참고**

- 마이데이터사업자는 서비스앱을 통해 본인확인 이용 동의서를 제공

③ **(정보주체)** 마이데이터 서비스앱을 통해 전송요구할 대상 정보 제공자를 선택하고, 전송요구 내역을 특정

- 마이데이터사업자는 서비스앱을 통해 신용정보법 제33조의2제5항에 의거, 정보주체가 아래의 내용을 특정할 수 있도록 화면을 구성 및 제공 필요

| 특정 사항 | 정보주체 선택 항목 |
|------------------------------|--|
| 정기적 전송을 요구하는지 여부 및 요구 시 그 주기 | <ul style="list-style-type: none"> • 정기적 전송 요구 여/부 선택 • 주기 |
| 전송요구의 종료시점 | <ul style="list-style-type: none"> • 전송요구의 종료시점 |
| 전송을 요구하는 목적 | <ul style="list-style-type: none"> • 전송을 요구하는 목적 |
| 전송을 요구하는 개인신용정보의 보유기간 | <ul style="list-style-type: none"> • 마이데이터사업자가 수집한 정보를 보유할 수 있는 기간 |
| 전송을 요구하는 개인신용정보 | <ul style="list-style-type: none"> • 업권별 상이(상세내용은 표준 API 규격 문서의 2.2-③의 “전송요구 scope” 참조) |

- 정보주체가 특정한 사항을 규격*에 따라 전송요구내역으로 생성

* “[첨부6] 전송요구내역 생성 및 전송 규격” 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 전송가능한 크기를 초과하여 전송이 불가능
 - * 현재, 통합인증 API 규격상 전송요구내역의 전송 크기는 7,000 Byte이므로, 보유 계좌 수가 약 234개를 초과하는 경우에는 전송요구내역 전송이 불가(계좌번호 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 하게 되는 경우, 추가 계좌도 전송요구에 포함됨을 고객에게 안내

④ **(마이데이터사업자)** 본인확인 이용 동의내역, 전송요구내역에 대하여 정보주체가 통합인증서를 이용하여 전자서명을 생성할 수 있도록 전자서명 생성 모듈을 호출(전자서명 요청)

- 정보주체가 인증서 선택화면을 통해 허용된 인증기관 및 인증서를 선택할 수 있도록 허용 인증기관 및 인증서*만을 식별 및 제시

* “[첨부4] 통합인증기관 및 인증서 식별정보”를 활용하여 허용 인증기관 및 인증서 확인

- 서비스 서버를 통해 재전송공격 방지정보(consentNonce, ucpidNonce)를 생성하여 서비스 앱 등에 제공하고, 서비스 앱은 재전송공격 방지정보를 포함하여 전자서명 요청(참고)

※ “[첨부7] 전자서명 요청 및 응답 규격(샘플 데이터 포함)” 참고

《 (참고) 재전송공격 방지정보(Nonce) 생성 및 전송 》

① **(Nonce 값 생성)** 고객이 통합인증 시도시 마이데이터 서버에서 다음의 각 Nonce 값(128 bits 숫자 생성 및 Base64 url-safe 인코딩)을 생성하여 전자서명이 생성되는 마이데이터 서비스 앱 등에 제공

- consentNonce : 전송요구내역 전자서명 값에 포함되는 Nonce 값
- ucpidNonce : 본인확인 전자서명 값에 포함되는 Nonce 값

② **(Nonce 값 전송)** 마이데이터 서버는 마이데이터 앱 등에서 생성한 전자서명 값(Nonce 포함)과 Nonce를 포함하여 정보제공자에게 통합인증 요청(통합인증-002 API)

※ 동시에 통합인증을 요청하는 정보제공자별로 Nonce 값을 서로 다르게 생성할 것을 권고(다만, 서비스 지연 및 부하 등을 고려하여 선택 가능)

⑤ **(정보주체)** 본인확인 이용 동의내역, 전송요구내역에 대한 전자서명 생성을 위해 인증서 비밀번호 등을 입력

⑥ **(마이데이터사업자)** 전자서명 생성 모듈로부터 본인확인 이용 동의내역 및 전송요구내역에 대한 전자서명 결과*(응답)을 수신

* 전자서명은 CMS SignedData(RFC 2630) 형식을 따르며, SignedAttributes에 PKCS#9 contentType, PKCS#9 signing Time, PKCS#9 messageDigest가 포함되어야 함

⑦ **(마이데이터사업자)** 전자서명과 종합포털로부터 발급받은 "서비스 자격증명"(client_id, client_secret) 등을 이용하여 각 정보제공자에게 병렬적으로 접근토큰을 요청(통합인증-002 API)

