금융분야 마이데이터 기술 가이드라인

2022.10.

금융위원회

금융보안원
FINANCIAL SECURITY INSTITUTE

『금융분야 마이데이터 기술 가이드라인』 이용 안내

본 가이드라인은 신용정보법 등 관련 법령 및 규정에서 정하지 않는 세부 절차 등을 제시하여 안전하고 신뢰 가능한 마이데이터서비스를 제공할 수 있도록 마련되었습니다.

관련 법령 및 규정이 본 가이드라인보다 우선하며, 본 가이드라인은 법적인 효력이 없음을 알려드립니다.

본 가이드라인에 기재된 내용 외 이슈사항 및 그에 따른 조치 필요사항은 「마이데이터 표준API 규격 관련 이슈사항 및 대응방안」에 기재되어 마이데이터 테스트베드를 통해 수시로 배포 예정입니다.

또한 최신성 유지를 위해 마이데이터 지원센터 홈페이지를 통해 최신내용임을 확인할 필요가 있습니다.

CONTENTS

제1장 개요

제2장 개인신용정보 전송

제3장
마이데이터 서비스

제4장
마이데이터 본인인증

CONTENTS

제6장
Q&A

제7장
참고

개정 이력

버전	개정일자	내 용	작성자
1.0	2021.2.23	금융분야 마이데이터 기술 가이드라인 제정	금융보안원
1.0	2021.3.23	오탈자 및 내용 오류 수정 - (10p) 전송을 요구하는 개인신용정보 : 비고 '전송받는 기간' 삭제 - (17p) 정기적 전송 : 1주의 기준 시점 '일요일→토요일(7일)'로 변경 - (19p) 개인신용정보 삭제 : 오타 수정 (정보제공자를 정보수신자로 수정) - (26p) 예시표 수정(개인신용정보를 제공받는 자 x→o 로 수정) - (43p) 서비스 등록 준비 TLS 관련 내용 삭제 - (50p) 개인신용정보 전송요구 철회 절차 수정(본인인증 삭제)	금융보안원
1.0	2021.4.19	일부 내용 추가 및 수정 - (12p) 전송지연시 마이데이터사업자의 고객 고지 의무 추가 - (41p, 42p) 개인신용정보 전송 내역 예시 추가 - (46p, 49p, 53p) 인증방식에 따라 일부 절차가 다를 수 있음 안내 추가 - (67p) 그림 수정	금융보안원
1.0	2021.5. 21	- (12p) 지연 전송 재개 안내 - (41p, 42p) 개인신용정보 전송 내역 보관 기간 등 내용 추가 - (78p) 개인신용정보 삭제 내용 수정 - (99p) Q&A 추가 - (103p, 109p) Q&A 내용 수정(테스트베드 관련)	금융보안원

개정 이력

버전	개정일자	내 용	작성자
1.0	2021.7.29.	- (5,6p) 용어 수정 - (10p) 알고하는 동의 반영 - (13p) 지연고지 면제(정기적 전송시) - (17p) API 기준 조회 기간 추가 - (18p) 정기적 전송 주기 변경 - (23p) 스크레이핑 금지 기간 변경 - (32p) 통합인증기관 요건 추가 - (41p) 전송내역 보관기간 변경 - (50p,51p) 개인신용정보 삭제 및 회원 탈퇴 수정 - (58p) 인증수단 제공 방식 변경 - (60p) 인증수단 예시 수정 - (65P) 통합인증수단 제공 방식 변경 - (66p) 통합인증 절차 추가 - (68p) 정보제공자 선택 화면구성 추가 - (97p~115p) Q&A 수정·추가 - (124p) 비대면실명확인 방식 수정	금융보안원
1.0	2021.11.10.	- (15p) 비밀, 보안 계좌 전송 수정 - (26p) 개인신용정보 전송 방식 수정 - (49p) 철회 절차 오류 수정 - (58p) 인증방식 제공 기준 수정 - (69p) 중계기관 본인인증 방식 수정 - (79p) 개인신용정보 삭제 수정 - (83p) 클라우드 이용 관련 문구 수정	금융보안원
1.0	2022.10	- 「금융분야 마이데이터 기술 가이드라인 이용안내」 수정 - (10p) 전송을 요구하는 목적에 '데이터 분석 서비스의 이용' 추가 - (36,40p) 접근토큰·리프레시토큰 발급·관리 의무 추가 - (36,40p) 접근토큰·리프레시토큰 중복 발급 여부 확인 의무 추가 - (52p) 용어 수정 - (55p) 내용 오류 삭제	금융보안원

개정 이력

버전	개정일자	내 용	작성자
		- (66p) 보유자산·상품 확인 단계 생략 안내 추가 - (83p) 중복토큰 관리 및 확인 시 처리 절차 추가 - (106p) Q&A 추가 - (126p) 참고5. 정보제공자용 접근토큰 관리 자체점검표 추가	
1.0	2022.10. (221115 수정)	- (33,44,58,103,108p) 개별인증 제공 필수를 선택으로 변경	금융보안원

PART.

01

개요

1 개요

본 장은 가이드라인의 목적, 적용대상 및 범위, 구성, 용어정의 등 서비스 제공에 있어서 기본적으로 확인해야 할 내용을 다룬다.

1.1. 목적

- 신용정보법에 따른 고객의 개인신용정보 전송요구 및 금융분야 마이데이터서비스 제공과 관련된 세부절차, 기준 등을 제시하여, 관련 이해관계자들이 안전하고 편리한 개인신용정보 전송 및 마이데이터서비스를 제공하도록 하는 데 있다.

1.2. 적용대상 및 범위

- **(대상)** 신용정보법에 따라 개인신용정보를 보유하여 정보주체(이하 고객)의 요구에 따라 개인신용정보를 전송하는 신용정보제공·이용자등(이하 정보제공자)과 고객의 전송요구에 의해 개인신용정보를 전송받는 자(이하 정보수신자), 수집한 개인신용정보를 이용하여 고객에게 개인신용정보 통합조회서비스 등을 제공하는 마이데이터사업자등을 주요 대상으로 한다.

- **(범위)** 신용정보법 상 마이데이터서비스와 관련한 사전준비사항, 전송요구, 전송요구에 따른 데이터 전송 과정에서 개인신용정보를 안전하게 전송하기 위한 방법·절차, 인증 및 보안 사항 등을 다룬다.

참고

본 가이드라인의 내용은 전송대상 간 원활한 개인신용정보 전송, 고객의 이용편의를 해치지 않는 경우, 일부 처리 순서 등을 변경하여 적용할 수 있다.

1.3. 구성

- 본 가이드라인은 총 5장으로 구성되며 각 장의 내용은 아래와 같다.

  - **(1장. 개요)** 가이드라인의 목적과 구성, 용어 정의 등을 설명한다.

  - **(2장. 개인신용정보 전송)** 고객이 정보제공자에게 개인신용정보 전송요구권을 행사하는데 있어서 필요한 기본원칙, 전송방식과 전송유형 등을 설명한다.

  - **(3장. 마이데이터서비스)** 신용정보법 상 마이데이터서비스(통합조회 서비스)와 관련된 참여자의 역할, 준비 필요사항, 참여자 간 세부 전송절차등을 설명한다.

  - **(4장. 마이데이터 본인인증)** 신용정보법 상 마이데이터서비스 제공과 관련하여 고객의 개인신용정보 전송 요구 시 수행되는 고객 본인인증 요건 및 절차 등을 설명한다.

  - **(5장. 마이데이터 보안)** 신용정보법 상 마이데이터서비스와 관련하여 안전한 개인신용정보 전송을 위해 준수해야 할 보안관련사항을 설명한다.

1.4. 용어 정의

- 본 가이드라인에서 사용하는 용어는 아래와 같으며 그 외 용어는 신용정보법 및 관련 법규의 용어를 따른다.

※ 가급적 신용정보법 및 관련 법규의 용어를 따르도록 하였으나, 일부 용어는 보다 쉬운 이해를 위해 별도로 정의하였음(고객, 정보제공자, 정보수신자, 마이데이터사업자 등)

- **(개인신용정보)** 금융거래 등 상거래에서 개인인 정보주체의 신용, 거래내용, 거래능력 등을 판단할 수 있는 정보

- **(고객)** 처리된 개인신용정보로 알아볼 수 있는 정보주체로 개인신용정보 전송 요구권을 행사하는 자(신용정보법 상 개인인 신용정보주체)

- **(정보제공자)** 고객의 개인신용정보 전송요구에 따라 보유하고 있는 고객의 개인신용정보를 정보수신자에게 전송하는 자(신용정보법 상 신용정보제공·이용자)

- **(정보수신자)** 고객의 개인신용정보 전송요구에 따라 정보제공자로부터 고객의 개인신용정보를 제공받는 자

- **(마이데이터사업자)** 금융위원회로부터 본인신용정보업 허가를 받아 고객에게 개인신용정보 통합조회서비스(이하 마이데이터서비스)를 제공하는 자

- **(마이데이터서비스)** 개인신용정보 통합조회서비스 등 마이데이터사업자가 고객에게 제공하는 서비스

- **(개인신용정보 전송요구)** 고객이 자기결정에 따라 해당 고객의 개인신용정보를 보유하고 있는자(이하 정보제공자)로부터 해당 고객의 개인신용정보를 받을 자격이 있는 제3자(이하 정보수신자)에게 전송할 것을 요구하는 행위(신용정보법 제33조의2①)

- **(본인인증)** 고객이 정보제공자에게 개인신용정보 전송을 요구할 때, 고객이 해당 개인신용정보의 소유자임을 정보제공자가 확인하기 위한 방법(개별인증과 통합인증으로 구분)
  - **(개별인증)** 정보제공자가 자율적으로 제공하는 인증수단을 이용한 본인인증 방법으로 고객이 개인신용정보 전송을 요구하는 정보제공자의 수만큼 인증이 이루어지는 방식
  - **(통합인증)** 고객이 공용의 인증수단을 이용하여 인증행위를 1회 수행함으로서 다수의 정보제공자에 인증이 가능한 방식

- **(개인신용정보 전송)** 고객의 개인신용정보 전송요구에 따라 정보제공자로부터 정보수신자로 개인신용정보가 전송되는 과정

- **(API, Application Programming Interface)** 마이데이터사업자와 정보제공자간 개인신용정보를 송수신하기 위한 미리 정의된 표준화된 전송규격 및 절차

- **(마이데이터 종합포털)** 마이데이터 산업 참여기관의 등록 및 관리, 자격증명의 발급 및 관리, 고객의 개인신용정보 전송요구내역 통합조회 서비스 등을 제공하는 마이데이터 지원센터가 제공하는 웹 기반 서비스 (이하 종합포털)

- **(중계기관)** 마이데이터사업자의 API 요청에 대해 하나 이상의 정보제공자를 대신하여 고객의 개인신용정보를 중계하는 신용정보법 상 기관

- **(거점중계기관)** 정보제공자를 대신하여 고객의 전송 요구에 따라 개인신용정보를 마이데이터사업자를 제외한 정보수신자에게 전송하는 기관

- **(인증기관)** 통합인증을 위한 본인인증수단을 발급하고, 발급된 인증수단을 관리하는 기관

- **(TLS 인증서)** 정보제공자와 마이데이터사업자 간 개인신용정보 전송 시 상호인증 및 암호화 채널 형성을 위한 인증서

- **(자격증명)** API 요청시 상호간 자격을 인증하고 식별하기 위해 종합포털로부터 발급받는 값

- **(접근토큰)** API를 이용하여 개인신용정보 전송을 요청한 마이데이터사업자가 정보제공자가 보유하고 있는 해당 고객의 개인신용정보에 접근할 수 있는 자격이 있는지를 확인하기 위해 발급받는 정보

PART.
02

개인신용정보 전송

2 개인신용정보 전송

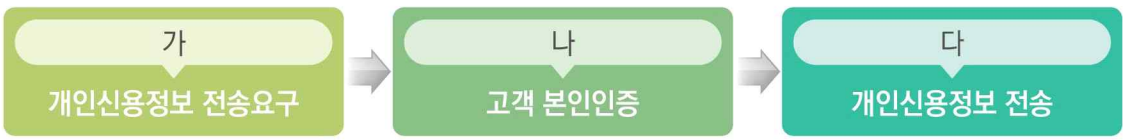
본 장은 고객, 정보제공자, 정보수신자간에 이루어지는 개인신용정보 전송 원칙과 각 유형별 전송 절차를 다룬다

각 유형별 전송규격 및 절차는 별도의 규격을 참조할 필요가 있으며, API 규격을 이용한 마이데이터 서비스 절차는 3장에서 설명한다.

2.1. 개인신용정보 전송 개요

- 개인신용정보 전송은 ❶개인신용정보 전송요구, ❷고객 본인인증 ❸개인신용정보 전송의 3단계로 이루어진다.

〈 개인신용정보 전송 절차 〉



가. 개인신용정보 전송요구

- **(개인신용정보 전송요구)** 고객은 정보제공자에게 본인의 개인신용정보를 정보수신자에 전송할 것을 요구할 수 있다.

〈 개인신용정보 전송 시 정보제공자 및 정보수신자 예시 〉

분류	예시
정보제공자	금융회사, 공공기관, 마이데이터사업자 등
정보수신자	고객, 마이데이터사업자, 금융회사 등

※ 개인신용정보를 제공 및 수신할 수 있는 전체 대상은 「[참고1] 정보제공자·정보수신자 범위」 참조

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ① 개인인 신용정보주체는 신용정보제공·이용자등에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 다음 각 호의 어느 하나에 해당하는 자에게 전송하여 줄 것을 요구할 수 있다.

  1. 해당 신용정보주체 본인
  2. 본인신용정보관리회사
  3. 대통령령으로 정하는 신용정보제공·이용자
  4. 개인신용평가회사
  5. 그 밖에 제1호부터 제4호까지의 규정에서 정한 자와 유사한 자로서 대통령령으로 정하는 자

- **(전송 요구 방법)** 고객은 정보제공자를 통해 비대면 방식으로 개인신용정보 전송을 요구할 수 있다.

  ※ 금융회사 창구등을 통한 대면 전송요구 방식은 제반여건에 따라 추후 검토

- **(전송 요구 사항)** 고객은 개인신용정보 전송요구 시 아래와 같이 법령상 요구하는 내용을 특정하여야 한다.

  - **(전송 요구 화면 구성)** 정보제공자는 고객이 전송요구 사항을 안전하고 편리하게 특정할 수 있도록 관련 양식, 화면 등을 제공해야 한다.

〈 전송요구 시 특정 정보 〉

분류	내용	비고
전송요구를 받는 자	개인신용정보를 보유하고 있는 정보제공자	• 정보제공자(상호/명칭)
개인신용정보를 제공받는 자	개인신용정보를 전송받는 정보수신자 (고객, 마이데이터사업자, 기타수신자 등)	• 정보수신자(상호/명칭)
전송을 요구하는 개인신용정보	고객이 전송 요구하고자 하는 개인신용정보	• 정보의 항목
정기적 전송을 요구하는지 여부	개인신용정보의 정확성 및 최신성을 유지하기 위해서 정기적으로 개인신용정보를 전송 받을지 여부와 전송 주기	• 요구/미요구 • 주기(주1회)
전송요구 종료 시점	개인신용정보 전송 요구의 종료 시점	• 최대 1년
전송을 요구하는 목적	개인신용정보 전송을 요구하는 목적	• 전송요구를 통한 본인 신용정보 통합조회 서비스의 이용 • 데이터 분석 서비스의 이용
전송을 요구하는 개인신용정보의 보유기간	개인신용정보를 전송받은 정보수신자가 수집한 정보를 보유할 수 있는 기간	• 서비스 종료시 또는 삭제 요구시까지

※ 특정 정보에 대한 상세 구성은 신용정보원의 '알고하는 동의' 참조

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ⑤ 개인인 신용정보주체가 제1항 각 호의 어느 하나에 해당하는 자에게 제1항에 따른 전송요구를 할 때에는 다음 각 호의 사항을 모두 특정하여 전자문서나 그 밖에 안전성과 신뢰성이 확보된 방법으로 하여야 한다.
  1. 신용정보제공·이용자등으로서 전송요구를 받는 자
  2. 전송을 요구하는 개인신용정보
  3. 전송요구에 따라 개인신용정보를 제공받는 자
  4. 정기적인 전송을 요구하는지 여부 및 요구하는 경우 그 주기
  5. 그 밖에 제1호부터 제4호까지의 규정에서 정한 사항과 유사한 사항으로서 대통령령으로 정하는 사항

- **신용정보법시행령 제28조의3(개인신용정보의 전송요구)** ⑧ 법 제33조의2제5항제5호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.
  1. 전송요구의 종료시점
  2. 그 밖에 금융위원회가 정하여 고시하는 사항

- **신용정보업감독규정 제39조의2(개인신용정보의 전송요구권)** ① 영 제28조의3제8항제2호에서 "그 밖에 금융위원회가 정하여 고시하는 사항"이란 다음 각 호의 사항을 말한다.
  1. 전송을 요구하는 목적
  2. 전송을 요구하는 개인신용정보의 보유기간

나. 고객 본인인증

○ **(고객 본인인증)** 고객의 개인신용정보 전송요구를 받은 정보제공자는 본인인증을 통해 고객 본인 여부를 확인한 후에 개인신용정보를 전송하여야 한다.

- **(본인인증 방식)** 전송요구 대상(정보제공자, 정보수신자), 전송요구 규격 및 방식(API방식, API외 방식)에 따라 개별인증 또는 통합인증을 선택적으로 적용된다.

※ 고객 본인인증 적용에 대한 상세 내용은 「4장. 본인인증」에서 다룬다.

다. 개인신용정보 전송

○ **(개인신용정보 전송)** 고객의 전송요구를 받은 정보제공자는 장애로 인한 지연을 제외하고는 개인신용정보를 즉시 전송하여야 한다.

- **(즉시 전송)** 정보제공자는 개인신용정보 전송요구를 받은 시점에 보유하고 있는 개인신용정보를 정보수신자에게 지체없이 전송하여야 한다.

즉시 전송 관련 사항

① 정보제공자는 개인신용정보 전송요청을 확인한 즉시 전산시스템에서 개인신용정보를 조회하여 응답하여야 하며, 개인신용정보 조회 및 전송 등 전산처리에 걸리는 시간 이외에 고의적인 지연이 있어서는 안 된다.

② 정보제공자는 개인신용정보 전송이 각사의 본질적인 금융업무에 영향을 줄 수 있다고 판단되는 경우 기간시스템 원장DB가 아닌 별도의 개인신용정보 저장·전송시스템을 두어 처리 할 수 있다. 단, 이 경우에도 ①과 마찬가지로 개인신용정보를 즉시 조회하여 전송하여야 하며, 기간시스템 원장DB에 저장된 개인신용정보를 조회하는 경우와 최신성에서 차이가 없어야 한다.

- **(지연 전송)** 정보제공자는 전산시스템 장애등으로 인해 전송이 지연되거나 불가한 경우, 고객에게 마이데이터서비스, 이메일, 모바일메신저 또는 SMS 등을 이용하여 지연 사유를 고지하고 해당 사유 해소 후 즉시 정보수신자에게 개인신용정보를 전송*하여야 한다.

* 클라이언트의 요청이 필요한 API의 전송특성 상 정보제공자가 자체적으로 전송을 재개하기 어려운 경우, 마이데이터사업자 및 고객의 전송 재요청에 응하여 전송을 재개할 수 있다.