- API를 통해, 고객 CI, 본인확인 이용 동의내역에 대한 전자서명*, 전송요구내역에 대한 전자서명, 재전송공격 방지정보(Nonce), 트랜잭션 ID(tx_id), 인증기관 기관코드(org_code)**를 전송

* 본인확인 서비스 가이드라인 상의 signedPersonInfoReq 메시지

** 전자서명 결과에 포함된 인증기관 식별자(caOrg)로 해당 인증기관 기관코드(org_code)를 확인

| API ID | 통합인증-002 | API명(URI) | /oauth/2.0/token |
|---------|---|-----------|------------------|
| API 설명 | 자산목록 조회 API, 정보제공 API 호출을 위한 접근토큰 발급 | | |
| API 제공자 | 정보제공자 | | |
| 요청 정보 | 서비스 자격증명, CI, 전자서명(본인확인 이용 동의내역), 전자서명(전송요구내역), 재전송공격 방지정보(consentNonce, ucpidNonce), 트랜잭션 ID(tx_id), 인증기관 기관코드(org_code) 등 | | |
| 응답 정보 | 접근토큰, scope 등 | | |

⑧ **(정보제공자)** 전자서명 검증 모듈을 이용하여 본인확인 이용 동의내역 및 전송요구내역에 대한 전자서명을 다음 절차에 따라 검증

* 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)

※ 정보제공자 및 중계기관은 1) 번 단계를 최우선 수행하여 고객이 아닌 경우 (CI 일치 고객 미존재), 이후 단계(본인확인 요청 등)를 수행하지 않고 즉시 에러를 반환

※ 2)~5) 검증 순서는 정보제공자 사정 등에 따라 변경 가능

2) (허용 인증서 여부 검증) 전자서명에 사용된 인증서가 통합인증에 허용된* 인증서인지 여부를 확인(非허용 인증서인 경우 거부)

* “[첨부4] 통합인증기관 및 인증서 식별정보”를 활용하여 허용 인증 기관 및 인증서 확인

3) (재전송 공격 탐지)

- 전자서명의 서명시간(signing time)*이 유효시간 범위** 내에 포함 되는지 여부를 확인(유효시간 범위를 벗어날 경우 거부)

* CMS에 포함된 PKCS#9 signing Time(UTC 기준)

** 현재시간 기준, 최대 1시간 이내에서 서버 및 네트워크 환경을 고려하여 설정(10분 내외 권장)

- 각 전자서명에 포함된 Nonce(consentNonce, ucpidNonce)와 API를 통해 전송받은 Nonce가 동일한지 여부를 확인(동일하지 않은 경우 거부)

* 전자서명의 consentNonce와 API의 consentNonce(consent_nonce) 비교, 전자서명의 ucpidNonce와 API의 ucpidNonce(ucpid_nonce) 비교

4) (전자서명 검증) 본인확인 이용 동의내역 및 전송요구내역에 대한 전자서명을 검증(전자서명 검증에 실패할 경우 거부)

5) (인증서 비교 및 검증)

- 본인확인 이용 동의내역 및 전송요구내역에 대한 전자서명에 사용된 정보주체의 인증서가 **동일한 인증서인지 여부를 비교 및 확인**(동일하지 않은 경우 거부)

《 인증서 비교 방법 》

- (1안) 각 서명 데이터(CMS)에서 추출한 인증서의 바이너리가 동일한지 비교
- (2안) 각 서명 데이터(CMS)에서 추출한 인증서에 대하여 체인(경로)검증*을 수행 후 인증서 간의 발급자 및 일련번호 비교
 - * 체인검증에 실패한 경우 해당 인증서는 정당한 KISA rootCA 기반 하에서 발급된 인증서가 아니거나, 테스트 인증서 또는 위변조된 인증서 등에 해당
- ※ (2안)에서의 체인(경로)검증은 본인확인 요청시 인증기관에서도 수행하여 결과를 제공(인증서 유효성 결과)하므로 이를 고려하여 인증서 비교 방법을 선정

- 전자서명에 사용된 인증서의 유효성*(OCSP 등)을 확인(유효하지 않은 경우 거부)