※ 개인신용정보 전송 요구로부터 5분이 경과하였을 경우 지연으로 봄

- **(지연 고지)** 정보제공자는 전송지연이 발생할 경우, 마이데이터사업자를 통해 고객에 지연사유를 고지할 수 있다. 단, 정보제공자가 서버 장애 등으로 인해 API 응답 지연을 인지하지 못하거나 고지할 수 없는 경우, 일정 시간 동안 회신을 받지 못한 마이데이터사업자는 장애로 판단하고, 정보제공자를 대신하여 고객에게 지연을 안내하여야 한다.

※ 고객의 명시적 전송 요청이 없는 정기적 전송 요청의 경우 고객에 지연 고지하지 않음

관련법령

- **신용정보법시행령 제28조의3(개인신용정보의 전송요구)**

  ⑤ 제4항에 따른 개인신용정보의 전송이 전산시스템 장애 등으로 지연되거나 불가한 경우에는 전송이 지연된 사실 및 그 사유를 개인인 신용정보주체에게 통지하고, 그 사유가 해소된 즉시 개인신용정보를 전송해야 한다.

- **(전송 거절 또는 정지·중단)** 정보제공자는 아래의 거절 사유 발생 시, 개인신용정보 전송 요구를 거절 또는 정지·중단할 수 있다. 이 경우, 정보제공자는 고객에게 마이데이터서비스, 이메일, 모바일메신저 또는 SMS 등을 이용하여 전송요구 거절 또는 정지·중단 사유를 고지하여야 한다.

전송 요구 거절 또는 정지·중단사유

- 고객 본인이 전송요구를 한 사실이 확인되지 아니하는 경우
- 고객 본인이 전송요구를 하였으나 제3자의 기망이나 협박에 의하여 전송요구를 한 것으로 의심되는 경우
- 전송 요구 사항이 특정되지 않은 경우
- 적법한 정보수신자가 아닌 자에게 전송하여 줄 것을 요구한 경우
- 고객의 인증정보 탈취 등 부당한 방법에 의한 전송요구임을 알게 된 경우 등

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ⑧ 제1항에 따라 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다.

- **신용정보법 시행령 제28조의3(개인신용정보의 전송요구)** ⑪ 법 제33조의2제8항에서 "대통령령으로 정하는 경우"란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인인 신용정보주체 본인이 전송요구를 한 사실이 확인되지 않은 경우
2. 신용정보주체 본인이 전송요구를 했으나 제3자의 기망이나 협박 때문에 전송요구를 한 것으로 의심되는 경우
3. 법 제33조의2제1항 각 호의 자가 아닌 자에게 전송해 줄 것을 요구한 경우
4. 법 제33조의2제5항에서 정한 사항이 준수되지 않은 경우
5. 개인인 신용정보주체의 인증정보 탈취 등 부당한 방법으로 인한 전송요구임을 알게 된 경우
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 경우와 유사한 경우로서 금융위원회가 정하여 고시하는 경우

⑫ 법 제33조의2제8항에 따라 전송요구를 받은 신용정보제공·이용자등이 전송요구를 거절하거나 전송을 정지·중단한 경우에는 지체 없이 해당 사실을 개인인 신용정보주체에게 통지해야 한다.

2.2. 개인신용정보 전송 원칙

○ **(전송 요구 정보)** 고객은 정보제공자가 고객으로부터 수집한 개인신용정보 등에 대해 전송 요구를 할 수 있다.

※ 타 정보제공자로부터 수집한 정보는 개인신용정보 전송 의무 없음

전송 요구 정보

- 정보제공자가 고객으로부터 수집한 정보
- 고객이 정보제공자에게 제공한 정보
- 고객과 정보제공자 간의 권리·의무 관계에서 생성된 정보

- **(대상정보)** 정보제공자는 신용정보법 시행령「[별표1] 본인신용정보관리업에 관한 신용정보의 범위」및「마이데이터 API 표준 규격」에서 정한 범위 내에서 개인신용정보를 전송할 수 있으며, 상기 범위에 따라 정보를 제공하되 필요시 업권 협의를 통해 개인신용정보 전송 대상을 추가할 수 있다.

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ② 제1항에 따라 개인인 신용정보주체가 전송을 요구할 수 있는 본인에 관한 개인신용정보의 범위는 다음 각 호의 요소를 모두 고려하여 대통령령으로 정한다.

1. 해당 신용정보주체(법령 등에 따라 그 신용정보주체의 신용정보를 처리하는 자를 포함한다. 이하 이 호에서 같다)와 신용정보제공·이용자등 사이에서 처리된 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보일 것
   가. 신용정보제공·이용자등이 신용정보주체로부터 수집한 정보
   나. 신용정보주체가 신용정보제공·이용자등에게 제공한 정보
   다. 신용정보주체와 신용정보제공·이용자등 간의 권리·의무 관계에서 생성된 정보
2. 컴퓨터 등 정보처리장치로 처리된 신용정보일 것
3. 신용정보제공·이용자등이 개인신용정보를 기초로 별도로 생성하거나 가공한 신용정보가 아닐 것

※ 구체적인 개인신용정보 전송 요구 대상 범위 및 내역 등은 별도로 배포되는「금융분야 마이데이터서비스 가이드라인」및「금융분야 마이데이터 표준 API 규격」참고

- **(보안·비밀 계좌 정보 전송)** 보안 계좌, 비밀 계좌 등과 같이 고객이 정보제공자에 비대면 정보 조회 금지를 요청한 정보는 원칙적으로 개인신용정보 전송요구 대상에서 제외된다. 해당 정보에 대해 전송요구를 하고자 하는 경우, 보안·비밀 계좌를 금융회사 창구 등을 이용하여 일반 계좌로 전환 후에 전송요구를 수행할 수 있다.

관련법령

- **신용정보법 시행령 제28조의3(개인신용정보의 전송요구)** ③개인인 신용정보주체는 법 제33조의2 제1항 및 제4항에 따라 개인신용정보의 전송요구권을 행사하는 경우에는 법 제32조제1항 각 호의 어느 하나에 해당하는 방법으로 해야 한다. 다만, 개인인 신용정보주체의 요청으로 특약사항을 기재하거나 약정하여 해당 정보의 제3자 제공을 금지한 경우 또는 비대면 정보 조회를 금지한 경우에는 해당 정보에 대하여 대면으로 전송요구권을 행사해야 한다.

○ **(전송 형태)** 정보제공자는 전송을 요구받은 개인신용정보를 컴퓨터 등 정보처리장치로 처리 가능한 형태로 정보수신자에게 전송하여야 한다.

※ 여기서 '정보처리장치로 처리가 가능한 형태'라 함은 정보수신자의 데이터베이스와 같은 정보처리장치에 전산상 자동화된 방식으로 이관(export)이 가능한 형태를 의미한다.

- 단, 고객이 최근 5년 내의 개인신용정보가 아닌 정보에 대해 전송을 요구할 경우, 정보제공자는 컴퓨터 등 정보처리장치로 처리 가능한 방식으로의 제공을 우선하되, 출력문서 등과 같이 사람이 인지할 수 있는 방식(컴퓨터 등 정보처리장치로 처리 가능한 방식 외의 방식)으로도 제공할 수 있다.

※ 5년 이내의 개인신용정보라 하더라도 삭제된 정보는 제공할 수 없으므로 전송 의무를 지지 않음

관련법령

- **신용정보법 시행령 제28조의3(개인신용정보의 전송요구)** ④ 제3항에 따라 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 전송요구를 받은 개인신용정보를 컴퓨터 처리가 가능한 방식으로 즉시 전송해야 한다. 다만, 최근 5년 내의 개인신용정보가 아닌 경우에는 신용정보제공·이용자등이 정하는 방식으로 제공할 수 있다.

- **(전송요구 기간)** 고객은 최대 1년까지 개인신용정보 전송을 요구할 수 있으며, 1년 이내에서 고객이 정한 정보전송 요구의 종료시점이 지나면 개인신용정보 전송을 다시 요구하여야 한다. 단, 고객은 종료시점이 도래하기 이전에 전송요구 기간을 변경하거나 연장할 수 있다.

- **(조회 기간)** 정보수신자가 API방식을 통해 개인신용정보를 조회하는 경우 과도한 전송트래픽 집중, 정보제공자 API서버 과부하, 전송지연 등을 방지하기 위해 일(Date) 기준 API는 최대 31일, 월(Month) 기준 API는 최대 3개월로 조회기간(From/To)을 설정하여 요청하여야 한다.

기준	업권	API ID	API 명
일(Date) 기준 조회 API	은행,금투,보험	IRP-004	개인형 IRP 계좌 거래내역 조회
	은행	은행-004	수신계좌 거래내역 조회
		은행-007	투자상품계좌 거래내역 조회
		은행-010	대출상품계좌 거래내역 조회
	카드	카드-008	국내 승인내역 조회
		카드-009	해외 승인내역 조회
	금투	금투-003	계좌 거래내역 조회
	보험	보험-006	보험 거래내역 조회
		보험-007	자동차보험 거래내역 조회
		보험-011	대출상품 거래내역 조회
	전금	전금-004	선불 거래내역 조회
		전금-103	결제내역 조회
	할부금융	할부금융-004	대출상품계좌 거래내역 조회
		할부금융-006	운용리스 거래내역 조회
	보증보험	보증보험-003	보증보험 거래내역 조회
	통신	통신-004	통신 결제내역 조회
월(Month) 기준 조회 API	카드	카드-004	청구 기본정보 조회
	통신	통신-003	통신 거래내역(납입내역) 조회

○ **(전송 주기)** 정기적 전송과 비정기적 전송으로 나뉜다.

- **(정기적 전송)** 개인신용정보의 정확성 및 최신성 유지를 위해 고객은 전송요구 기간 동안 정보제공자에 정기적으로 개인신용정보를 전송할 것을 요구할 수 있다. 단, 마이데이터사업자가 고객의 정기적 전송 요구에 의해 정보제공자에 개인신용정보를 요청할 경우, 원칙적으로 사전에 정의된 횟수(1주 1회) 이하로 개인신용정보 전송 요청이 가능하다.

  * 1주의 기준 시점은 일요일에서 토요일(7일)로 함

※ 정기적 전송 시 수수료 부과가 가능하며, 관련하여 「금융분야 마이데이터서비스 가이드라인」 참고

예시 **고객요청에 의한 정기적 전송 예시**

● **(정기적 전송)** 고객이 개인신용정보 전송을 정기적으로 요청할 경우, 마이데이터사업자는 1주 1회에 한하여 개인신용정보 전송요청이 가능하다.

- **(비정기적 전송)** 고객은 전송 요구 기간 내 비정기적으로 정보제공자에 개인신용정보를 전송할 것을 요구할 수 있다. 고객이 정보제공자가 제공하는 서비스에 접속하여 마이데이터서비스의 실행, 새로고침 등을 통해 개인신용정보를 조회하는 경우 등이 이에 해당된다.

예시 고객 요청에 의한 비정기적 전송 예시

- **(비정기적 전송)** 고객은 다운로드, 마이데이터서비스 실행, 새로고침등을 수행하여 개인신용정보를 비정기적으로 전송요구할 수 있다. 이와 같은 비정기적 전송요구에 대한 별도의 횟수 제한은 없다.

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ④ 제1항에 따라 신용정보주체 본인이 개인신용정보의 전송을 요구하는 경우 신용정보제공·이용자등에 대하여 해당 개인신용정보의 정확성 및 최신성이 유지될 수 있도록 정기적으로 같은 내역의 개인신용정보를 전송하여 줄 것을 요구할 수 있다.

- **신용정보법 시행령 제22조의9(본인신용정보관리회사의 행위규칙)** ⑥ 신용정보제공·이용자 등은 제33조의2제4항에 따라 개인신용정보를 정기적으로 전송할 경우에는 필요한 범위에서 최소한의 비용을 본인신용정보관리회사가 부담하도록 할 수 있다.

- **(개인신용정보 삭제)** 정보수신자등과 같이 개인신용정보 전송 요구에 의해 개인신용정보를 보유한 자는 고객이 개인신용정보 전송 요구시 특정한 개인신용정보 보유기간이 지났을 경우, 또는 고객이 개인신용정보 삭제를 명시적으로 요구할 경우, 해당 개인신용정보를 완전히 삭제하여야 한다.

  ※ 개인신용정보 삭제시 신용정보법 시행령 제17조의2(개인신용정보의 관리방법 등)를 따라 복구 또는 재생되지 않도록 삭제하여야 한다.

참고

- 마이데이터사업자는 고객이 개인신용정보 철회를 요구할 경우, 고객에게 개인신용정보 삭제 여부를 선택할 수 있는 인터페이스를 제공하여야 한다.

※ 상세내용은 3.4. 마이데이터 개인신용정보 전송 내역 관리 참조

관련법령

- **제17조의2(개인신용정보의 관리방법 등)** ⑦ 신용정보제공·이용자는 제1항제2호 및 법 제20조의2 제2항 각 호 외의 부분 본문에 따라 신용정보주체의 개인신용정보를 삭제하는 경우 그 삭제된 개인신용정보가 복구 또는 재생되지 아니하도록 조치하여야 한다.

2.3. 개인신용정보 전송 방식

○ **(전송방법)** API 방식 및 API 외 방식으로 전송이 가능하다.

- **(API방식)** 사전에 정의된 API 규격에 따라 개인신용정보를 전달하는 방식으로, 마이데이터사업자가 고객의 전송요구에 따라 정보제공자에게 개인신용정보 전송을 요청하는 경우 반드시 API방식을 이용해야 한다. API방식의 전송과 관련 상세 절차는 「3. 마이데이터서비스」에서 설명한다.

※ 세부 API 전송 규격은 「금융분야 마이데이터 표준 API 규격」 참고

- **(스크린 스크레이핑 방식 등 이용 금지)** 마이데이터사업자는 반드시 API방식과 같은 정해진 방식을 이용하여 개인신용정보를 수집하여야하며 전자식카드, 이용자번호 등의 접근매체 또는 고객의 신분증표 제시 등의 수단 등과 같이 법령상 금지하는 방식으로 개인신용정보를 수집할 수 없다.

관련법령

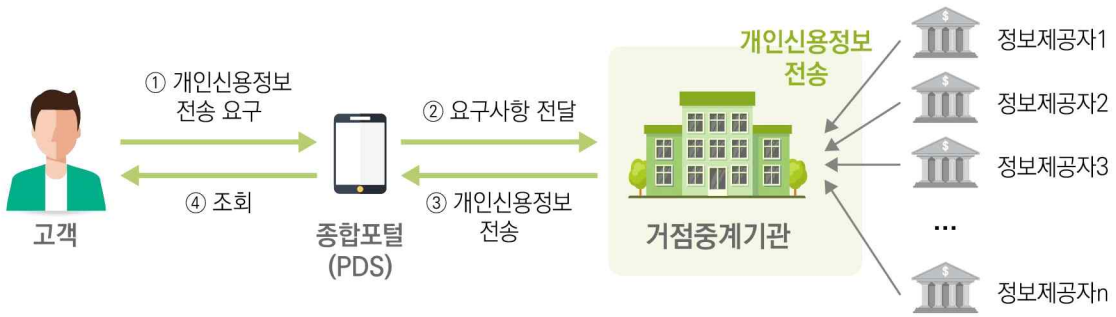
- **신용정보법 제22조의9(본인신용정보관리회사의 행위규칙)** ③ 본인신용정보관리회사는 다음 각 호의 수단을 대통령령으로 정하는 방식으로 사용·보관함으로써 신용정보주체에게 교부할 신용정보를 수집하여서는 아니 된다.
  1. 대통령령으로 정하는 신용정보제공·이용자나 「개인정보 보호법」에 따른 공공기관으로서 대통령령으로 정하는 공공기관 또는 본인신용정보관리회사(이하 이 조 및 제33조의2에서 "신용정보제공·이용자등"이라 한다)가 선정하여 사용·관리하는 신용정보주체 본인에 관한 수단으로서 「전자금융거래법」 제2조 제10호에 따른 접근매체
  2. 본인임을 확인받는 수단으로서 본인의 신분을 나타내는 증표 제시 또는 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법

- **(API 외 방식)** 정보제공자가 전문 등과 같이 API 이외의 방식을 이용하여 개인신용정보를 전송하는 방식으로, 마이데이터사업자 이외의 정보수신자가 고객을 위해 개인신용정보를 수집할 때 적용할 수 있는 방식을 말한다.

2.4. 개인신용정보 전송 유형

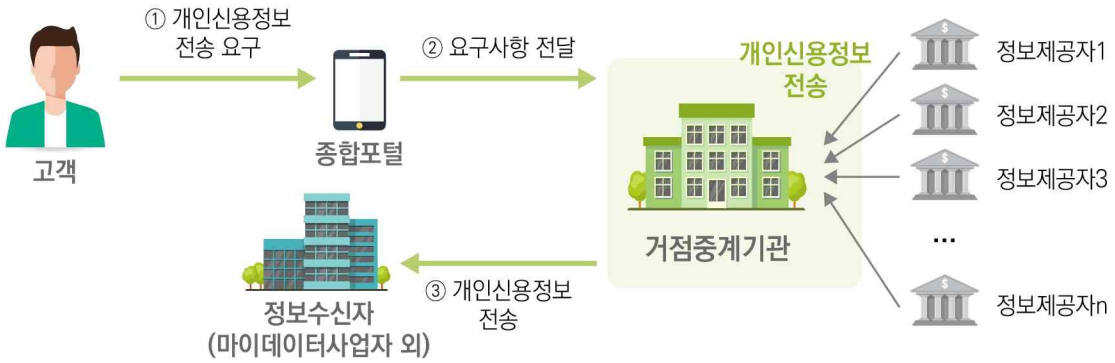
○ 개인신용정보 전송 유형은 아래와 같이 크게 3가지로 분류된다.

❶ **(고객에 전송)** 고객이 종합포털을 통해 정보제공자에 고객 본인에게 개인신용정보를 전송할 것을 요구하면, 정보제공자는 고객이 해당 개인신용정보를 조회·활용할 수 있도록 거점중계기관을 통해 고객의 PDS에 개인신용정보를 전송한다.



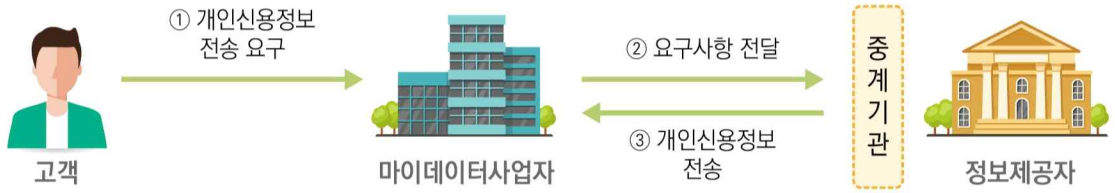
※ 상기 절차는 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 서비스 가이드라인」 참고

❷ (마이데이터사업자 외 기관에 전송) 고객이 종합포털을 통해 마이데이터사업자 외 기관에 개인신용정보를 전송할 것을 요구하면, 정보제공자는 거점중계기관을 통해 개인신용정보를 전송한다.



※ 상기 절차는 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 서비스 가이드라인」 참고

❸ (마이데이터사업자에 전송) 고객이 마이데이터사업자에게 개인신용정보를 전송할 것을 요구하면, 해당 정보제공자가 마이데이터사업자에게 API를 이용하여 개인신용정보를 전송한다.



〈 참고 : 전송 유형 비교 〉

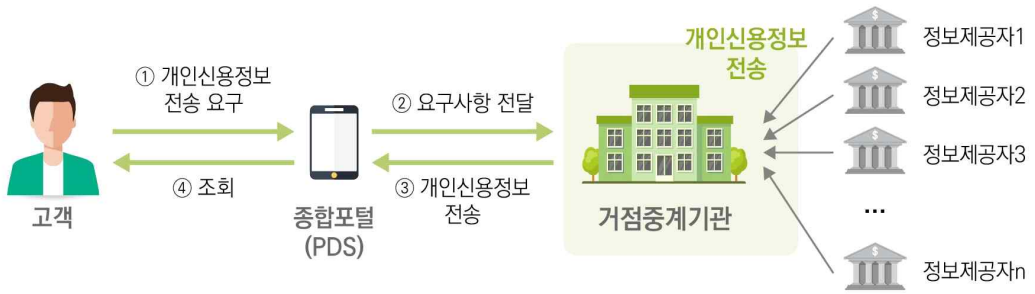
구분	① 고객에 전송	② 마이데이터사업자 외 기관에 전송	③ 마이데이터사업자에 전송
용도	개인신용정보 전송	개인신용정보 전송	마이데이터 서비스
전송요구 주체	고객	고객	고객
전송요구 요청 대상	정보제공자	정보수신자	정보수신자
정보 수신자	고객	마이데이터사업자 외 정보수신자	마이데이터 사업자
전송방식	API 외 방식 + API 방식	API 외 방식 + API 방식	API방식
본인인증	통합인증과 유사 또는 이에 준하는 방식	통합인증과 유사 또는 이에 준하는 방식	개별인증 통합인증
중계기관, 거점중계기관	거점중계기관	거점중계기관	중계기관

※ 스크린 스크레이핑이 금지되는 2022.1.1. 이후 마이데이터사업자가 정보제공자로부터 개인신용정보를 수집할 경우, 정보제공자-마이데이터사업자는 반드시 API를 이용하여 개인신용정보를 전송하여야 한다.

2.5. 전송 유형별 전송 절차 및 규격

가. 고객에 개인신용정보 전송

〈 고객에 개인신용정보 전송 〉



- **(전송 요구)** 고객은 종합포털을 통해 개인신용정보 전송을 요구(비대면요구)할 수 있다. 이때 고객은 아래의 내용을 특정하여 전송을 요구하여야 한다.

〈 전송 요구시 특정 사항 예시 〉

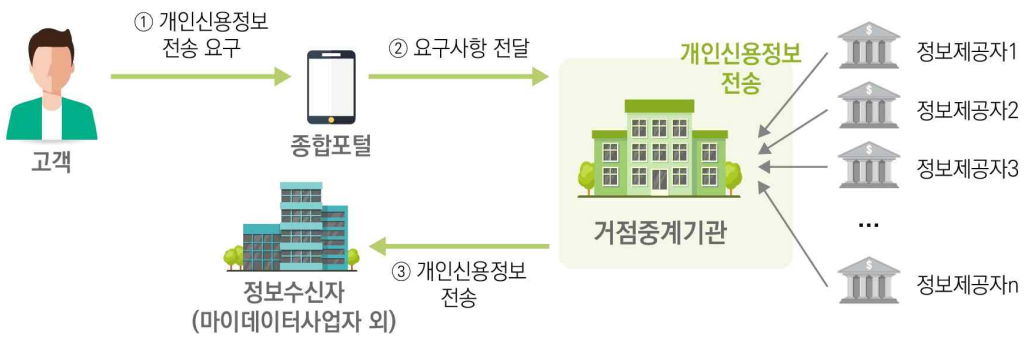
특정 사항	특정 필요	설 명
전송요구를 받는 자	○	
개인신용정보를 제공받는 자	×	본인
전송을 요구하는 개인신용정보	○	
정기적 전송을 요구하는지 여부 및 요구 시 그 주기	○	
전송요구의 종료시점	○	
전송을 요구하는 목적	○	
전송을 요구하는 개인신용정보의 보유기간	○	

- **(본인인증)** 정보제공자는 신뢰할 수 있는 제3의 기관(이하 종합포털(App), 거점중계기관)이 제공하는 통합인증 결과에 따라 전송요구 주체가 고객 본인임을 확인한다.

- **(전송 절차 및 규격)** PDS(Personal Data Storage)를 통해 전송하며 규격, 절차 및 보호대책은 별도로 정하는 바에 따른다.
  ※ 상기 내용은 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 서비스 가이드라인」 참고

나. 마이데이터사업자 외 기관에 개인신용정보 전송

〈 마이데이터사업자 외 기관에 개인신용정보 전송 〉



- **(전송 요구)** 고객은 종합포털을 이용하여 개인신용정보 전송을 요구할 수 있으며 이때 아래의 내용을 특정하여 전송을 요구하여야 한다.

〈 전송 요구시 특정 사항 예시 〉

특정 사항	특정 필요	설 명
전송요구를 받는 자	○	
개인신용정보를 제공받는 자	○	해당 정보수신자
전송을 요구하는 개인신용정보	○	정보주체가 직접 입력 또는 선택
정기적 전송을 요구하는지 여부 및 요구 시 그 주기	○	
전송요구의 종료시점	○	
전송을 요구하는 목적	○	
전송을 요구하는 개인신용정보의 보유기간	○	

- **(본인인증)** 정보제공자는 신뢰할 수 있는 제3의 기관(이하 종합포털(App), 거점중계기관)이 제공하는 통합인증 결과에 따라 전송요구 주체가 고객 본인임을 확인한다.

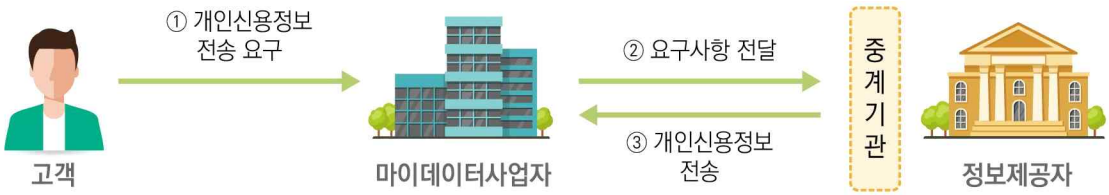
- **(전송 방식)** 전송요구 주체가 고객본인임이 확인되면 정보제공자가 정보수신자에게 거점중계기관을 통해 개인신용정보를 전송한다.

- **(규격 및 절차)** 거점중계기관이 정보제공자와 정보수신자를 중계하여 개인신용정보를 전송하며 규격, 절차 및 보호대책은 별도로 정하는 바에 따른다.

  ※ 상기 내용은 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 서비스 가이드라인」 참고

다. 마이데이터사업자에 개인신용정보 전송

〈 마이데이터사업자에 개인신용정보 전송 〉



※ 공공 마이데이터(국세, 지방세, 사회보험료 납부정보 등)에 대한 중계 관련 업무는 한국신용정보원에서 수행

- **(전송 요구)** 정보주체는 마이데이터사업자가 제공하는 웹 및 모바일 서비스를 이용하여 개인신용정보 전송을 요구할 수 있으며 이때 아래의 내용을 특정하여 전송을 요구하여야 한다.

〈 전송 요구시 특정 사항 〉

특정 사항	특정 필요	설 명
전송요구를 받는 자	○	정보제공자
개인신용정보를 제공받는 자	×	해당 마이데이터사업자
전송을 요구하는 개인신용정보	○	정보주체가 직접 입력 또는 선택
정기적 전송을 요구하는지 여부 및 요구 시 그 주기	○	
전송요구의 종료시점	○	
전송을 요구하는 목적	○	
전송을 요구하는 개인신용정보의 보유기간	○	

- **(본인인증)** 정보제공자는 자체적으로 제공하는 인증수단(개별인증) 또는 공통으로 제공되는 인증수단(통합인증)을 통해 고객본인임을 확인한다.

- **(전송 방식)** 본인인증을 통해 고객본인임이 확인되면 정보제공자는 마이데이터사업자에게 직접 또는 중계기관을 통해 개인신용정보를 전송한다.

- **(규격 및 절차)** 별도로 정해진 API규격과 관련절차를 통해 개인신용정보를 전송하여야 하며, 개인신용정보 전송 관련 상세 절차는 3장. 마이데이터서비스에서 설명한다.

www.fsec.or.kr

금융분야 마이데이터 기술 가이드라인

PART.

03

마이데이터서비스

3 마이데이터서비스

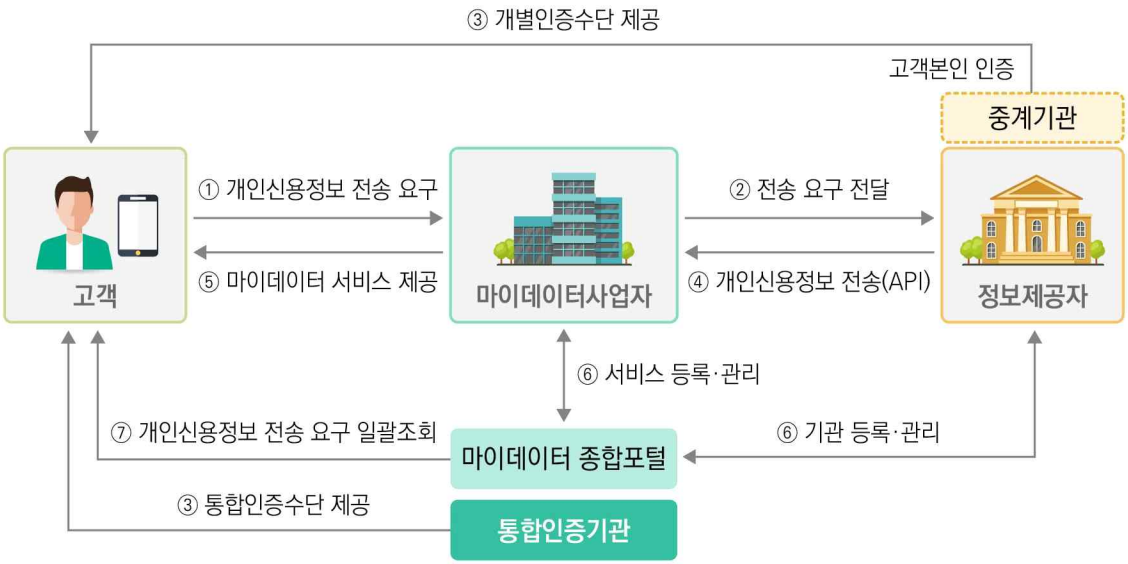
본 장은 마이데이터사업자가 API방식을 이용하여 고객의 개인신용정보를 수집하고 고객에게 통합조회 서비스를 제공하는 것과 관련된 준비사항, 세부절차 등을 설명한다.

3.1. 마이데이터서비스 개요 및 참여자 역할

- 마이데이터사업자는 고객의 개인신용정보 전송 요구를 통해 정보제공자로부터 개인신용정보를 API방식으로('21년 8월 이후) 수집하고, 수집한 개인신용정보를 저장·분석하여 고객에게 마이데이터서비스(통합조회 등)를 제공하게 된다.

가. 마이데이터서비스 주요절차

〈 마이데이터서비스 구성 및 절차 〉



- **(개인신용정보 전송 요구)** ① 고객은 마이데이터사업자가 제공하는 마이데이터서비스를 이용하여, ② 본인의 개인신용정보를 보유하고 있는 정보제공자를 대상으로 API규격에 따라 개인신용정보를 전송할 것을 요구한다.

- **(개인신용정보 전송)** ③ 고객의 개인신용정보를 보유하고 있는 정보제공자는 인증수단을 활용하여 고객 본인임을 확인하고, ④ API규격에 따라 마이데이터사업자에 개인신용정보를 전송한다.

- **(마이데이터서비스 제공)** ⑤ 마이데이터사업자는 하나 이상의 정보제공자로부터 수집된 고객의 개인신용정보를 토대로 통합조회 등 마이데이터서비스를 고객에게 제공한다.

- **(종합포털 등 지원업무)** ⑥ 종합포털은 정보제공자와 마이데이터사업자간의 신뢰관계 형성을 지원하고, ⑦ 고객에게 전송요구 이력 일괄 조회등의 서비스를 제공한다.

※ ⑥~⑦의 종합포털 등의 지원업무는 ①~⑤의 마이데이터서비스 절차 순서와는 무관하다.

나. 마이데이터서비스 주요 참여자 및 역할

- **(참여자)** 마이데이터서비스는 고객·정보제공자·중계기관·마이데이터사업자·마이데이터 종합포털·인증기관 등으로 구성되며 세부요건과 역할은 다음과 같다.

〈 마이데이터 참여자 요건 및 주요 역할 〉

참여자	요건	역할
고객	하나 이상의 정보제공자에 개인신용정보를 보유한 자	• 개인신용정보 전송 요구 • 마이데이터서비스 이용
정보제공자	고객의 개인신용정보를 보유하고 있는 자로 신용정보법상 신용정보제공·이용자등	• 개인신용정보 제공(전송) • 개별인증수단 발급·관리 • 고객 본인인증
중계기관	신용정보법령 상 중계기관	• 개인신용정보 전송중계 • 고객 본인인증
마이데이터 사업자	금융위원회로부터 본인신용정보관리업 허가를 받은 자	• 개인신용정보 전송 요구 전달 • 개인신용정보 수신 • 마이데이터서비스 제공 등
마이데이터 종합포털	신용정보법 상 마이데이터 지원기관	• 서비스 등록·관리 • 자격증명 발급·관리 • 개인신용정보 전송 요구 내용 일괄조회 기능지원 • 실환경 테스트 등
통합인증기관	CI활용이 가능한 인증수단 제공기관 (본인확인기관, 전자서명인증사업자 등)	• 통합인증 수단 발급·관리

- **(고객)** 고객은 하나 이상의 정보제공자에 본인의 개인신용정보를 보유한 자로 자신의 개인신용정보를 수집·관리하는 정보제공자를 대상으로 자신의 개인신용정보를 전송하기를 희망하는 마이데이터사업자에게 개인신용정보를 전송하도록 요구할 수 있다.

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ① 개인인 신용정보주체는 신용정보제공·이용자등에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 다음 각 호의 어느 하나에 해당하는 자에게 전송하여 줄 것을 요구할 수 있다.

  1. 해당 신용정보주체 본인
  2. 본인신용정보관리회사
  3. 대통령령으로 정하는 신용정보제공·이용자
  4. 개인신용평가회사
  5. 그 밖에 제1호부터 제4호까지의 규정에서 정한 자와 유사한 자로서 대통령령으로 정하는 자

- **(정보제공자)** 고객의 개인신용정보 전송 요구에 응하여, 전송요구 주체가 고객 본인임이 확인되면 마이데이터사업자에게 해당 고객의 개인신용정보를 전송하여야 한다.

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ⑧ 제1항에 따라 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다.

- **(마이데이터사업자)** 고객이 정보제공자에 개인신용정보 전송요구를 할 수 있도록 지원하고 정보제공자로부터 전송받은 고객의 개인신용정보를 활용하여 고객에게 통합조회 등의 마이데이터서비스를 제공한다.

- **(마이데이터 종합포털)** 정보제공자와 마이데이터사업자를 등록·관리하고 고객의 개인신용정보 전송 요구 내역 일괄조회 등 마이데이터서비스를 위한 지원기능을 제공한다.

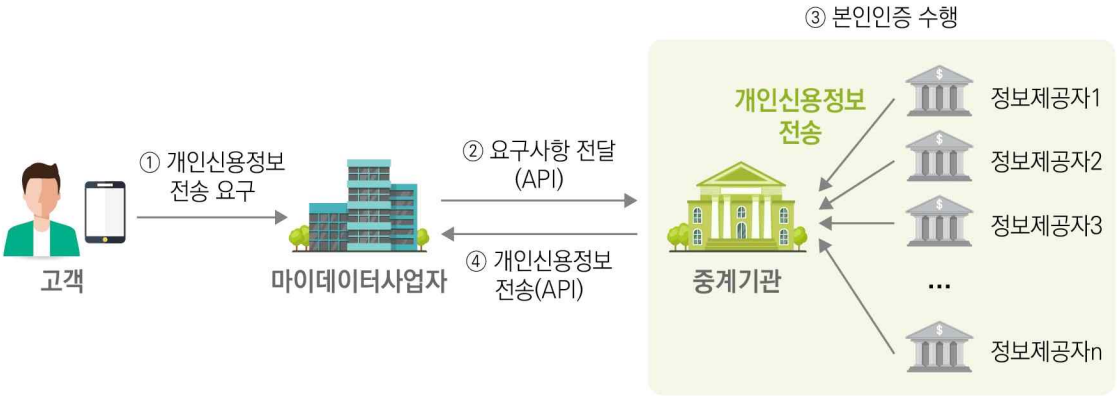
- **(인증기관)** 통합인증을 위한 본인인증수단을 발급하고 발급된 인증수단을 관리한다.

  - 정보제공자와 마이데이터사업자는 인증기관이 발급하는 인증수단(통합인증)을 고객에 제공하여야 하며 정보제공자가 개별적으로 마련한 별도의 인증수단(개별인증)은 선택하여 제공할 수 있다.

※ 본인인증에 대한 상세 설명은 4장. 마이데이터 본인인증 참조

- **(중계기관)** 중소형 금융회사 등(세부 기준은 관련 법령 및 고시 참고)과 같은 일부 정보제공자를 대신하여 고객의 개인신용정보 전송 요구에 따라 마이데이터사업자에 개인신용정보를 전송할 수 있다.

〈 중계기관을 이용한 개인신용정보 전송 요구 절차 〉



(참고) 마이데이터 중계기관

- 종합신용정보집중기관
- 사단법인 금융결제원
- 상호저축은행중앙회, 새마을금고중앙회, 각 협동조합의 중앙회
- 중앙기록관리기관
- 행정안전부, 코스콤
- 한국정보통신진흥협회

※ 중계기관과 정보제공자 간 전송규격, 절차 등은 중계기관이 정한 별도의 규격과 절차를 따른다.

관련법령

- **신용정보법 제22조의9(본인신용정보관리회사의 행위규칙)** ⑤ 제4항에도 불구하고 신용정보제공·이용자등의 규모, 금융거래 등 상거래의 빈도 등을 고려하여 대통령령으로 정하는 경우에 해당 신용정보제공·이용자등은 대통령령으로 정하는 중계기관을 통하여 본인신용정보관리회사에 개인신용정보를 전송할 수 있다.

- **신용정보법시행령 제18조의6(본인신용정보관리회사의 행위규칙 등)** ⑧ 법 제22조의9제5항에서 "대통령령으로 정하는 경우"란 법 제22조의9제3항제1호의 신용정보제공·이용자등의 특성을 고려하여 자산 규모, 관리하고 있는 개인신용정보의 수, 시장 점유율, 외부 전산시스템 이용 여부 등 금융위원회가 정하여 고시하는 기준에 해당하는 경우를 말한다.

- **신용정보법감독규정 제23조의3(본인신용정보관리회사의 행위규칙 등)** ③ 영 제18조의6제8항에서 "금융위원회가 정하여 고시하는 기준"이란 신용정보제공·이용자등이 다음 각 호의 어느 하나에 해당하지 않는 경우를 말한다.