* 인증서 유효성은 본인확인 요청·응답(⑨~⑪ 단계)을 통해 확인 가능하므로 인증서 유효성 확인은 정보제공자 자율에 따라 적용

⑨ (정보제공자) 본인확인 요청 모듈을 이용하여 본인확인 요청 메시지를 생성하여 인증기관에 고객 본인확인을 요청

《 본인확인 요청 메시지 생성 》

- (ISPreqInfo 생성) 마이데이터사업자로부터 전송받은 signedPersonInfoReq 메시지에 재전송공격 방지정보(ucpidNonce)*를 생성 및 추가하고, 마이데이터사업자로부터 전송받은 트랜잭션 ID(tx_id)를 cpRequestNumber 필드에 추가하여 생성
 - * ④~⑧단계의 Nonce와는 무관한 정보로서 별도 생성 및 추가
- (UCPIDRequest 생성) ISPreqInfo 메시지를 서버용 공동인증서로 전자서명한 후 본인확인용 기관코드(cpCode) 등을 추가하여 생성

※ 중계기관의 경우에는 인증기관에 따라 다음과 같이 cpRequestNumber 및 cpCode를 설정하여 메시지를 생성 및 요청

| 인증기관 구분 | cpRequestNumber | cpCode |
|-------------------------|---|---------------------------|
| 금융결제원 | "트랜잭션 ID(tx_id)" + "-" + "정보제공 cpCode" | 중계기관 cpCode |
| 코스콤 한국정보인증 한국전자인증 | 트랜잭션 ID(tx_id) | 중계 이용기관 (정보제공자) cpCode |

- ⑩ **(통합인증기관)** 인증 이용 동의에 대한 전자서명을 검증하고, 그 결과로서 본인확인 결과*(CI 등)를 정보제공자에게 제공(⑨에 대한 응답)

* 본인확인 서비스 가이드라인 상의 UCPIIDResponse 메시지 전송

- ⑪ **(정보제공자)** 본인확인 응답 처리 모듈을 이용하여 본인확인 결과를 확인*하고 이를 토대로 정보주체를 인증(CI 활용)한 후, 접근토큰을 발급하여 마이데이터 사업자에게 제공(⑦에 대한 응답)

* 본인확인 서비스 가이드라인 상의 UCPIIDResponse 메시지 내에 포함된 PersonInfo 메시지를 추출 및 분석(CI 추출 등)

- 1) **(재전송 공격 탐지)** 본인확인 결과 메시지에 포함된 Nonce(ucpidNonce)가 ⑨ 단계에서 본인확인 요청 메시지에 추가했던 Nonce가 동일한지 여부를 확인(동일하지 않은 경우 거부)
- 2) **(동일 고객 여부 확인)** API를 통해 전송받은 고객 CI와 통합인증기관으로부터 제공받은 CI가 동일한지 여부를 확인(동일하지 않은 경우 거부)

《 본인확인 응답 메시지 처리 》

- **(UCPIIDResponse 확인)** 통합인증기관으로부터 제공받은 UCPIIDResponse 메시지에서 본인확인 결과 및 응답코드(status)를 확인하고 PersonInfo 메시지(전자서명 및 암호화된 값) 추출
- **(PersonInfo 분석 및 CI 추출)** 서버용 인증서(개인키)를 이용하여 PersonInfo 메시지를 복호화하고, 통합인증기관의 인증서(공개키)를 이용하여 전자서명을 검증한 후, CI 등을 추출

⑫ **(마이데이터사업자)** 통합인증 결과를 고객에게 안내 및 접근토
큰을 이용하여 개인신용정보를 요청·수집

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

2. 통합인증 API 명세

| API ID | API 명 | URI | | | HTTP Method |
|----------|--------------------------|---------|----------|------------------|-------------|
| | | version | industry | resource | |
| 통합인증-002 | 접근토큰 발급 요청 (정보제공자 제공) | 해당 없음 | 해당 없음 | /oauth/2.0/token | POST |

□ (통합인증-002) API 접근토큰 발급 요청(정보제공자 제공)

○ 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 | 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) | <ul style="list-style-type: none"> 인증서 본인확인기관 이용 : 0 전자서명인증사업자 이용 : 1 |
| consent_type | 전자서명 유형 | Y | aN (1) | <ul style="list-style-type: none"> 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) ※ 전송요구내역 규격은 [첨부6] 준용 |
| 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 <ul style="list-style-type: none"> 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 | 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 | 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 API 처리 관련 에러 발생시, 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. | | |

| | | | | | |
|--|--|-----------|---|--|---|
| | | 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. | | 정보제공 자에서 발생한 에러 |
| | | 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 과정에서 발생한 에러 |
| | | SIGN_002 | 고객 CI가 일치하지 않습니다. | | |
| | | SIGN_100 | 전자서명 검증에 실패하였습니다. | | |
| | | SIGN_101 | 전자서명 메시지 디코딩에 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)