  1. 영 제5조제2항제1호에 따른 은행, 같은 조 제8호에 따른 금융투자업자(투자중개업자에 한한다), 같은 조 제15호에 따른 보험회사, 같은 조 제16호에 따른 여신전문금융회사(신용카드업자에 한한다)인 경우에는 개인신용정보를 처리하는 자로서 다음 각 목에 모두 해당하는 경우
     가. 직전연도 말 기준 자산총액이 10조원 이상인 경우
     나. 직전년도 말 기준 해당 업권 전체가 보유하고 있는 개인신용정보의 총 수에서 당해 회사가 보유하고 있는 개인신용정보의 비율(이하 "시장점유율"이라 한다)이 다음의 어느 하나에 해당하는 경우
        1) 시장점유율이 자기보다 높은 자의 시장점유율과 자기의 시장점유율을 합하여 100분의 90 이하인 경우
        2) 해당 회사 단독으로 시장점유율이 100분의 5 이상인 경우
     다. 자신의 정보처리 업무를 제3자에게 위탁하거나 자신의 정보처리 업무를 제3자와 공동으로 수행하지 않는 경우
  2. 「전기통신사업법 시행령」 제37조의6제1항에 따른 이동통신서비스를 제공하는 전기통신사업자로서 같은 법 시행령 제58조제1항제3호에 따른 "전기통신이용자" 수가 직전연도 말 기준 해당 업권 전체 전기통신이용자의 100분의 15 이상인 경우
  3. 법 제2조제5호에 따른 신용정보회사에 해당하는 경우. 다만, 신용조사회사는 제외한다.
  4. 법 제2조제9호의3에 따른 본인신용정보관리회사에 해당하는 경우. 다만, 제1호에 따른 금융투자업자가 「상법」에 따라 설립된 주식회사 코스콤에 자신의 정보처리 업무를 위탁한 경우는 제외한다.

다. 마이데이터서비스 주요 제공 기능 및 참여자 역할

○ 마이데이터서비스 주요 제공기능은 아래와 같으며 각 참여자는 서비스 제공에 필요한 업무를 수행해야 한다.

〈 마이데이터서비스 참여자 별 주요 역할 〉

역할	마이데이터사업자	정보제공자	마이데이터 종합포털
개인신용정보 전송요구사항 전달	O		
개인신용정보 전송	O	O	
개인신용정보 전송요구 관리	O		
허가요건 준수	O		
보안 고려사항 준수	O	O	
보안수준 진단(상시평가)	O	O	
기능 적합성 심사 및 서비스 취약점 점검	O		
API 시스템 개발·관리	O	O	O
접근토큰·리프레시토큰 발급 관리		O	
접근토큰·리프레시토큰 중복발급 확인	O		
마이데이터서비스 제공	O		
기관간 상호인증	O	O	O
고객 본인인증		O	
요구 내역 일괄 조회			O
참여기관 등록·관리			O
자격증명 발급·관리			O
개인신용정보 송수신 내역 기록·보관	O	O	
개인신용정보 수신 내역 통지	O		

개인신용정보 전송 요구사항 전달

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

고객이 마이데이터사업자를 통해 정보제공자에게 개인신용정보 전송을 요구할 경우, 마이데이터사업자는 고객의 개인신용정보 전송요구사항을 변경없이 API규격을 이용하여 정보제공자에게 전달하여야 한다.

※ 관련 규격은 금융분야 마이데이터 표준 API 규격 참조

개인신용정보 전송(API)

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

고객이 마이데이터사업자를 통해 정보제공자에게 개인신용정보 전송을 요구할 경우, 정보제공자는 개인신용정보 전송요구 주체가 고객 본인임을 확인 한 후 API를 이용하여 개인신용정보를 안전하게 전송하여야 한다.
(마이데이터사업자도 정보제공자로서 개인신용정보 전송의 의무를 갖는다.)

※ 관련 규격은 금융분야 마이데이터 표준 API 규격 참조

관련법령

- **신용정보법 제22조의9(본인신용정보관리회사의 행위규칙)** ④ 신용정보제공·이용자등은 개인인 신용정보주체가 본인신용정보관리회사에 본인에 관한 개인신용정보의 전송을 요구하는 경우에는 정보제공의 안전성과 신뢰성이 보장될 수 있는 방식으로서 대통령령으로 정하는 방식으로 해당 개인인 신용정보주체의 개인신용정보를 그 본인신용정보관리회사에 직접 전송하여야 한다.

개인신용정보 전송요구 관리 (조회·변경·철회)

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

고객이 본인의 개인신용정보 전송요구 내역을 관리(조회·변경·철회)할 수 있도록 사용자 인터페이스를 제공하여야 한다. 이때 변경이나 철회 절차를 최초 전송요구에 필요한 절차보다 어렵게 해서는 안 된다.

관련법령

- **신용정보법 시행령 제18조의6(본인신용정보관리회사의 행위규칙 등)** ① 법 제22조의9 제1항제2호에서 "대통령령으로 정하는 행위"란 다음 각 호의 어느 하나에 해당하는 행위를 말한다.

  1.~3. (생략)

  4. 본인신용정보관리회사 자신 또는 제3자에 대한 전송요구의 변경 및 철회의 방법을 최초 전송요구에 필요한 절차보다 어렵게 하는 행위

  5.~11. (생략)

허가요건 준수

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

신용정보업 감독규정에서 정한 본인신용정보관리업 허가요건을 준수하여야 한다.

※ 본인신용정보관리업 허가요건 중 일부는 보안 고려사항의 내용을 포함

※ 상세 허가요건 및 절차는 「[참고2] 본인신용정보관리업자 허가요건 및 절차」 및 금융감독원이 배포한 「본인신용정보관리업(MyData) 허가 매뉴얼」 참고

관련법령

- **신용정보업감독규정 제5조(신용정보업 허가 등의 절차)** ①다음각호에따른절차는별표1과같다.

  1. 법 제4조에 따른 신용정보업, 본인신용정보관리업 및 채권추심업 허가

  2,3. (생략)

  ② 다음 각 호에 따른 허가 등을 신청하려는 자(이하 "신청인"이라 한다)는 다음 각 호에서 각각 정하는 서식 및 별표 1의2에 따른 신청서류를 제출하여야 한다.

  1. 영 제4조에 따라 신용정보업, 본인신용정보관리업 및 채권추심업의 허가를 받으려는 신청인: 별지 제1호 서식
  2. 영 제4조에 따라 신용정보업, 본인신용정보관리업 및 채권추심업의 허가받은 사항에 대한 변경 허가를 받으려는 신청인: 별지 제2호 서식

보안 고려사항 준수

마이데이터사업자 정보제공자 마이데이터종합포털

개인신용정보를 안전하게 처리하기 위하여 신용정보법 제19조①항의 기술적·물리적·관리적 보호대책, 제20조③, ④항 의 신용정보관리·보호인 지정 및 본 가이드라인 내 「5장.마이데이터 보안」을 적용하며, 클라우드 이용, 망분리 등 신용정보법에서 별도로 규정하지 않은 조항은 전자금융거래법 등 해당법령을 참고하여 준수하여야 한다.

관련법령

- **신용정보법 제19조(신용정보전산시스템의 안전보호)** ① 신용정보회사등은 신용정보전산시스템(제25조6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.
- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ③신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 제4항에 따른 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자는 신용정보관리·보호인을 임원(신용정보의 관리·보호 등을 총괄하는 지위에 있는 자로서 대통령령으로 정하는 자를 포함한다)으로 하여야 한다.

  ④ 제3항에 따른 신용정보관리·보호인은 다음 각 호의 업무를 수행한다.
  1~2.(생략)

보안수준 진단(상시평가)

마이데이터사업자 정보제공자 마이데이터종합포털

금융권 정보보호 상시평가제를 통하여 보안수준 진단을 수행하여야 한다.

관련법령

- **신용정보법 제45조의5(개인신용정보 활용·관리 실태에 대한 상시평가)** ① 금융위원회는 대통령령으로 정하는 신용정보회사등이 제20조제6항에 따라 신용정보관리·보호인을 통하여 점검한 결과를 제출받아 확인하고, 그 결과를 점수 또는 등급으로 표시할 수 있다.

기능 적합성 심사 및 보안 취약점 점검

마이데이터사업자 정보제공자 마이데이터종합포털

마이데이터사업자는 고객에게 마이데이터서비스를 제공하기 전 해당 서비스가 표준 API규격에 맞게 개발되어있는지 확인하기 위한 기능 적합성 심사와 보안 취약점 점검을 수행하여야 한다.

※ 취약점 점검 대상, 시기 및 방법 등은 추후 가이드라인 개정시 반영 예정

API 시스템 개발·관리

마이데이터사업자 **정보제공자** **마이데이터종합포털**

고객의 개인신용정보 및 전송요구 관련 정보를 송·수신하기 위한 API 시스템을 개발하고 관리하여야 한다.

※ 데이터 전송을 위한 API 시스템을 개발하여야 하며 서비스 제공 전에 API가 표준에 맞게 개발되었는지 확인하여야 한다. (종합포털과 연계된 API테스트베드를 이용하여 API가 표준에 맞게 적절히 개발되었는지 확인)

접근토큰·리프레시토큰 발급·관리

마이데이터사업자 **정보제공자** 마이데이터종합포털

접근토큰·리프레시토큰을 규격에 맞게 발급하고 안전하게 관리하여야 한다.

* 접근토큰·리프레시토큰이 중복발급되지 않아야하며, 원활하게 갱신되도록 하여야 한다.
* 이를 위해 [참고5]정보제공자용 접근토큰 관리 자체점검표'를 참고하여 주기적으로(연1회이상) 자체점검을 실시하여야하며, 금융당국 및 지원기관은 자체점검 결과를 요청할 수 있다.

접근토큰·리프레시토큰 중복발급 확인

마이데이터사업자 정보제공자 마이데이터종합포털

접근토큰·리프레시토큰 수신시 기존 토큰과의 중복 여부를 확인하여야한다. 단 실시간 확인으로 인해 시스템 부하 등 서비스에 중대한 차질이 발생할 경우 최소 1일1회 이상 확인한다.

* 접근토큰 중복발급으로 인한 책임은 원칙적으로 정보제공자에 있으며, 안전한 마이데이터 서비스 제공 환경 조성을 위하여 마이데이터 사업자는 토큰 중복 발급 확인 의무가 부여된다.

마이데이터서비스 제공

마이데이터사업자 정보제공자 마이데이터종합포털

API를 통해 전송받은 데이터를 수집·분석하여 고객에게 마이데이터서비스(개인신용정보 통합조회 서비스)를 제공한다.

기관간 상호인증

마이데이터사업자 **정보제공자** **마이데이터종합포털**

TLS인증서를 이용하여 마이데이터사업자와 정보제공자, 마이데이터종합포털 간 안전한 개인신용정보 및 데이터 전송을 위한 상호인증을 수행한다.

※ 안전한 개인신용정보 전송을 위해 마이데이터사업자와 정보제공자 간 상호인증을 수행하고, 참여자 관리 등을 위해서 마이데이터종합포털과 금융회사, 마이데이터사업자 간 상호인증을 수행한다.

고객 본인인증

마이데이터사업자 **정보제공자** 마이데이터종합포털

고객의 개인신용정보 전송 요구에 응하기 전에 본인인증을 수행하여 반드시 고객 본인 여부를 확인하여야 한다.

요구 내역 일괄 조회

마이데이터사업자 정보제공자 **마이데이터종합포털**

고객이 요구한 개인신용정보 전송 요구 내역을 통합적으로 조회하는 기능을 제공한다.

참여기관 등록·관리

마이데이터사업자 정보제공자 **마이데이터종합포털**

정보제공자와 마이데이터사업자(마이데이터서비스)를 종합포털에 등록하고 관리한다.

자격증명 발급·관리

마이데이터사업자 정보제공자 **마이데이터종합포털**

정보제공자와 마이데이터사업자 간 API 호출 자격을 인증하고 식별하기 위한 자격증명을 발급하고 관리한다.

개인신용정보 전송 내역 관리·보관

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

개인신용정보를 전송하는 정보제공자(또는 중계기관)와 개인신용정보를 전송받는 마이데이터사업자(또는 중계기관)는 개인신용정보 전송 내역을 관리·보관하여야 한다. 개인신용정보 전송 내역에는 개인신용정보 전송 요구 특정사항을 반드시 포함하되 그 외 사항은 자율적으로 구성한다. 개인신용정보 전송 내역은 고객의 서비스이용 종료 시 폐기한다.

〈 개인신용정보 전송 내역 기록 예시〉

개인신용정보 전송 내역(ID:전송202104141300)	
전송요구를 받는 자	A은행
개인신용정보를 제공받는 자	'가' 마이데이터 사업자
전송을 요구하는 개인신용정보	계좌1 (123-12-001234) 계좌2 (123-13-004321)
정기적 전송을 요구하는지 여부 및 요구 시 그 주기	정기적 전송 요구
전송요구의 종료시점	1년
전송을 요구하는 목적	통합자산관리
전송을 요구하는 개인신용정보의 보유기간	서비스 해지 시까지

관련법령

- **신용정보법 시행령 제18조의6(본인신용정보관리회사의 행위규칙 등)** ⑩ 법 제22조의9제4항 및 제5항에 따라 개인신용정보를 전송한 신용정보제공·이용자등과 개인신용정보를 전송받은 중계기관 및 본인신용정보관리회사는 전송내역에 대한 기록을 작성하고 보관해야 하며, 본인신용정보관리회사는 전송받은 신용정보내역에 관한 기록을 신용정보주체에게 연 1회 이상 통지해야 한다.

개인신용정보 전송 내역 통지

마이데이터사업자 | 정보제공자 | 마이데이터종합포털

마이데이터사업자는 전송받은 개인신용정보 내역에 관한 기록을 고객에 연 1회 이상 통지*하여야 한다. 개인신용정보 전송 내역에는 개인신용정보 전송 요구 특정사항을 반드시 포함하되 그 외 사항은 자율적으로 구성한다.

* 1년 이내 철회된 전송 요구에 대해서도 통지 필요(철회되었음을 명시)

〈 개인신용정보 전송 내역 기록 예시〉

개인신용정보 전송 내역(ID:전송202104141300)	
전송요구를 받는 자	A은행
개인신용정보를 제공받는 자	'가' 마이데이터 사업자
전송을 요구하는 개인신용정보	계좌1 (123-12-001234) 계좌2 (123-13-004321)
정기적 전송을 요구하는지 여부 및 요구 시 그 주기	정기적 전송 요구
전송요구의 종료시점	1년
전송을 요구하는 목적	통합자산관리
전송을 요구하는 개인신용정보의 보유기간	서비스 해지 시까지

관련법령

- **신용정보법 시행령 제18조의6(본인신용정보관리회사의 행위규칙 등)** ⑩ 법 제22조의9 제4항 및 제5항에 따라 개인신용정보를 전송한 신용정보제공·이용자등과 개인신용정보를 전송받은 중계기관 및 본인신용정보관리회사는 전송내역에 대한 기록을 작성하고 보관해야 하며, 본인신용정보관리회사는 전송받은 신용정보내역에 관한 기록을 신용정보주체에게 연 1회 이상 통지해야 한다.

3.2. 마이데이터서비스 등록 준비

- 정보제공자와 마이데이터사업자는 고객에게 마이데이터서비스를 제공하기 위해 마이데이터 종합포털에 기관정보 등을 등록한 후 자격증명을 발급받아야 한다.

  ※ 상세 등록절차는 「금융분야 마이데이터 서비스 가이드라인」 참고

  - **(정보제공자 등록)** 정보제공자는 고객의 개인신용정보 전송을 수행하기 위해 마이데이터 종합포털에 기관정보 등을 등록하고 자격증명을 발급받아야 한다.

  - **(마이데이터서비스 등록)** 마이데이터사업자는 고객에게 마이데이터서비스를 제공하기 위해 종합포털에 기관정보, 마이데이터서비스 정보 등을 등록하고 자격증명을 발급받아야 한다.

3.3. 마이데이터 개인신용정보 전송 절차

- **(전송 요구)** ①, ② 고객은 마이데이터사업자를 통해 정보제공자에게 개인신용정보를 전송할 것을 요구한다.

- **(본인인증)** ③ 정보제공자는 본인인증을 통해 고객 본인임을 확인한 후에 고객 개인신용정보를 전송하여야 한다. 이때 정보제공자는 본인인증수단으로서 통합인증 방식을 제공하여야 한다.

  ※ 개별인증 제공 여부는 선택
  ※ 상세 본인인증 절차는 4장.본인인증 참조

- **(접근토큰 발급)** ④, ⑤ 정보제공자는 고객본인의 전송요구임이 확인(본인인증)되면 접근토큰을 발급하여 API요청을 허용한다.

- **(개인신용정보 전송)** ⑥, ⑦ 정보제공자는 마이데이터사업자가 유효한 접근토큰을 이용하여 API규격에 따라 전송요청을 하는 경우에 한하여 개인신용정보를 전송한다.

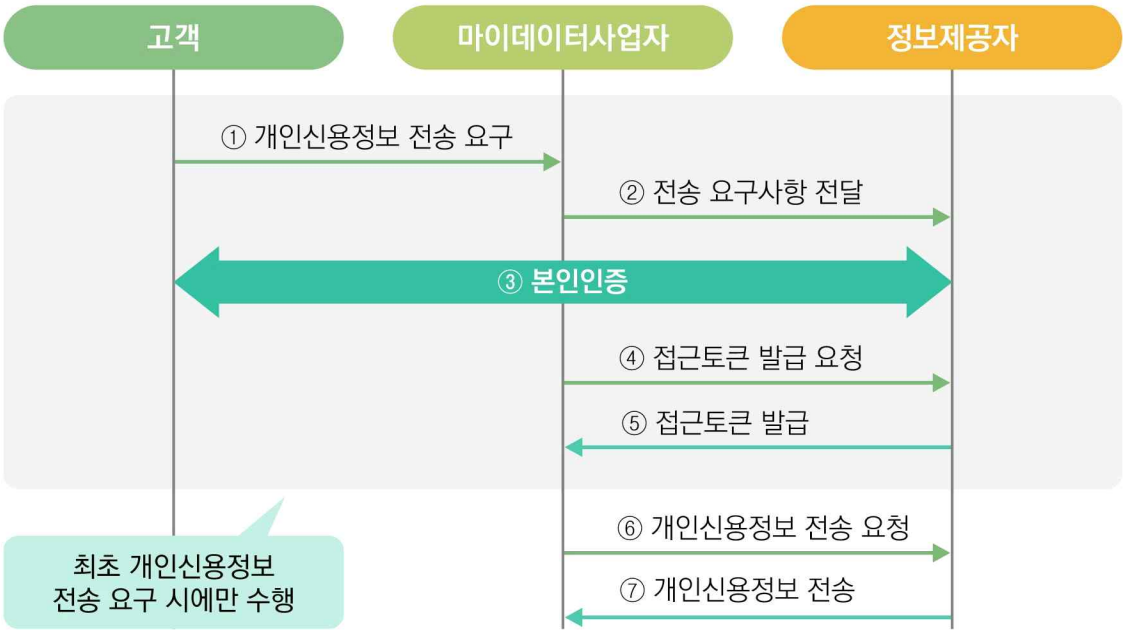
  ※ 상세 전송 절차 및 관련 API는 별도배포되는 「금융분야 마이데이터 표준API 규격」 참조

  – **(전송규격)** 정보제공자와 마이데이터사업자 간 개인신용정보 전송 시 반드시 표준 API방식을 사용한다.

참고

- 신용정보법령에 따라 중계기관을 이용할수 있는 정보제공자는 중계기관으로 하여금 마이데이터 사업자에게 개인신용정보를 전송하도록 할 수 있다. 이 경우에도 마찬가지로 중계기관과 마이데이터사업자 간 개인신용정보 요청 및 전송은 표준 API방식을 사용해야 한다. 다만, 중계기관과 정보제공자간 전송규격, 절차 등은 중계기관과 정보제공자 간 자율적으로 정할 수 있다.

〈 개인신용정보 전송 절차 〉



❶ **(개인신용정보 전송요구)** 고객은 마이데이터사업자가 제공하는 마이데이터서비스를 통해 개인신용정보 전송을 정보제공자에 요구

❷ **(전송 요구사항 전달)** 마이데이터사업자는 고객의 개인신용정보 전송 요구사항을 정보제공자에 전달

❸ **(본인인증)** 정보제공자는 본인인증 수단을 이용하여 개인신용정보 전송을 요구한 고객의 본인인증을 수행

❹ **(접근토큰 발급 요청)** 마이데이터사업자는 개인신용정보 전송 요청 권한을 획득하기 위해 정보제공자에 접근토큰 발급을 요청

❺ **(접근토큰 발급)** 고객이 전송요구한 개인신용정보 전송요구 권한을 포함하는 접근토큰을 생성하여 마이데이터사업자에게 발급

※ 최초 개인신용정보 전송요구 시만 ❶~❺ 과정을 수행하며 이후 별도의 변경내역 없이 개인신용정보 전송 시는 기발급된 접근토큰을 이용하여 전송 수행

※ ❶~❺ 과정은 인증방식(개별 또는 통합)에 따라 일부 절차가 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 표준API 규격」 참조

❻ **(개인신용정보 전송 요청)** 마이데이터사업자는 접근토큰을 이용하여 정보제공자에 고객이 전송 요구한 개인신용정보를 전송할 것을 요청

❼ **(개인신용정보 전송)** 정보제공자는 접근토큰 유효성을 확인하고 고객의 개인신용정보를 마이데이터사업자에게 전송

3.4. 마이데이터 개인신용정보 전송 내역 관리

- 마이데이터사업자는 고객에게 개인신용정보 전송 내역 조회, 변경 및 철회를 할 수 있는 기능을 제공해야 한다. 이때 변경 및 철회를 최초 전송 요구보다 어렵게 해서는 안된다.

가. 마이데이터 개인신용정보 전송요구 내역 조회

- **(전송요구 내역 조회)** 고객은 마이데이터사업자에게 기존의 개인신용정보 전송요구 내역에 대한 조회 요청을 할 수 있으며, 마이데이터사업자는 이에 대응할 수 있는 환경을 고객에게 제공해야 한다.

예시 **고객에 제공하는 전송 요구 내역 항목**

- 개인신용정보를 전송하는 정보제공자 정보
- 전송요구한 개인신용정보 세부 항목
- 실제 전송된 개인신용정보 세부 항목 및 전송 기간
- 개인신용정보 수집 목적 및 용도
- 개인신용정보 전송 요구 일시 및 만료 일시 등

- **(전송요구 내역 일괄 조회)** 고객은 종합포털이 제공하는 전송요구 내역 일괄 조회 기능을 이용하여, 마이데이터사업자를 통해 요구한 전체 개인신용정보 전송요구 내역을 조회할 수 있다.

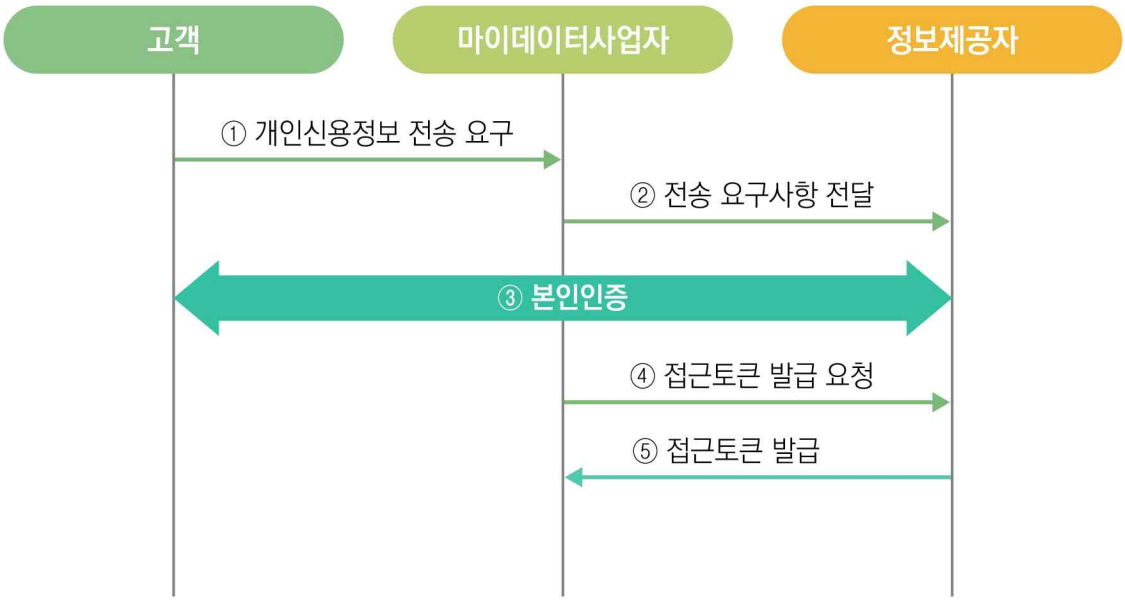
※ 상세 절차는 「금융분야 마이데이터 서비스 가이드라인」 참조

나. 마이데이터 개인신용정보 전송요구 내역 변경

○ **(전송요구 내역 변경)** 고객은 기존 전송요구 내역의 전송세부항목, 기간 등에 대해 변경 필요성이 생겨 고객이 새로운 전송요구를 통해 내역 변경을 요청하는 것을 의미하는 것으로 마이데이터사업자는 이에 응하는 환경을 제공하여야 한다.

- **(내역 변경 절차)** 고객이 요구 내역 변경을 포함하는 전송요구를 생성하여 마이데이터 사업자를 통해 정보제공자에게 전송하면, 정보제공자는 고객 본인의 변경 요청임을 본인인증을 통해 확인하여 전송요구 내역을 변경하고, 변경 내역을 반영한 새로운 접근토큰을 생성하여 마이데이터사업자에게 발급한다.

〈 개인신용정보 전송요구 내역 변경 〉



❶ **(전송요구 내역 변경 요청)** 고객은 마이데이터사업자를 통해 개인신용정보 전송요구 내역 변경을 요청

❷ **(전송요구 내역 변경 요청 전달)** 마이데이터사업자는 고객의 개인신용정보 전송요구 내역 변경 요청을 정보제공자에게 전달

❸ **(본인인증)** 정보제공자는 본인인증 수단을 이용하여 고객의 개인신용정보 전송요구 변경 요청에 대한 고객 본인인증을 수행

❹ **(접근토큰 신규 발급 요구)** 마이데이터사업자는 변경된 개인신용정보 전송 요청 권한을 획득하기 위해 정보제공자에 접근토큰 발급을 요청

❺ **(접근토큰 발급)** 고객이 전송요구한 개인신용정보 전송요구 권한을 포함하는 접근토큰을 생성하여 마이데이터사업자에게 발급하고 기발급된 접근토큰 폐기

※ ❶~❺ 과정은 인증방식(개별 또는 통합)에 따라 일부 절차가 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 표준API 규격」 참조

다. 마이데이터 개인신용정보 전송요구 내역 철회

○ **(전송요구 철회)** 고객이 전송요구의 필요성이 없어져 개인신용정보 전송을 중지해달라고 요청하는 것으로 마이데이터사업자는 이에 응하는 환경을 제공하여야 한다.

- **(철회 절차)** 고객이 마이데이터사업자를 통해 개인신용정보 전송요구 철회를 요청할 경우, 정보제공자는 기발급된 접근토큰을 폐기함으로서 개인신용정보 전송요구를 철회한다.

- **(철회 주의사항 고지)** 마이데이터사업자는 고객이 개인신용정보 전송요구 철회 시 주의사항에 대해 고객의 철회 수행 전에 고지하여야 한다.

예시 **철회시 고지 항목**

- 수집한 개인신용정보 목록 및 수집 기간
- 수집한 개인신용정보 보유기간
- 철회 시 발생할 수 있는 서비스 불이익 등 안내

- **(삭제 여부 알림)** 마이데이터사업자는 고객에게 전송요구 철회 시 수집한 개인신용정보가 삭제되는 것이 아님을 알리고, 철회와 동시에 수집된 정보를 삭제할 것인지 고객이 선택할 수 있도록 인터페이스를 제공하여야 한다.

- **(개인신용정보 삭제)** 마이데이터사업자는 수집한 개인신용정보에 대해 고객이 삭제 요청할 수 있도록 개인신용정보 삭제 메뉴를 제공하며, 이때, 고객은 정보제공자 단위 이상으로 삭제할 개인신용정보를 선택할 수 있어야 한다. 만일 삭제 대상 개인신용정보의 전송요구가 유효할 경우 고객에 안내 후, 해당 전송요구를 철회한다.

- **(회원탈퇴)** 마이데이터사업자는 고객이 필요시 마이데이터서비스 이용을 중지할 수 있도록 회원탈퇴 메뉴를 제공하여야 한다.

※ 뱅킹앱 등과 같이 인앱(in-app) 형태로 마이데이터서비스를 제공하는 경우, 고객에게 해당 마이데이터서비스에 대한 이용 해지 기능 등을 제공

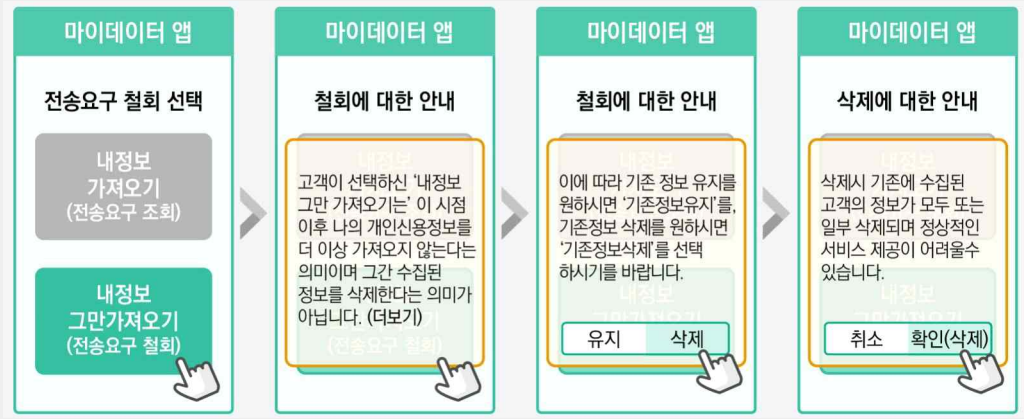
- **(회원탈퇴시 전송요구 철회 및 삭제)** 마이데이터사업자는 고객이 서비스탈퇴(회원탈퇴)를 요청하는 경우, 모든 전송요구를 철회하고 해당 고객의 개인신용정보를 즉시 삭제하여야 한다.

(참고) 서비스 탈퇴, 전송 철회 시 개인신용정보 삭제 관련

- **(서비스 탈퇴)** 고객이 더 이상 마이데이터 서비스 이용을 원하지 않아 서비스 탈퇴(회원탈퇴)를 요청할 경우, 마이데이터사업자는 서비스 탈퇴와 동시에 모든 전송요구를 철회하고 해당 고객의 개인신용정보를 즉시 모두 삭제하여야 한다.
- **(전송 철회)** 전송 철회과정에서 고객 필요에 따라 개인신용정보 삭제를 할 수 있도록 화면을 제공해야 하며(아래 참조), 고객이 삭제를 요청하는 경우 해당 고객의 개인신용정보를 즉시 삭제하여야 한다.

※ 이 경우, 삭제 범위는 전송 요구 이후 수집한 고객의 개인신용정보로 한정한다.

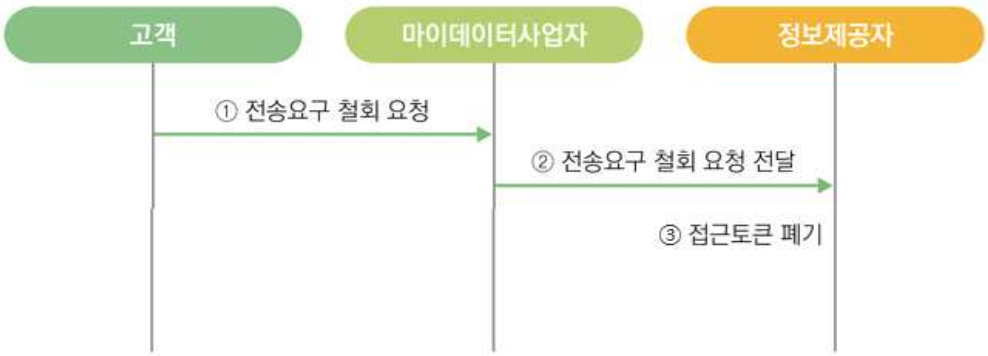
〈 (예시) 마이데이터사업자의 개인신용정보 전송요구 철회 시나리오 〉



• **(그 외)** 마이데이터사업자는 최초 요구 시 특정한 개인신용정보 보유기간이 지났을 경우 또는 고객이 명시적으로 삭제를 요구할 경우 수집한 개인신용정보를 삭제 하여야 한다.

※ 상기 삭제 관련 내용은 기능 적합성 심사, 상시평가 등을 통해 확인

〈 개인신용정보 전송요구 철회 〉



❶ **(전송요구 철회 요청)** 고객은 마이데이터사업자를 통해 개인신용정보 전송요구 철회를 요청

❷ **(전송요구 철회 요청 전달)** 마이데이터사업자는 고객의 개인신용정보 전송요구 철회 요청을 정보제공자에게 전달

❸ **(접근토큰 폐기)** 정보제공자는 기발급된 접근토큰을 폐기

라. 마이데이터 개인신용정보 전송요구 기간 연장

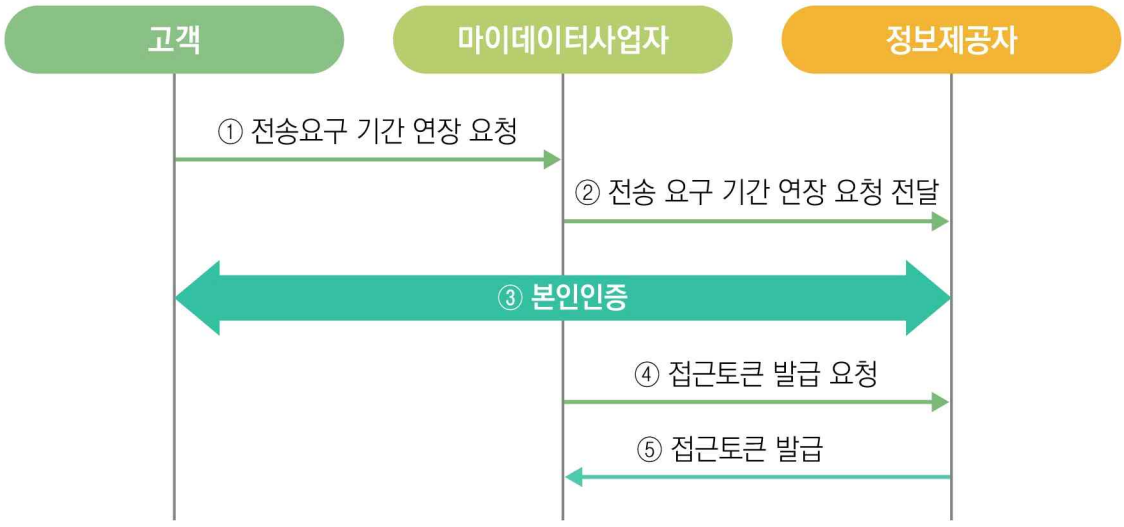
○ **(전송요구 기간 연장 요청)** 마이데이터사업자는 고객이 지정한 개인신용정보 전송요구 기간 만료 시점 1개월 전부터 고객에게 개인신용정보 전송요구 기간 연장을 요청할 수 있다.

- **(전송요구 기간 연장 절차)** 개인신용정보 전송요구 절차와 동일하며, 정보제공자는 본인인증 수행 후 마이데이터사업자에게 새로운 접근토큰을 발급하여 전송요구 기간을 연장한다.

* 통합인증을 이용하여 다수의 정보제공자에 대한 개인신용정보 전송 연장 요구 시, 최초 1개의 만료 시점에 일괄적으로 연장 요청 가능

- **(전송요구 기간 연장 화면)** 연장화면은 마이데이터사업자가 고객편의를 고려하여 자율적으로 그 방식으로 정할 수 있다.

〈 전송요구 기간 연장 〉



❶ **(전송요구 기간 연장 요청)** 고객은 전송요구 기간 만료시점이 도래한 개인신용정보 전송요구에 대해 마이데이터사업자를 통해 개인신용정보 전송 요구 기간 연장을 요청

❷ **(전송요구 기간 연장 요청 전달)** 마이데이터사업자는 고객의 개인신용정보 전송요구 기간 연장 요청을 정보제공자에게 전달

❸ **(본인인증)** 정보제공자는 본인인증 수단을 이용하여 고객의 개인신용정보 전송요구 기간 연장 요청에 대한 고객 본인인증을 수행

❹ **(접근토큰 신규 발급 요구)** 마이데이터사업자는 기간이 연장된 개인신용정보 전송 요청 권한을 획득하기 위해 정보제공자에 접근토큰 발급을 요청

❺ **(접근토큰 발급)** 고객이 전송요구한 개인신용정보 전송요구 권한을 포함하는 접근토큰을 생성하여 마이데이터사업자에게 발급하고 기발급된 접근토큰 폐기

※ ❶~❺ 과정은 인증방식(개별 또는 통합)에 따라 일부 절차가 변경될 수 있으며, 상세 절차는 「금융분야 마이데이터 표준API 규격」 참조

- **(전송요구 기간 만료)** 고객이 개인신용정보 전송요구 기간 연장에 응하지 않아 개인신용정보 전송요구 기간이 만료되었을 경우, 정보제공자는 기존의 접근토큰을 폐기한다. 이후 개인신용정보 전송이 중지되며 전송재개를 위해서는 3.3. 마이데이터 개인신용정보 전송 절차를 수행하혀야 한다.

마. 마이데이터 개인신용정보 전송 내역 관리

- **(전송 내역 기록)** 고객의 개인신용정보를 전송한 정보제공자·중계기관과 개인신용정보를 전송받은 마이데이터사업자·중계기관은 개인신용정보 송수신 내역에 대한 기록을 작성하고 보관하여야 한다.

- **(전송 내역 통지)** 고객의 개인신용정보를 전송받은 마이데이터사업자는 개인신용정보 송수신 내역에 대한 기록을 고객에게 연 1회 이상 통지하여야 한다.

  - **(전송 내역 통지 방법)** 마이데이터사업자는 마이데이터서비스, 이메일, 모바일 메신저 또는 SMS등을 통해 내역을 통지할 수 있다.