첨부 4

통합인증기관 및 인증서 식별정보

| 인증기관(식별값*) * 인증서 내 'issuer DN'의 'o' 값 | 인증서 종류 | 인증서 식별값(OID) |
|--|--------------|--|
| 금융결제원("yessign") | 범용 공동인증서 | · 1.2.410.200005.1.1.1 |
| | 은행용 공동인증서 | · 1.2.410.200005.1.1.4 · 1.2.410.200005.1.1.4.1 · 1.2.410.200005.1.1.4.2 · 1.2.410.200005.1.1.4.3 · 1.2.410.200005.1.1.4.4 · 1.2.410.200005.1.1.4.5 · 1.2.410.200005.1.1.4.6 · 1.2.410.200005.1.1.4.7 |
| | 금융인증서* | · 1.2.410.200005.1.1.1.10 |
| 코스콤("SignKorea") | 범용 공동인증서 | · 1.2.410.200004.5.1.1.5 |
| | 증권용 공동인증서 | · 1.2.410.200004.5.1.1.9 |
| 한국정보인증("KICA") | 범용 공동인증서 | · 1.2.410.200004.5.2.1.2 |
| | 은행용 공동인증서 | · 1.2.410.200004.5.2.1.7.1 |
| 한국전자인증("CrossCert") | 범용 공동인증서 | · 1.2.410.200004.5.4.1.1 |

* 금융인증서의 OID는 정보제공자(API 직접구축) 및 중계기관은 모두 적용(허용)하여야 하며, 마이데이터 사업자는 금융인증서를 선택한 기관만 필요시 적용

※ 인증기관 추가시 기관정보 조회 API(지원-002)를 통해 지속 배포

- (규 격) 74자리 문자열(숫자 및 알파벳 구성, 구분자 '_' 포함)

< 트랜잭션 ID 생성 포맷 >

| 필드* | 포맷(길이) |
|------------------|------------------------------|
| 식별자 | 'MD' 고정값 (2) |
| 마이데이터사업자 기관코드 | 종합포털이 부여한 마이데이터사업자 기관코드 (10) |
| 정보제공자 기관코드 | 종합포털이 부여한 정보제공자 기관코드 (10) |
| 중계기관 기관코드 | 종합포털이 부여한 중계기관 기관코드 (10) |
| | 구 분 |
| | 지정 값 |
| | API 직접구축 정보제공자 '0000000000' |
| | 중계기관 이용 정보제공자 중계기관 기관코드 |
| 인증기관 기관코드 | 종합포털이 부여한 인증기관 기관코드 (10) |
| 통합인증 요청 시간 | 'YYYYMMDDHHMMSS' (14) |
| 일련번호** | 숫자(1씩 증가) (12) |

* 각 필드는 '_'로 구분

** 일련번호는 고객에 상관없이 마이데이터 사업자가 통합인증을 요청하는 건별로 1씩 증가(권고) 및 매일 자정 기준으로 초기화(권고). 다만, 통합인증 요청 건별로 일련번호의 유일성은 반드시 보장(중복 X)되어야 함.

- (생성 규칙) 고객이 통합인증을 요청시 정보제공자 수만큼 '정보제공자 및 중계기관 기관코드 등'이 상이한 tx_id를 생성(일련번호 등은 동일)

- 트랜잭션 ID 생성 예시

- 2021년8월4일 자정 이후, 마이데이터 사업자(O100000001)의 첫 번째 고객이 API 직접구축 은행(A100000001) 및 카드사(C100000001)에 통합인증 요청

은행 : MD_O100000001_A100000001_0000000000_Q100000001_20210805011015_000000000001
카드 : MD_O100000001_C100000001_0000000000_Q100000001_20210805011015_000000000001

- 2021년8월4일 자정 이후, 마이데이터 사업자(O100000001)의 두 번째 고객이 API 직접구축 은행(A100000003), 중계기관(P100000001) 이용 보험사(B100000002)에 통합인증 요청

은행 : MD_O100000001_A100000003_0000000000_Q100000001_20210805011015_000000000002
보험 : MD_O100000001_B100000002_P100000001_Q100000001_20210805011015_000000000002

첨부 6

전송요구내역 생성 및 전송 규격

※ 고객이 보유한 asset이 매우 많아 전송요구내역의 길이(인코딩 후)가 전송 가능한 길이(7000)를 초과하는 경우에는 모든 asset을 열거하는 대신, scope 지정 후, asset_list에는 "asset" = "all_asset" 으로 표기(예시 5). 전송 가능한 최대 길이(7000)를 초과하는 경우에만 적용