관련법령

- **신용정보법 시행령 제18조의6(본인신용정보관리회사의 행위규칙 등)** ⑩ 법 제22조의9제4항 및 제5항에 따라 개인신용정보를 전송한 신용정보제공·이용자등과 개인신용정보를 전송받은 중계기관 및 본인신용정보관리회사는 전송내역에 대한 기록을 작성하고 보관해야 하며, 본인신용정보관리회사는 전송받은 신용정보내역에 관한 기록을 신용정보주체에게 연 1회 이상 통지해야 한다.

PART.

04

마이데이터 본인인증

4 마이데이터 본인인증

본 장은 마이데이터를 위해 개인신용정보 전송요구 시 전송요구의 행위가 고객본인의 것인지를 확인하기 위한 본인인증의 기본원칙과 정보제공자가 자율적으로 제공하는 개별인증의 세부적인 절차, 별도의 인증기관이 공통으로 제공하는 통합인증을 절차를 중심으로 설명한다.

4.1. 마이데이터 본인인증 개요

가. 본인인증 기본 원칙

- **(본인인증 목적)** 정보제공자는 안전한 개인신용정보 전송을 위하여 고객이 개인신용정보 전송을 요구할 경우 해당 고객에 대해 반드시 본인인증을 수행하여야 한다.

관련법령

- **신용정보법 제33조의2(개인신용정보의 전송요구)** ⑧제1항에 따라 본인으로부터 개인신용정보의 전송요구를 받은 신용정보제공·이용자등은 신용정보주체의 본인 여부가 확인되지 아니하는 경우 등 대통령령으로 정하는 경우에는 전송요구를 거절하거나 전송을 정지·중단할 수 있다.

- **(본인인증 수행 주체)** 본인인증은 개인신용정보 전송요구의 정당성을 확인하기 위한 것으로 고객으로부터 개인신용정보 전송요구를 받은 정보제공자가 수행한다.

- **(인증 수단)** 정보제공자는 안전성 및 신뢰성이 확보된 인증 수단('나. 인증 수단' 참고)을 이용하여 고객 본인인증을 수행하여야 한다.

- **(인증 수단 관리)** 고객이 인증수단을 직접 소유하고 통제할 수 있어야 한다.

- **(사고시 책임소재)** 인증수단과 관련된 사고의 원인행위제공여부에 따라 책임지는 것을 원칙으로 한다.

예시 **사고 원인별 과실여부에 따른 책임 예시(인증서 방식 기준)**

① (고객과실) 인증서 비밀번호 타인 양도로 인한 문제발생 등

② (인증기관 과실) 인증서 발급과정에서 본인확인이 잘못된 경우, 인증서 유효성 검증 과정상의 오류로 인한 문제발생 등

③ (정보제공자) 전자서명 검증과정상의 오류로 인한 문제발생 등

- **(인증 보안)** 인증 정보의 입력, 전송, 보관, 관리 등 처리는 안전성 및 보안성이 확보된 정보처리시스템 및 단말, 네트워크 등을 통해 수행하여야 한다.

- **(인증 방식)** 고객이 본인인증을 수행하는 방식으로 개별인증방식과 통합인증방식이 있다.

  - **(개별 본인인증)** 고객이 개별 정보제공자가 제공 또는 인정하는 인증수단을 이용하여 각 정보제공자별로 개인신용정보 전송요구 및 인증을 수행하는 방식을 말한다.

  - **(통합 본인인증)** 고객이 통합 인증기관*이 발급한 인증수단을 이용하여 1회 인증만으로 다수의 정보제공자에 개인신용정보 전송요구 및 인증을 수행하는 방식을 말한다.

* (통합 인증기관) 고객에게 통합인증수단을 발급하고 정보제공자의 요청에 따라 통합인증수단 검증을 통해 공통의 고객 식별정보(CI정보)를 적법하게 제공 가능하며, 통합인증에 요구되는 충분한 보안수준을 갖춘 기관 중 별도의 절차에 따라 통합인증기관으로 참여한 기관

- **(인증 방식 제공)** 정보제공자 및 마이데이터사업자는 고객의 편리한 전송요구권 행사 및 인증방식 선택권을 고려하여, 인증수단을 제공하여야 한다. 이를 위해 통합인증은 기본으로 제공하되, 개별인증은 선택적으로 제공할 수 있다.

(참고) 본인인증 유형 비교

비교 기준	개별 본인인증	통합 본인인증
인증 수행 주체	정보제공자	정보제공자
인증 수단 제공자	정보제공자, 제3의 인증기관 등	통합 인증기관
인증 수단	다중 인증 등*(정보제공자별 상이) * '나. 인증 수단' 참고	다중요소 공개키 인증서(PKI) * CI 제공 필요
인증 횟수 (고객 관점)	전송요구 대상 정보제공자의 수만큼 반복적 인증 수행	전송요구 대상 정보제공자의 수와 무관하게 1회 수행

- **(인증 환경 제공)** 고객이 개인신용정보 전송요구에 따른 본인인증을 원활히 수행할 수 있도록 정보제공자, 마이데이터 사업자, 인증기관 등은 인증방식에 따라 적절한 인증 환경(인증화면, S/W 모듈 등)을 구성 및 제공하여야 한다.

  - **(개별 본인인증)** 정보제공자 및 인증기관 등은 고객 본인인증을 위한 화면 등의 환경*을 마이데이터서비스를 통해** 고객에게 제공하여야 한다.

  * 일반적으로 웹 화면 및 별도 앱 등의 형태로 제공되며, 이를 통해 인증수단 발급 및 인증정보 입력 화면 등을 제공하여야 함.

  ** 마이데이터서비스에서 인증화면을 직접 보여주거나, 인증화면을 호출

  - **(통합 본인인증)** 정보제공자, 인증기관, 마이데이터사업자 등은 관련 규격에 따라 각 기관의 역할 수행에 필요한 인증환경을 직접 구성 및 제공하여야 한다.

나. 본인인증 수단

○ 정보제공자는 다중인증, 다중요소 공개키인증서, 비대면 실명확인 방식 등과 같이 신뢰성 및 안전성이 확보된 인증수단을 사용하여 고객 본인인증을 수행하여야 한다.

주요 인증 규격(가이드라인) 참고 사례

- 미국, 유럽, 국제표준기구 등의 주요 인증 규격(가이드라인)은 계좌정보 등 민감한 개인정보에 접근하거나, 개인정보 유출 위험이 높은 경우 다중인증 이상의 보안 수준을 갖춘 인증 수단을 적용하도록 권고

  ※ (참고 3) 주요 인증 규격(가이드라인)의 인증 수준 요구 현황

– **(다중 인증)** 지식, 소유, 특징 기반 인증수단 중 소유 기반 인증수단을 포함하여 2가지 이상의 인증수단을 동시에 적용*하되, 각 인증정보는 서로 분리된 환경에서 생성 및 전송되는 방식이어야 한다.

* (예시) ID/PW 인증(지식 기반) + SMS 인증(소유 기반)

예시 **인증 요소별 인증수단 예시**

- **(지식 기반)** ID/PW, 문답식인증, PIN 번호, 패턴 인증 등
- **(소유 기반)** OTP(One Time Password), 휴대폰 SMS 인증(자체 SMS 인증, 휴대폰 본인확인 등), 공개키 인증서, ARS 인증(신용카드 본인확인 등), 계좌 인증 등
- **(특징 기반)** 생체인증(지문, 홍채, 안면, 정맥 등), 서명 패턴 등

– **(다중요소 공개키인증서)** 안전하게 생성·보호*된 개인키 및 공개키 인증서로서, 인증요구를 위한 전자서명을 생성하기 위해 개인키 인증정보(비밀번호, 생체정보 등)를 요구하는 방식**을 말한다.

* H/W 및 S/W 기반 안전한 보호기술(SE, TZ, White Box 등) 적용 권고

** (예시) 정보제공자 자체 발급 인증서, 신뢰할 수 있는 제3의 기관이 발급 인증서 등 안전성이 확보된 인증서를 이용.

- **(비대면 실명확인 방식 활용)** 비대면 실명확인 방식(①~⑦) 중 2가지 이상을 중첩 확인하는 방식을 말한다.

비대면 실명확인 방식

① 실명확인증표 사본 제출, ② 영상통화, ③ 접근매체 전달과정에서 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 방법(생체인증 등), ⑥ 타 기관 확인결과 활용, ⑦ 다수의 고객정보 검증

※ (참고4) 비대면 실명확인 방식

다. 본인인증 절차

○ 고객 본인인증은 '① 인증수단 발급', '② 인증 환경 제공', '③ 인증 확인·검증', '④ 본인인증 확인' 순으로 진행된다.

① **(인증수단 발급)** 고객은 인증수단을 정보제공자, 또는 인증기관을 통해 발급받아 등록한다.

①-가. **(개별인증 발급 절차)** 통상 고객은 정보제공자 회원가입 시에 정보제공자, 또는 제3의 인증기관으로부터 인증수단을 발급받아 등록한다.

* 세부 절차 등은 각 정보제공자가 전송요구 편의성, 안전성등을 해치지 않는 범위에서 자율적으로 정할수 있다.

①-나. **(통합인증 발급 절차)** 고객이 기존에 발급받은 유효한 인증서를 보유하지 않은 경우, 일반적으로 마이데이터서비스를 최초 이용하는 과정에서 통합 인증기관을 통해 인증수단을 발급한다.*

* 통합인증은 별도의 인증서 등록절차(예: 타행인증서 등록) 불필요

② **(본인인증 환경 제공)** 정보제공자, 마이데이터사업자, 제3의 인증기관은 고객에게 본인인증을 수행할 수 있는 환경(화면 등)을 제공한다.

②-가. **(개별인증 환경 제공)** 정보제공자가 앱 또는 웹화면의 형태로 제공한다.

②-나. **(통합인증 환경 제공)** 마이데이터사업자 등이 앱 또는 웹화면의 형태로 제공한다

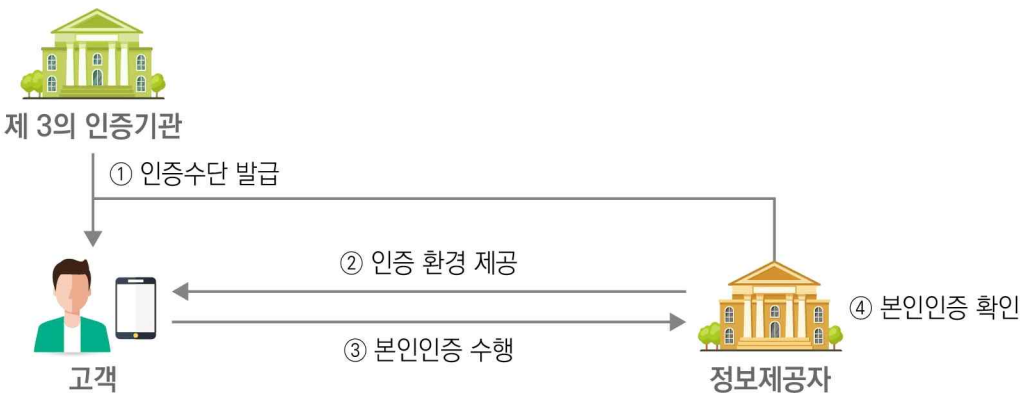
③ **(본인인증 수행)** 고객은 개인신용정보 전송요구를 위해 인증기관 또는 정보제공자가 제공하는 인증수단을 이용해 본인인증을 수행한 결과를 정보제공자에게 전달한다.

③-가. **(개별인증 수행 절차)** 마이데이터서비스를 통해 제공되는 정보제공자의 인증 환경을 통해 인증수단을 입력 및 제출한다.

③-나. **(통합인증 수행 절차)** 마이데이터사업자 등이 제공하는 인증 환경을 통해 인증수단을 선택 및 입력하여 제출한다.

④ **(본인인증 확인)** 정보제공자는 고객의 인증 요구에 대한 확인 및 검증을 통해 고객의 정보주체 본인 여부를 확인한다.

〈 본인인증 절차 〉



4.2. 개별인증

- **(개별인증)** 고객은 정보제공자가 개별적으로 제공하는 인증수단 및 환경을 이용하여 개별인증을 수행한다.

  - **(개별 인증수단)** 정보제공자는 인증 신뢰성과 고객의 인증 편의성을 고려하여 본 가이드라인('나. 인증 수단')을 참고하여 각사가 자율적으로 개별 인증수단을 제공할 수 있다.

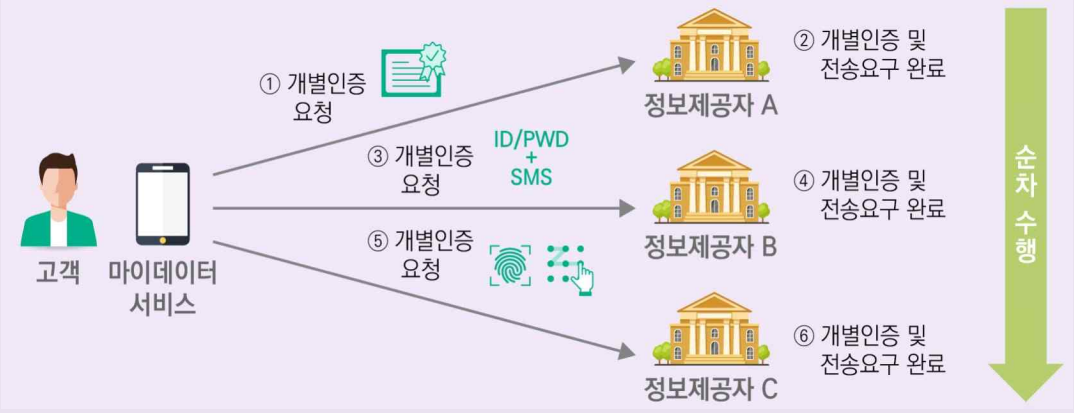
  * 개별인증의 특성에 따라 다수 정보제공자가 동일한 인증수단(예: 공동인증서 등)을 요구하는 경우에도 고객은 각 정보제공자별로 순차적으로 인증을 수행

  - **(개별인증 인터페이스)** 정보제공자는 제공 인증수단의 특성 및 인증 절차상의 정보보호 수준등을 고려하여 개별인증 환경*을 제공하여야 한다.

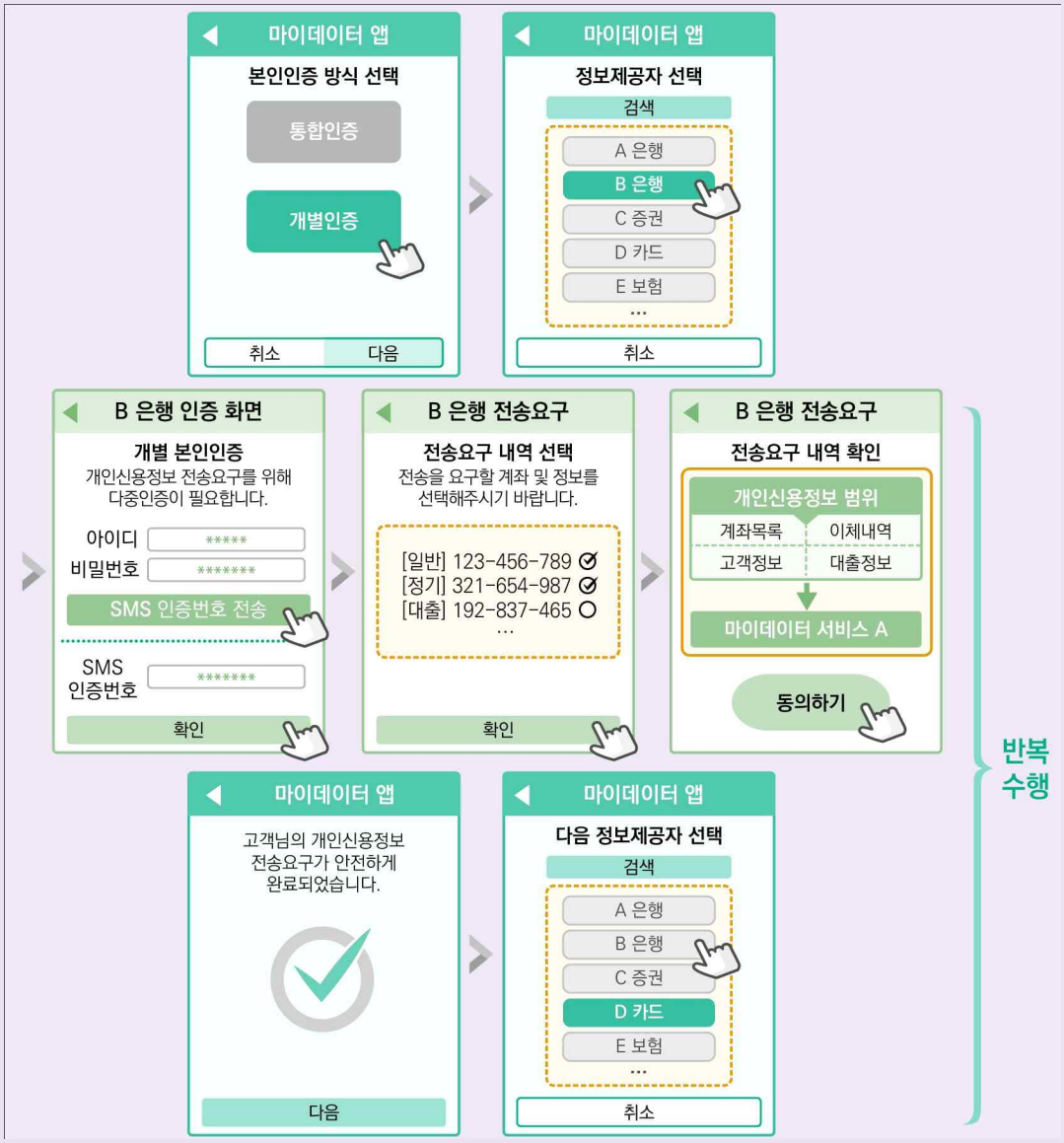
  * 인증 인터페이스의 유형(웹 화면, 별도 앱 등)은 각사가 자율적으로 결정할수 있으며, 반드시 인터페이스 호출을 위한 표준 API를 제공하여야 한다.(「금융분야 마이데이터 표준 API 규격」 참조).

예시 **개별 본인인증 절차 개요**

- 각 정보제공자는 각자의 인증수단을 통해 개별적으로 고객을 인증
- 고객은 마이데이터서비스 이용 시 각 정보제공자별로 본인인증을 수행



예시 개별 본인인증 절차(고객 관점)



※ 본 그림은 예시이며, 정보제공자 선택 및 개별인증 수행화면은 본 가이드라인에 따라 마이데이터 사업자 및 정보제공자가 자율적으로 구성 가능

※ 개별인증 API관련 세부 절차 및 기술 규격은 「금융분야 마이데이터 표준 API 규격」 참고

4.3. 통합인증

○ **(통합 본인인증)** 고객은 통합 인증기관이 제공하는 인증수단(통합인증수단)을 이용하여 1회 인증으로 다수의 정보제공자에게 일괄적으로 인증을 수행하게 된다.

- **(통합인증수단)** 통합 인증기관은 모든 정보제공자가 공통적으로 고객을 인증할 수 있도록, 인증결과로서 CI정보*를 제공할 수 있는 다중요소 공개키인증서를 고객에게 발급한다.

* '본인확인기관 지정 등에 관한 고시(방통위 고시)'의 '연계정보'

- **(통합인증 환경)** 마이데이터사업자는 고객이 통합인증수단을 이용하여 안전하게 인증을 요구(전자서명 생성 및 전송)할 수 있도록 인증수단의 선택* 및 입력 화면 등 일체를 자율적으로 구성 및 제공할 수 있으며, 정보제공자 및 통합 인증기관은 인증수단 전송 및 검증 등을 위한 인터페이스**를 제공한다.

* 인증수단 선택화면은 향후에 필요한 경우 표준창 형태로 제공 가능

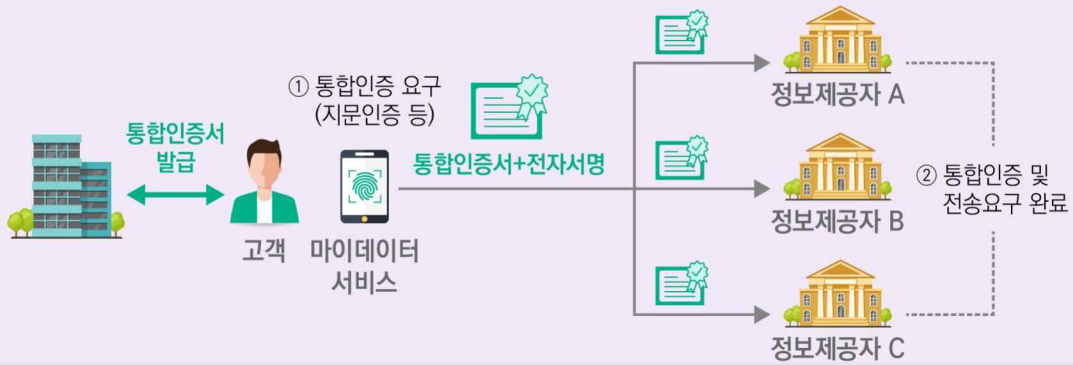
** 정보제공자는 마이데이터사업자가 인증수단을 전송할 수 있도록, 인증기관은 정보제공자가 인증수단의 검증·확인 등을 요청할 수 있도록, 통합인증을 위한 표준 API를 제공하여야 한다.(「금융분야 마이데이터 표준 API 규격」 참조).

통합인증 환경 제공시 고려사항

- **(인증수단 선택권 보장)** 마이데이터사업자는 고객의 통합인증수단 선택권을 보장하기 위하여 고객이 통합인증수단을 선택 가능하도록 인증수단 선택 화면 등을 구성해야만 하며, 고객에게 제공하고자 하는 통합인증 수단의 선정은 마이데이터사업자 자율로 한다. 단, 공동인증서는 기본제공하되 그 외 인증서는 최소 1개 이상 적용한다. (단, 마이데이터사업자의 자체인증서 제외)
- **(인증정보 보호)** 마이데이터사업자는 인증정보(인증서 비밀번호 등)이 유출되지 않도록 보안 키패드, 앱 위변조 탐지, 백신 등 필요한 보호 대책 적용하여야 한다.

예시 통합 본인인증 절차 개요

- 고객은 마이데이터서비스 이용 시 1회 인증으로 동시에 다수의 정보제공자에게 인증 수행
- 각 정보제공자는 통합인증수단을 통해 개별적으로 고객을 인증



(참고) 통합 본인인증 참여기관별 역할

구 분	역 할
마이데이터사업자	인증수단 및 전송요구내역 선택화면 구성·제공, 전자서명 생성 및 전송 등
정보제공자	전자서명 검증 및 고객 인증 등
통합 인증기관	인증수단 발급, 인증서 검증 등

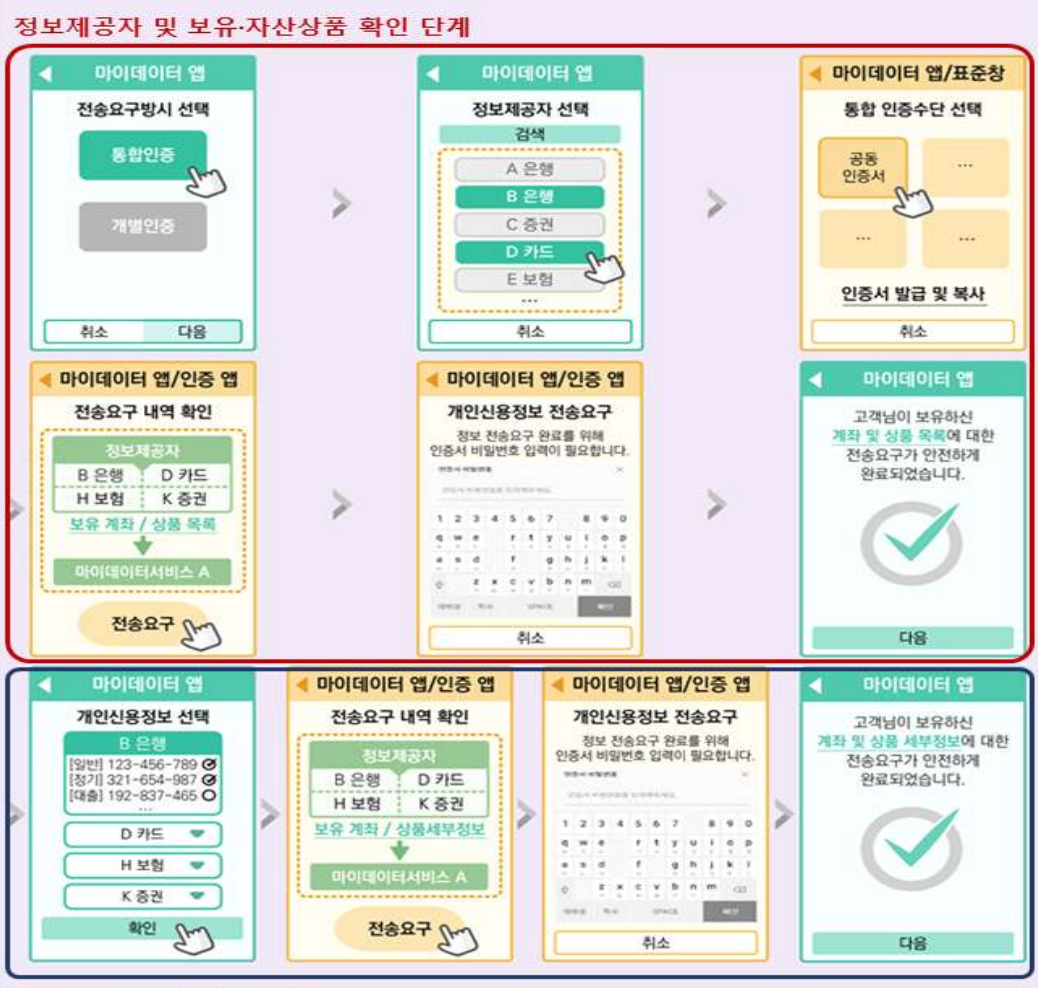
○ **(통합 본인인증 절차)** 통합 본인인증은 고객이 가입한 정보제공자 및 보유자산·상품을 확인하는 단계와 자산·상품단위별 전송요구를 하는 단계로 구성된다.

- **(보유자산·상품 확인 단계 생략)** 마이데이터 사업자가 보유자산·상품 정보를 사전에 보유하고 있는 경우(기수집된 정보 등) 보유자산·상품 확인 단계를 생략하고 자산·상품단위별 전송요구를 수행하여도 된다.

- **(자산·상품 전송 요구 시 개수 제한)** 전송요구대상 자산·상품의 수가 상당히 많은 일부 고객은 전송요구시 자산·상품 개수의 선택이 제한될 수 있으며(최대 7천바이트로 계좌 기준 약 200개), 제한을 넘게될 경우 개별선택없이 전체 자산·상품 선택으로 대체

※ 통합인증 세부 절차 및 기술 규격은 「금융분야 마이데이터 통합인증 절차 및 규격」을 참고

예시 **통합 본인인증 절차(고객 관점)**



※ 본 그림은 예시이며, 정보제공자 선택 및 개별인증 수행화면은 본 가이드라인에 따라 마이데이터 사업자가 자율적으로 구성 가능(향후, 필요시 표준창 형태의 인증수단 선택화면 제공 가능)

정보제공자 선택 화면 구성시 고려사항

- **(1회 전송요구시 일괄 선택가능한 정보제공자 수 제한)** 마이데이터사업자가 고객에게 정보제공자 일괄선택 기능을 제공하는 경우 일괄선택 할 수 있는 정보제공자 선택은 기관코드 기준으로 50개를 초과할 수 없다.(한 금융회사가 여러 개의 기관코드를 보유한 경우 각각의 기관코드별로 하나의 정보제공자로 봄). 여러번에 나누어 일괄선택 기능을 제공하는 경우에도 일괄선택 기능으로 선택하는 정보제공자는 합하여 50개를 초과할 수 없다. 단, 고객은 마이데이터 사업자가 자율 구성한 정보제공자에 대해 개별적으로 추가·수정 선택할 수 있어야 하며, 고객이 각 정보제공자를 개별적으로 추가 선택한 경우에는 50개 초과가 가능하다.

4.4. 중계기관을 통한 본인인증

- 정보제공자가 중계기관을 통해 고객에게 개인신용정보를 전송하는 경우, 원칙적으로 개별인증은 각 정보제공자가, 통합인증은 중계기관이 수행한다.

  - **(개별인증)** 고객이 개별인증을 통해 본인인증을 수행할 경우, 각 정보제공자가 고객 인증을 직접 수행하며 불가피한 상황으로 인해 개별인증을 제공하지 못하는 경우 중계기관이 제공하는 통합인증으로 대체할 수 있다.

※ 관련된 세부절차는 중계기관(공공마이데이터의 경우 한국신용정보원)이 별도로 정하는 바를 따른다.

  - **(통합인증)** 고객이 통합인증을 통해 본인인증을 수행할 경우, 중계기관은 고객이 인증수행 결과를 이용하여 본인인증을 수행하고, 본인인증이 완료되면 각 정보제공자는 중계기관을 통해 개인신용정보를 전송한다.

PART.

05

마이데이터 보안

5 마이데이터 보안

본 장은 마이데이터서비스 제공과 관련하여 안전한 개인신용정보 전송, 저장 등의 처리를 위해 신용정보법령등에서 요구하는 보안요구사항등을 설명한다.

5.1. 마이데이터 보안 개요

가. 목 적

○ 고객의 개인신용정보를 보유수집하는 정보제공자, 정보수신자는 안전한 개인신용정보 보호를 위해 본 가이드라인의 보안 준수사항을 참고하여 관리·운영 등에 적용하여야 한다.

나. 관련법규 및 규정

○ 정보제공자 및 정보수신자는 개인신용정보 전송 및 마이데이터서비스 제공에 있어 신용정보법령 및 신용정보업 감독규정의 정보보호 조항을 준수하여야 한다.

관련법령

- **신용정보법 제19조(신용정보전산시스템의 안전보호)** ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.

- **신용정보법 시행령 제6조(허가의 세부요건 등)** ① 법 제6조제1항 및 제3항에 따라 신용정보업, 본인신용정보관리업 또는 채권추심업의 허가를 받으려는 자가 갖추어야 할 인력 및 물적 시설의 세부요건은 다음 각 호의 구분에 따른다.

  1.~4. (생략)

  5. 본인신용정보관리업을 하는 경우: 제2항제2호에 따른 설비를 갖출 것

  ② 제1항 각 호(제4호는 제외한다)에 따른 상시고용인력 및 설비는 다음 각 호의 구분에 따른다.

  1. (생략)

  2. 설비: 신용정보 등의 처리를 적정하게 수행할 수 있다고 금융위원회가 정하여 고시하는 정보처리·정보통신 설비

- **신용정보업 감독규정 제6조(정보처리·정보통신설비)** 영 제6조제2항제2호에서 "금융위원회가 정하여 고시하는 정보처리·정보통신 설비"란 해당 신용정보업, 본인신용정보관리업 또는 채권추심업의 범위와 규모에 비추어 신용정보를 원활히 처리할 수 있는 수준의 정보처리·정보통신 설비로서 별표 2에 규정된 사항을 말한다.

- 마이데이터사업자 허가 시 망분리 기준 및 클라우드컴퓨팅서비스 이용등은 전자금융감독규정을 따른다.

관련법령

- **전자금융감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등)** ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

  1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가

  2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가

  3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

  ② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

  ③~⑦ (생략)

⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

⑨ (생략)

- **전자금융감독규정 제15조(해킹 등 방지대책)** ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1.~2. (생략)

3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)

4. (생략)

5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.) 〈신설 2013. 12. 3., 개정 2015. 2. 3.〉

②~ ⑥ (생략)

- 개인신용정보의 보호는 특별법인 신용정보법을 우선 적용하고 신용정보법에 규정되지 않은 사항은 일반법인 개인정보보호법을 적용하여야 한다.

※ 개인신용정보를 제외한 개인정보는 개인정보보호법을 적용한다.

5.2. 관리적 보안사항

가 . 신용정보관리·보호인

○ **(신용정보관리·보호인 지정)** 정보제공자와 정보수신자는 개인신용정보 보호 계획 수립·시행 등의 업무 수행을 위해 신용정보의 관리·보호 등을 총괄하는 지위에 있는 사람을 신용정보관리·보호인*으로 지정하여야 한다.

* 개인정보보호법상 개인정보보호 책임자 겸임 가능

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ③ 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 제4항에 따른 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자는 신용정보관리·보호인을 임원(신용정보의 관리·보호 등을 총괄하는 지위에 있는 사람으로서 대통령령으로 정하는 사람을 포함한다)으로 하여야 한다.

신용정보관리·보호인의 자격

1. 사내이사
2. 집행임원(「상법」 제408조의2에 따라 집행임원을 둔 경우로 한정)
3. 신용정보의 제공·활용·보호 및 관리 등에 관한 업무집행 권한이 있는 사람(「상법」 제401조의2 제1항제3호에 해당하는 자)
4. 그 밖에 신용정보의 제공·활용·보호 및 관리 등을 총괄하는 위치에 있는 직원

– **(마이데이터사업자의 신용정보관리·보호인)** 마이데이터사업자는 신용정보관리·보호인을 임원 또는 집행임원, 신용정보의 제공·활용·보호 및 관리 등에 관한 업무 집행 권한이 있는 사람으로 지정하여야 한다.

- **(신용정보관리·보호인의 주업무)** 신용정보관리·보호인은 개인신용정보 보호 계획 수립·시행 등의 업무를 수행한다.

신용정보관리·보호인의 주업무

1. 개인신용정보 보호 계획의 수립 및 시행
2. 개인신용정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인신용정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인신용정보 누설 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인신용정보 보호 교육 계획의 수립 및 시행
6. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검

- **(개인신용정보 관리 및 보호 실태 점검)** 신용정보관리·보호인은 신용정보관리·보호인의 주업무에 대하여 점검을 실시하고 보고하여야 한다.

개인신용정보 관리 및 보호 실태 점검

- **(점검 내용)**
  ① 신용정보관리·보호인의 주업무를 수행한 실적
  ② ①의 실적을 기재한 보고서를 대표이사 및 이사회에 보고한 실적
- **(점검 주기)** 연 1회 이상
- **(제출기한)** 매 사업연도 종료 후 3개월 이내
- **(제출처)** 금융위원회

☞ 신용정보관리·보호인 지정은 개인정보보호법상 개인정보보호 책임자와 겸임이 가능하며, 개인신용정보 보호 교육은 개인정보보호법상 개인정보보호 교육으로 갈음할 수 있다.

나. 개인신용정보 보호 교육

○ **(개인신용정보보호 교육)** 신용정보관리·보호인은 개인신용정보의 적정한 취급을 위하여 개인신용정보 보호 교육을 계획하고 수립하여 개인신용정보취급자에게 정기적인 교육*을 실시하여야 한다.

* 개인정보보호법상 개인정보보호 교육으로 갈음할 수 있다.

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ④ 제3항에 따른 신용정보관리·보호인은 다음 각 호의 업무를 수행한다.

  2. 기업신용정보의 경우 다음 각 목의 업무

     마. 임직원 및 전속 모집인 등에 대한 신용정보보호 교육계획의 수립 및 시행

- **(개인신용정보보호 교육 계획 수립)** 교육 계획에는 교육 목적, 대상, 내용(프로그램 등 포함), 일정 및 방법 등을 포함하여 내부 관리계획 등에 규정하거나 별도의 교육 계획으로 수립한다.

- **(개인신용정보보호 교육 시행)** 조직 여건 및 환경에 따라 사내교육, 외부교육, 위탁교육, 온라인교육 등 다양한 방법으로 개인신용정보 보호 교육을 시행할 수 있다.

예시 **개인신용정보 보호 교육 예시**

- 개인신용정보 보호의 중요성
- 내부 관리계획의 제·개정에 따른 준수 및 이행
- 위험 및 대책이 포함된 조직 보안 정책, 보안지침, 지시 사항, 위험관리 전략
- 개인신용정보처리시스템의 안전한 운영·사용법(하드웨어, 소프트웨어 등)

- 개인신용정보 안전성 확보조치 기준
- 개인신용정보 보호업무의 절차, 책임, 방법
- 개인신용정보 처리 절차별 준수사항 및 금지사항
- 개인신용정보 누설·노출 및 침해신고 등에 따른 사실 확인 및 보고, 피해구제 절차 등

다. 개인신용정보 관리

○ **(신용정보 활용체제 공시)** 정보제공자는 신용정보활용체제를 작성하고 고객에게 공시하여야 한다.

관련법령

- **신용정보법 제31조(신용정보활용체제의 공시)** ① 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.

신용정보 활용체제 포함 사항

- 개인신용정보 보호 및 관리에 관한 기본계획(총자산, 종업원 수 등을 고려하여 대통령령으로 정하는 자로 한정한다)
- 관리하는 신용정보의 종류 및 이용 목적
- 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적
- 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법
- 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자
- 신용정보주체의 권리와 그 행사 방법
- 신용정보관리·보호인 또는 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처

- **(공시 방법)** 고객이 신용정보활용체제를 열람할 수 있도록 점포사무소 안의 보기 쉬운 장소에 갖추어두거나 인터넷 홈페이지를 통해 게시하여야 한다.

- **(개인신용정보 수집)** 개인신용정보 수집 시 신용정보법 또는 정관으로 정한 업무 범위에서 신용정보를 수집하고 처리목적을 명확화한다.

관련법령

- **신용정보법 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)** ①신용정보회사등은 신용정보의 수집·처리·이용 및 보호 등에 대하여 금융위원회가 정하는 신용정보 관리기준을 준수하여야 한다.

  ② 신용정보회사등은 다음 각 호의 구분에 따라 개인신용정보의 처리에 대한 기록을 3년간 보존하여야 한다.

  1~4.(생략)

- **(개인신용정보 처리 기록 보존)** 정보제공자와 정보수신자는 개인신용정보 처리에 대한 기록을 처리 구분(수집·이용, 제공, 폐기 등)에 따라 분류하여 기록이 발생한 날로부터 3년간 보존하여야 한다.