《 전송요구내역 규격 (JSON) 》

| 항목 | 타입 (길이, byte) | 설명 | | | | | | | | | | | | | | | | | | |
|--------------|------------------|--|----|--------|----|-------|------------|---|------------|------------|---|----|--------|----|-------|------------|---|-------|------------|--|
| snd_org_code | String(10) | 정보제공자 기관코드(org_code) | | | | | | | | | | | | | | | | | | |
| rcv_org_code | String(10) | 마이데이터사업자(정보수신자) 기관코드(org_code) | | | | | | | | | | | | | | | | | | |
| is_scheduled | String(5) | 정기적 전송 여부("true" 또는 "false") | | | | | | | | | | | | | | | | | | |
| fnd_cycle | String(5) | 기본 정보의 정기적 전송 주기(is_scheduled가 true인 경우 적용) - 규격(횟수/기준) : "1/주"(주1회), "2/주"(주2회), "1/m"(월1회) - 기준 : 월 기준 = "m", 주 기준 = "w", 일 기준 = "d" ※ 현재, 정기적 전송 주기는 모두 주1회로 정하고 있으므로, "1/w"을 고정값으로 사용 | | | | | | | | | | | | | | | | | | |
| add_cycle | String(5) | 추가 정보의 정기적 전송 주기(is_scheduled가 true인 경우 적용) - fnd_cycle 항목 생성 규격 준용 ※ 현재, 정기적 전송 주기는 모두 주1회로 정하고 있으므로, "1/w"을 고정값으로 사용 | | | | | | | | | | | | | | | | | | |
| end_date | String(8) | 전송요구의 종료시점("YYYYMMDD") - 자산목록조회 전송요구(1차) : 전송요구시점부터 7일째 되는 일자 - 고객선택자산에 대한 세부 전송요구(2차) : 전송요구시점부터 1년째 되는 일자 또는 고객이 선택한 기간이 종료되는 일자 | | | | | | | | | | | | | | | | | | |
| purpose | String(150) | 전송을 요구하는 목적(한글 최대 50글자) | | | | | | | | | | | | | | | | | | |
| period | String(8) | 전송을 요구하는 개인신용정보의 보유기간("YYYYMMDD") - 자산목록조회 전송요구(1차) : 전송요구시점부터 7일째 되는 일자 - 고객선택자산에 대한 세부 전송요구(2차) : "99991231"(고정값) | | | | | | | | | | | | | | | | | | |
| target_info | JSON[] | <table> <tr> <th>항목</th><th>타입(길이)</th><th>설명</th></tr> <tr> <td>scope</td><td>String(20)</td><td>전송요구 정보에 해당하는 Scope</td></tr> <tr> <td>asset_list</td><td>JSON[]</td><td> <table> <tr> <th>항목</th><th>타입(길이)</th><th>설명</th></tr> <tr> <td>asset</td><td>String(70)</td><td>전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략)</td></tr> <tr> <td>seqno</td><td>String(10)</td><td>계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅)</td></tr> </table> </td></tr> </table> | 항목 | 타입(길이) | 설명 | scope | String(20) | 전송요구 정보에 해당하는 Scope | asset_list | JSON[] | <table> <tr> <th>항목</th><th>타입(길이)</th><th>설명</th></tr> <tr> <td>asset</td><td>String(70)</td><td>전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략)</td></tr> <tr> <td>seqno</td><td>String(10)</td><td>계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅)</td></tr> </table> | 항목 | 타입(길이) | 설명 | asset | String(70) | 전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략) | seqno | String(10) | 계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅) |
| 항목 | 타입(길이) | 설명 | | | | | | | | | | | | | | | | | | |
| scope | String(20) | 전송요구 정보에 해당하는 Scope | | | | | | | | | | | | | | | | | | |
| asset_list | JSON[] | <table> <tr> <th>항목</th><th>타입(길이)</th><th>설명</th></tr> <tr> <td>asset</td><td>String(70)</td><td>전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략)</td></tr> <tr> <td>seqno</td><td>String(10)</td><td>계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅)</td></tr> </table> | 항목 | 타입(길이) | 설명 | asset | String(70) | 전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략) | seqno | String(10) | 계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅) | | | | | | | | | |
| 항목 | 타입(길이) | 설명 | | | | | | | | | | | | | | | | | | |
| asset | String(70) | 전송요구 대상 계좌(상품) 식별자 목록 (고객 단위로 설정되는 xxx.list, card.card, cardbill 등 Scope의 경우에는 본 항목을 생략) | | | | | | | | | | | | | | | | | | |
| seqno | String(10) | 계좌(상품)식별자 (구분자 생략) 회차번호 (구분자 생략) (은행 및 할부금융 계좌목록 조회 결과 seqno가 존재하는 경우에만 세팅) | | | | | | | | | | | | | | | | | | |

| | | |
|--------------------------------|-----------|---|
| is_consent_trans_memo | String(5) | 적요 또는 거래메모 전송요구 여부 ("true" 또는 "false") * 은행업권, 전금업권 전송요구(2차)시에만 설정 |
| is_consent_merchant_name_regno | String(5) | 가맹점명/사업자등록번호 전송요구 여부 ("true" 또는 "false") * 카드업권, 전금업권, 통신업권 전송요구(2차)시에만 설정 |
| is_consent_trans_category | String(5) | 상품(구매)분류 전송요구 여부 ("true" 또는 "false") * 전금업권 전송요구(2차)시에만 설정 |

《 전송요구내역 예시 1(예: 은행 계좌목록 정보 전송요구) 》

```
{
  "snd_org_code":"O100000001",
  "rcv_org_code":"A100000001",
  "is_scheduled":"true",
  "fnd_cycle":"1/w",
  "add_cycle":"1/w",
  "end_date":"20220804",
  "purpose":"상세정보 전송요구를 위한 가입상품목록 조회",
  "period":"20220804",
  "target_info":[
    {
      "scope":"bank.list"
    }
  ]
}
```

《 전송요구내역 예시 2(예: 은행 대상 수신계좌 정보 전송요구) 》

```
{
  "snd_org_code":"O100000001",
  "rcv_org_code":"A100000001",
  "is_scheduled":"true",
  "fnd_cycle":"1/w",
  "add_cycle":"1/w",
  "end_date":"20220804",
  "purpose":"본인신용정보 통합조회 서비스의 이용",
  "period":"99991231",
  "target_info":[
    {
      "scope":"bank.list"
    },
    {
      "scope":"bank.deposit",
      "asset_list":[
        {
          "asset":"1111111111",
          "seqno":"1231234"
        },
        {
          "asset":"2222222222"
        }
      ]
    }
  ]
},
  "is_consent_trans_memo":"true"
}
```

《 전송요구내역 예시 3(예: 은행 대상 수신·마이너스 계좌 정보 전송요구) 》

```
{
  "snd_org_code":"O100000001",
  "rcv_org_code":"A100000001",
  "is_scheduled":"true",
  "fnd_cycle":"1/w",
  "add_cycle":"1/w",
  "end_date":"20220804",
  "purpose":"본인신용정보 통합조회 서비스의 이용",
  "period":"99991231",
  "target_info":[
    {
      "scope":"bank.list"
    },
    {
      "scope":"bank.deposit",
      "asset_list":[
        {
          "asset":"1111111111",
          "seqno":"1231234"
        }
      ]
    },
    {
      "scope":"bank.loan",
      "asset_list":[
        {
          "asset":"1111111111",
          "seqno":"1231234"
        }
      ]
    }
  ],
  "is_consent_trans_memo":"true"
}
```

《 전송요구내역 예시 4(예: 카드사 대상 카드, 포인트, 청구 정보 전송요구) 》

```
{
  "snd_org_code":"O100000001",
  "rcv_org_code":"C100000001",
  "is_scheduled":"true",
  "fnd_cycle":"1/w",
  "add_cycle":"1/w",
  "end_date":"20220804",
  "purpose":"본인신용정보 통합조회 서비스의 이용",
  "period":"99991231",
  "target_info":[
    {
      "scope":"card.card",
      "asset_list":[
        {
          "asset":"1111111111111111"
        },
        {
          "asset":"2222222222222222"
        }
      ]
    },
    {
      "scope":"card.list"
    },
    {
      "scope":"card.point"
    },
    {
      "scope":"card.bill"
    }
  ],
  "is_consent_merchant_name_regno":"true"
}
```

《 전송요구내역 예시 5(예: 전송요구내역 길이가 최대 전송 가능 길이를 초과시 규격) 》

```
{
  "snd_org_code":"O100000001",
  "rcv_org_code":"A100000001",
  "is_scheduled":"true",
  "fnd_cycle":"1/w",
  "add_cycle":"1/w",
  "end_date":"20220804",
  "purpose":"본인신용정보 통합조회 서비스의 이용",
  "holding_period":"99991231",
  "target_info":[
    {
      "scope":"bank.list"
    },
    {
      "scope":"bank.deposit",
      "asset_list":[
        {
          "asset":"all_asset"
        }
      ]
    },
    {
      "scope":"bank.irp",
      "asset_list":[
        {
          "asset":"all_asset"
        }
      ]
    }
  ],
  "is_consent_trans_memo":"true"
}
```

첨부 7

전자서명 요청 및 응답 규격(샘플 데이터 포함)

※ 본 전자서명 요청 및 응답 JSON 규격은 마이데이터서비스에 적용된 인증모듈(업체)에 따라 일부 상이할 수 있음. 다만, 응답 값의 각 항목(orgCode, signedPersonInfoReq, signedConsent, caOrg)은 반드시 규격에 따라 생성되어야 함.

《 전자서명 요청 규격 (JSON) 》

| 타입 | 설명 | | | | | | |
|-------------|-----------------------|--|----------------------|--|--|---------|----|
| JSON[] | 항목 | 타입 | 설명 | | | | |
| | orgCode | String | 정보제공자 기관코드(org_code) | | | | |
| | ucpidRequestInfo | JSON | 항목 | 타입 | 설명 | | |
| | | | userAgreement | String | - (고정값) "금융분야 마이데이터 통합인증을 위한 인증서 본인 확인서비스 이용약관, 개인정보 처리, 고유식별정보 수집·이용 및 위탁에 동의합니다." - ucpid메시지 생성시 위 문자열이 UTF-8 인코딩된 상태로 적용 | | |
| | | | userAgreeInfo | JSON | 요청하고자 하는 본인확인정보 | | |
| | | | | | 항목 | 타입 | 설명 |
| | | | | | realName | Boolean | 실명 |
| | | | | | gender | Boolean | 성별 |
| | nationalInfo | Boolean | | | 국적 | | |
| | birthDate | Boolean | 생년월일 | | | | |
| | ci | Boolean | CI 정보 | | | | |
| | - 각 항목은 true로 설정(기본값) | | | | | | |
| ispUrlInfo | String | 마이데이터 서비스 도메인 정보 (마이데이터사업자가 제공하는 지원 API 서버 도메인) | | | | | |
| ucpidNonce | String | - 마이데이터 서버가 생성한 Nonce (Base64 url-safe 인코딩) - 128 bits 숫자(인코딩 이전 원문 기준) - ucpid메시지 생성시에는 128 bits 숫자(인코딩 이전 원문) 상태로 적용 | | | | | |
| consentInfo | JSON | 항목 | 타입 | 설명 | | | |
| | | consent | JSON | - 전송요구내역 - "[첨부6] 전송요구내역 생성 및 전송 규격" 참고 | | | |
| | | consentNonce | String | - 마이데이터 서버가 생성한 Nonce (Base64 url-safe 인코딩) - 128 bits 숫자(인코딩 이전 원문 기준) | | | |

《 전자서명 응답 규격 (JSON) 》

| 항목 | 타입 | 설명 | | |
|----------------|---------|--|--------|---|
| signedDataList | JSON[] | | | |
| | | 항목 | 타입 | 설명 |
| | | orgCode | String | 정보제공자 기관코드(org_code) |
| | | signedPersonInfoReq | String | UCPID 가이드라인의 UCPIDRequestInfo(PersonInfoReq에 인증모듈 정보 등을 추가)를 서명한 CMS SignedData (Base64 url-safe 인코딩) |
| | | signedConsent | String | 전송요구내역(consentinfo)를 서명(반드시 중괄호 '{}'를 포함하여 서명 생성)한 CMS SignedData (Base64 url-safe 인코딩) |
| caOrg | String | <ul style="list-style-type: none"> - 전자서명에 사용된 고객 인증서 발급기관명(인증서 dn의 o값: yesign, SignKorea, KICA, CrossCert 등) - 마이데이터 사업자는 caOrg를 통합인증기관의 해당하는 ca_code(org_code)로 변경하여 통합인증-002 API를 호출하여야 함 | | |

《 전자서명 요청 샘플 데이터 》

```
[
  {
    "orgCode": "O100000001",
    "ucpidRequestInfo": {
      "userAgreement": "금융분야 마이데이터 통합인증을 위한...",
      "userAgreeInfo": {
        "realName": true,
        "gender": true,
        "nationalInfo": true,
        "birthDate": true,
        "ci": true
      },
      "ispUrlInfo": "www.mydata.or.kr",
      "ucpidNonce": "djVJqSSmujAS..."
    },
    "consentInfo": {
      "consent": "...",
      "consentNonce": "sdkljflksdjopg..."
    }
  },
  {
    "orgCode": "O100000002",
    "ucpidRequestInfo": {
      "userAgreement": "금융분야 마이데이터 통합인증을 위한...",
      "userAgreeInfo": {
        "realName": true,
        "gender": true,
        "nationalInfo": true,
        "birthDate": true,
        "ci": true
      },
      "ispUrlInfo": "www.mydata.or.kr",
      "ucpidNonce": "padlkjdfklQW..."
    },
    "consentInfo": {
      "consent": "...",
      "consentNonce": "xcTRioERkjsadf..."
    }
  }
]
```

※ (참고) consentInfo에 대한 전자서명 값은 종괄호'}'를 반드시 포함하여 생성

《 전자서명 응답 샘플 데이터 》

```
{
  "signedDataList": [
    {
      "orgCode": "O100000001",
      "signedPersonInfoReq": "djVJqSSmujAS...",
      "signedConsent": "fjVJqBSmuyAX..."
    },
    {
      "orgCode": "O100000002",
      "signedPersonInfoReq": "fjVJqSSmujAS...",
      "signedConsent": "djVJqBSmuyAX..."
    }
  ],
  "caOrg": "yessign"
}
```


◆ 인증서 본인확인서비스(공동인증서 등) 기반 통합인증시 본인확인 관련 법령상의 고객동의 요건 준수를 위한 이용약관 및 동의서

□ (구 성) 인증기관의 통합인증(인증서 본인확인서비스) 제공을 위한 이용약관 1종, 동의서 2종으로 구성

| 구 분 | 세부 내용 |
|------|--|
| 이용약관 | 1. 금융분야 마이데이터 통합인증을 위한 인증서 본인확인서비스 이용약관 |
| 동의서 | 2. 금융분야 마이데이터 통합인증(인증서 본인확인)을 위한 개인정보 처리 동의 3. 금융분야 마이데이터 통합인증(인증서 본인확인)을 위한 고유식별정보 수집·이용 및 위탁 동의 |

□ (배포 방식) 각 약관 및 동의서를 웹 문서 형태(링크)로 배포

○ 마이데이터 사업자는 필요에 따라 웹 문서(링크)를 자체 UI, PDF 형태로 변환하여 활용*

* (고려사항) 자체 UI로 적용할 경우, 약관 및 동의서 개정시 서비스 앱 재배포 등이 필요할 수 있음(링크 적용시 재배포 불필요)

| 구 분 | 링 크 |
|-------------------------|---|
| 1. 인증서 본인확인서비스 이용약관* | https://crosscert.com/mydata/terms.html |
| 2. 개인정보 처리 동의 | https://crosscert.com/mydata/privacy_agreement.html |
| 3. 고유식별정보 수집·이용 및 위탁 동의 | https://crosscert.com/mydata/consignment_agreement.html |

※ 한국전자인증이 대표로 링크를 제공하는 것이며, 인증기관에 상관 없이 공통 사용(고객이 타 인증기관 인증서를 선택하더라도 동일하게 사용)

※ 각 인증기관은 각사 홈페이지 등에 인증서 본인확인서비스 이용약관을 게시

□ **(적용 기준)** 마이데이터 사업자는 다음 기준에 따라 약관 및 동의서를 적용

- **(시 점)** 알고하는 동의와는 별도로, 고객이 공동인증서 등을 통해 **통합인증(인증서 본인확인서비스)**을 요청*할 때마다 매번 동의 여부를 확인

* 통합인증-002 API 호출을 위한 전자서명 생성시 마다 동의 필요

- **(방 식)** 세부적인 동의 절차* 및 화면UI 등은 개보법 등 관련 법령상의 절차 및 기준을 준수하여 자율적으로 결정

* 예) 고객이 인증방식으로 공동인증서 기반 통합인증을 선택한 후, 인증서 비밀번호 입력 전에 동의 여부 확인

- **(전자서명)** 통합인증시 인증기관의 고객 동의사실 확인을 위해 본인확인 요청 메시지*에 다음의 확인 문구를 포함하여 전자서명

* “[첨부7] 전자서명 요청 및 응답 규격(JSON)”의 “userAgreement” 항목에 확인 문구를 적용

《 고객 동의사실 확인 문구(고정값) 》

금융분야 마이데이터 통합인증을 위한 인증서 본인확인서비스 이용약관, 개인정보 처리, 고유식별정보 수집·이용 및 위탁에 동의합니다.