〈 개인신용정보 처리 방법에 따른 구분 〉

구분	항목
1. 개인신용정보를 수집·이용한 경우	가. 수집·이용한 날짜 나. 수집·이용한 정보의 항목 다. 수집·이용한 사유와 근거
2. 개인신용정보를 제공하거나 제공받은 경우	가. 제공하거나 제공받은 날짜 나. 제공하거나 제공받은 정보의 항목 다. 제공하거나 제공받은 사유와 근거
3. 개인신용정보를 폐기한 경우	가. 폐기한 날짜 나. 폐기한 정보의 항목 다. 폐기한 사유와 근거
4. 그 밖에 대통령령으로 정하는 사항	-

- **(개인신용정보 보관)** 정보제공자와 정보수신자는 금융거래 등 상거래 관계가 종료된 날부터 해당 고객의 개인신용정보가 안전하게 보호될 수 있도록 관리하여야 한다.

상거래 관계가 종료된 개인신용정보의 관리 방법

- 금융거래 등 상거래관계의 설정 및 유지 등에 필수적인 개인신용정보의 경우
  1. 상거래관계가 종료되지 아니한 다른 신용정보주체의 정보와 별도로 분리
  2. 접근권한 관리책임자를 두어 해당 개인신용정보에 접근할 수 있는 사람을 지정
  3. 접근권한을 부여받은 자가 해당 개인신용정보를 이용하려는 경우에는 접근권한 관리책임자의 사전 승인을 얻어 그 개인신용정보를 이용하게 하고, 그 이용내역을 3년간 보관
- 금융거래등 상거래 관계의 설정 및 유지 등에 필수적이지 않은 개인신용정보의 경우
  1. 해당 정보 모두 삭제

- **(개인신용정보 삭제)** 정보제공자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 고객의 개인신용정보를 관리대상에서 삭제하여야 한다. 마이데이터사업자는 고객의 개인신용정보 삭제 요청 시 또는 회원탈퇴 시 해당 고객의 개인신용정보를 관리대상에서 삭제하여야 한다.

관련법령

- **신용정보법 제38조의3(개인신용정보의 삭제 요구)** ① 신용정보주체는 금융거래 등 상거래 관계가 종료되고 대통령령으로 정하는 기간이 경과한 경우 신용정보제공·이용자에게 본인의 개인신용정보의 삭제를 요구할 수 있다. 다만, 제20조의2제2항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

- **(개인신용정보 삭제 방법)** 개인신용정보 삭제 시, 보존매체의 특성을 고려하여 복구 또는 재생되지 아니하도록 하여야 한다.

〈 보존매체 특성에 따른 개인신용정보 삭제 방법 〉

보존매체 구분	삭제 방법
전자적 파일	현재 기술 수준에서 적절한 비용이 소요되는 방법으로서 복원이 불가능하도록 영구 삭제
인쇄물, 서면, 그 밖의 기록매체	파쇄 또는 소각

- **(개인신용정보를 삭제 할 수 없는 경우)** 현재 거래 중인 고객의 개인신용정보와 분리하는 등의 조치를 통해 안전하게 보관하고 해당 개인신용정보 활용 시 고객에게 통지하여야 한다.

개인신용정보를 관리대상에서 삭제하지 않는 경우

- 신용정보법 또는 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우
- 개인의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우
- 가명정보를 이용하는 경우로서 그 이용 목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존하는 경우
- 예금·보험금의 지급을 위한 경우
- 보험사기자의 재가입 방지를 위한 경우
- 개인신용정보를 처리하는 기술의 특성 등으로 개인신용정보를 보존할 필요가 있는 경우

라. 개인신용정보처리 시스템 접근 관리

- **(내부 접근권한 관리)** 정보제공자와 정보수신자는 서비스 제공을 위하여 필요한 최소한의 인원에게만 개인신용정보를 처리할 수 있도록 개인신용정보처리시스템에 대한 접근권한 관리하여야 한다.

- **(내부 접근권한 부여)** 서비스 제공을 위하여 필요한 최소한의 인원에게만 개인신용정보 접근 권한을 직급별·업무별로 차등하여 부여하여야 한다.

- **(내부 접근권한 변경)** 정보제공자와 정보수신자의 지휘·감독을 받아 개인신용정보 업무를 처리하는 개인신용정보 취급자가 전보 또는 퇴직 등 인사이동으로 인하여 변경되었을 경우, 지체없이 개인신용정보처리시스템의 접근권한을 변경 또는 말소하여야 한다.

- **(내부 접근권한 변경 기록)** 내부 접근권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

- **(외부 접근권한 관리)** 업무목적을 위하여 불가피한 경우 외부사용자에게 개인신용정보처리 시스템에 대해 최소한의 접근 권한을 부여하고, 권한 부여에 관한 기록을 3년 이상 보관하는 적절한 통제시스템을 마련하여야 한다.

- **(외부 접속 보안)** 외부에서 개인신용정보처리시스템 접속 시 안전한 접속수단 또는 안전한 인증수단(VPN 등)을 적용하여야 한다.

- **(접속기록 관리)** 개인신용정보처리 시스템에 접속하여 개인신용정보를 처리한 경우 처리일시, 처리내역 등 접속 내역을 기록하여야 한다.

  - **(접속기록 확인·감독)** 저장된 접속기록을 월 1회 이상 정기적으로 확인·감독한다.

  - **(접속기록 백업)** 개인신용정보처리 시스템의 접속기록을 1년 이상 저장하고, 위변조되지 않도록 별도 저장장치에 백업 보관한다.

- **(비밀유지서약서 징구)** 정보제공자와 정보수신자는 개인신용정보처리 시스템 등에 접근하는 내·외부직원을 대상으로 정보보호비밀유지서약서를 징구하여야 한다.

  - **(작성 방법)** 정보보호에 대한 책임 및 준수사항을 포함하는 서류를 임직원 및 외부자의 서명과 함께 작성한다.

마. 직무분리

- **(직무분리 기준 마련)** 권한 오남용 등 고의적인 행위로 발생할 수 있는 잠재적인 피해를 줄이기 위하여 직무분리 기준을 마련한다.

  - **(직무분리 기준 수립)** 직무별 권한과 책임을 분산시켜 직무 간 상호견제를 할 수 있도록 직무별 역할과 책임을 명확하게 기술한다.

- **(직무분리 보완책 마련)** 인적자원 부족 등 불가피하게 직무분리가 어려운 경우 직무자간 상호 검토 등 별도의 보완책을 마련한다.

바. API 시스템 관리

- **(자격증명·접근토큰 관리)** 정보제공자와 마이데이터사업자는 자격증명 및 접근토큰을 안전하게 관리하고 위변조를 방지하기 위한 수단을 마련하여야 한다.

  - **(중복토큰 발급 확인)** 정보제공자는 접근토큰과 리프레시토큰 중복발급 방지를 포함하여 토큰이 안전하게 관리될 수 있는 수단을 마련하고 이를 주기적으로 확인하여야 하며, 마이데이터사업자는 정보제공자로부터 수신한 토큰의 중복발급 여부를 확인하고, 중복발급을 확인한 즉시 전송요청를 중지하여야 한다.

- **(중복토큰 발급 사실 확인 시 조치)** 정보제공자 및 마이데이터사업자는 중복토큰 발급 사실 확인시, 오전송되는 개인신용정보가 없도록 상호 협조하여야 한다.

- **(API 관련 시스템 보호)** 정보제공자는 API와 관련된 시스템에 방화벽, 침입탐지·차단 시스템, 망분리, 백신 소프트웨어 등 외부 공격 시도에 대한 방어 장치를 마련하여야 한다.

- **(비정상 API 탐지)** 정보제공자는 비정상적인 API 접근을 모니터링하고 필요 시 API의 접근 제한 등을 수행할수 있어야 한다.

- **(클라우드 이용)** 마이데이터사업자는 클라우드 이용시 전자금융감독규정 등 관련 법규에서 요구하는 사항을 만족하여야 한다.

관련법령

- **전자금융감독규정 제14조의2(클라우드컴퓨팅서비스 이용절차 등)** ① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.
  1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
  2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
  3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

  ② 금융회사 또는 전자금융업자는 제1항에 따른 평가결과 및 자체 업무 위수탁 운영기준에 대하여 제8조의2에 따른 정보보호위원회의 심의·의결을 거쳐야 한다.

  ③~⑦ (생략)

  ⑧ 제2항의 절차를 거친 클라우드컴퓨팅서비스 제공자의 정보처리시스템이 위치한 전산실에 대해서는 제11조제11호 및 제12호, 제15조제1항제5호를 적용하지 아니한다. 다만, 금융회사 또는 전자금융업자(전자금융거래의 안전성 및 신뢰성에 중대한 영향을 미치지 않는 외국금융회사의 국내지점, 제50조의2에 따른 국외 사이버몰을 위한 전자지급결제대행업자는 제외한다)가 제3항제1호에 따른 고유식별정보 또는 개인신용정보를 클라우드컴퓨팅서비스를 통하여 처리하는 경우에는 제11조제12호를 적용하고, 해당 정보처리시스템을 국내에 설치하여야 한다.

  ⑨ (생략)

사. 이용자 보호

○ **(개인신용정보 누설)** 정보제공자는 개인신용정보가 업무 목적 외로 누설되었음을 알게 되었을 시, 서면, 전화, 전자우편, 휴대전화 문자메시지(SMS) 등을 통해 지체없이 해당 고객에게 통지하여야 한다.

개인신용정보 누설의 예

- 신용정보회사등이 개인신용정보에 대하여 통제를 상실하거나 권한 없는 자의 접근을 허용한 경우로서 아래의 예시 및 이와 유사한 경우 등에는 개인신용정보 누설로 볼 수 있음

1. 개인신용정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인신용정보가 저장된 데이터베이스 또는 개인신용정보처리시스템에 권한 없는 자가 접근한 경우
3. 신용정보회사등의 고의 또는 과실로 개인신용정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한이 없는 자에게 잘못 전달된 경우

※ 출처 : 신용정보업감독규정 [별표 4-2] 신용정보 관리기준

관련법령

- **신용정보법 제39조의4(개인신용정보 누설통지 등)** ① 신용정보회사등은 개인신용정보가 업무 목적 외로 누설되었음을 알게 된 때에는 지체 없이 해당 신용정보주체에게 통지하여야 한다. 이 경우 통지하여야 할 사항은 「개인정보 보호법」 제34조제1항 각 호의 사항을 준용한다.

개인신용정보 누설 시 통지 사항

- 누설된 개인신용정보의 항목
- 누설 시점과 그 경위
- 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 신용정보회사등의 대응조치 및 피해 구제절차
- 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

- 개인신용정보가 누설된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

○ **(1만명 이상의 개인신용정보 누설)** 1만명 이상의 고객에 관한 개인신용정보가 누설되었을 경우, 신용정보주체 통지와 더불어 추가적인 방법으로 신용정보 누설을 알려야한다.

1만명 이상의 개인신용정보 누설시 통지 사항

- 누설된 개인신용정보의 항목
- 누설 시점과 그 경위
- 누설로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
- 신용정보회사등의 대응조치 및 피해 구제절차
- 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

1만명 이상의 개인신용정보 누설시 통지 방법

1. 15일간 인터넷 홈페이지에 그 사실을 게시
2. 15일간 사무실이나 점포 등 해당 신용정보주체로 하여금 그 사실을 열람토록 조치
3. 7일간 주된 사무소가 있는 특별시·광역시·특별자치시·도 또는 특별자치도 이상의 지역을 보급지역으로 하는 일반일간신문, 일반주간신문 또는 인터넷 신문에 그 사실을 게재

- **(신고서 제출)** 1만명 이상의 고객에 관한 개인신용정보가 누설된 경우, 지체없이 금융위원회 또는 금융감독원에 “개인신용정보 누설신고서”(신용정보업감독규정 별지 제18호 서식)를 제출하여 신고하여야 한다.

  - 단, 신용정보 추가누설을 방지하기 위한 조치가 시급한 경우 해당 조치를 취한 후 지체없이 조치의 내용과 함께 신고서를 제출할 수 있다.

관련법령

- **신용정보법 제39조의4(개인신용정보 누설통지 등)** ③ 신용정보회사등은 대통령령으로 정하는 규모 이상의 개인신용정보가 누설된 경우 제1항에 따른 통지 및 제2항에 따른 조치결과를 지체 없이 금융위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 "금융위원회등"이라 한다)에 신고하여야 한다. 이 경우 금융위원회등은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

- **신용정보법 시행령 제34조의4(개인신용정보의 누설사실의 통지 등)** ④ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 규모 이상의 개인신용정보"란 1만명 이상의 신용정보주체에 관한 개인신용정보를 말한다.

  ⑤ 법 제39조의4제3항 전단에서 "대통령령으로 정하는 기관"이란 금융감독원을 말한다.

  ⑥ 법 제39조의4제3항 전단에 따라 신고해야 하는 신용정보회사등(상거래 기업 및 법인은 제외한다)은 그 신용정보가 누설되었음을 알게 된 때 지체 없이 금융위원회가 정하여 고시하는 신고서를 금융위원회 또는 금융감독원에 제출해야 한다.

  ⑦ 제6항에도 불구하고 제3항 전단에 해당하는 경우에는 우선 금융위원회 또는 금융감독원에 그 개인신용정보가 누설된 사실을 알리고 추가 유출을 방지하기 위한 조치를 취한 후 지체 없이 제6항에 따른 신고서를 제출할 수 있다. 이 경우 그 조치의 내용을 함께 제출해야 한다.

아. 재해·재난 대응 대비

○ **(백업 및 복구 시스템 운영)** 정보제공자와 마이데이터사업자는 개인신용정보처리시스템의 데이터 백업 시스템 및 재해·재난 침해사고 등 위협 발생 시 대응을 위한 복구 시스템을 설치·운영하여야 한다.

- **(백업·복구 대책 마련)** 사고 발생 시 개인신용정보처리시스템의 신속한 백업 및 복구를 위한 대책을 마련한다.

- **(재해·재난 대응 체계 수립)** 재해·재난 발생을 대비하는 비상계획, 재해복구 훈련 실시 체계를 수립한다.

5.3. 물리적 보안사항

가. 접근통제

○ **(전산설비 분리)** 개인신용정보처리시스템을 운영하는 장소는 물리적 보호구역으로 지정하여 운영하고, 물리적 접근 방지를 위한 출입통제시스템을 설치하여 수립된 출입통제 절차에 따라 출입하여야 한다.

※ 외부 공동전산시설(IDC)을 이용하는 경우 일정수준 이상*의 물리적·기술적 보호조치를 갖춘 시설을 이용할 것을 권고
* 정보보호 관리체계(ISMS, ISO27001 등) 인증을 득한 안전한 시설 이용 권장

※ 개인신용정보를 수집 관리하는 전산 설비는 국내에 위치하여야 한다.(단, 전자금융감독규정 제14조의2항에 따라 국외 사이버몰을 위한 전자지급결제대행업자에 대해서는 그렇지 아니하다.)

- **(출입내역 기록·관리)** 비밀번호 기반, 스마트카드 기반, 바이오정보 기반 등 출입통제 시스템을 설치·적용하고 출입 내역(출입자, 출입일시, 출입목적, 소속 등)을 기록·관리한다.

○ **(보조저장 매체 반·출입 통제)** 보조저장매체 사용 시 책임자 승인, 반·출입 내역 관리 등 통제 절차를 수립하고 적용한다.

- (보조저장매체 접근 통제조치) 개인신용정보처리시스템의 보조저장 매체 접근을 통제하는 보안통제방안*을 설치·운영한다.
  * 접근통제 소프트웨어, 보안스티커 부착, 물리적 봉인 등

- **(보조저장 매체 반·출입 기록 및 관리)** 보조저장매체를 사용할 경우 사용 목적, 일시, 담당자 승인 등 관련 내역을 세부적으로 기록하고 관리한다.

- **(외부자 출입 통제)** 제휴, 위탁 또는 외부주문에 의한 개인신용정보처리시스템 등의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영한다.

나. 물리적 보안

- **(물리적 보안설비 구축)** 안전한 물리적 보안설비(통신회선 이중화, CCTV 등)를 갖추어야 한다.

- **(문서 보관)** 개인신용정보가 포함된 문서 등은 보존기간을 정하여 잠금장치가 있는 캐비넷 등 안전한 장소에 보관하며 열람, 대여 등에 관한 통제시스템을 확립하고 시행한다.

5.4. 기술적 보안사항

가. 비밀번호 관리

- **(비밀번호 관리)** 생일, 주민등록번호, 전화번호 등 추측하기 쉬운 숫자를 비밀번호로 이용하지 않도록 비밀번호 작성 규칙을 수립하고 이행한다.

예시 **비밀번호 작성 규칙 예시**

- 비밀번호는 문자, 숫자의 조합·구성에 따라 최소 10자리 또는 8자리 이상의 길이로 설정
  * 기술 발달에 따라 비밀번호의 최소 길이는 늘어날 수 있다.
  - 최소 10자리 이상 : 영대문자(A~Z, 26개), 영소문자(a~z, 26개), 숫자(0~9, 10개), 특수문자(#, [, “, 〈 등, 32개) 중 2종류 이상으로 조합·구성한 경우

- 최소 8자리 이상 : 영대문자, 영소문자, 숫자, 특수문자 중 3종류 이상으로 구성한 경우

• 비밀번호는 추측하거나 유추하기 어렵도록 설정
- 일련번호(12345678 등), 전화번호, 잘 알려진 단어(love, happy 등), 키보드 상에서 나란히 있는 문자열(qwer 등) 등을 사용하지 않도록 한다.

• 비밀번호를 최소 6개월마다 변경하도록 변경 기간을 적용하는 등 장기간 사용하지 않는다.
- 변경 시 동일한(예시 : Mrp15@*1aT와 Mrp15@*1at) 비밀번호를 교대로 사용하지 않도록 한다.

※ 출처 : 개인정보의 안전성 확보조치 기준 해설서

- **(비밀번호의 주기적 변경)** 각종 비밀번호는 정기적으로 변경하여야 하며 비밀번호 유효기간을 내부정책에 반영하고 시행·관리한다.

- **(비밀번호 차단 및 해제)** 비밀번호를 일정 횟수 이상 잘못 입력한 경우 해당 계정의 접속을 차단하고 본인 여부 확인을 내부정책 및 절차에 따라 실시하여야 하며, 접속 차단 및 해제 등의 이력을 기록·관리한다.

○ **(비밀번호 암호화)** 비밀번호(개인식별이 가능한 바이오 정보, 본인인증정보 등 포함)는 복호화되지 아니하도록 일방향 암호화하여 저장한다.

나. 암호 통제

○ **(개인신용정보 암호화)** 개인신용정보(고유식별정보, 비밀번호, 바이오정보 등 포함)를 암호화하여 저장한다.

〈 암호화 의무 적용 주요내용 〉

적용 기준	구 분	암호화 적용 기준
저장 시	비밀번호, 바이오 정보	• 암호화하여 저장하여 조회할 수 없도록 조치 – 조회가 불가피한 경우 조회사유·내용 등 기록·관리
	개인신용정보	• PC에 저장시 암호화
	주민등록번호	• 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ)에 저장시 암호화 • 내부망에 주민등록번호 저장시 암호화 • 업무용 컴퓨터에 저장 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장
송·수신 시	개인신용정보, 비밀번호, 바이오 정보	• 정보통신망을 통한 송·수신시 SSL 또는 암호화 응용 프로그램 등을 이용하여 암호화
	주민등록번호	• 정보통신망을 통하여 송수신하거나 보조저장매체를 통하여 전달하는 경우 암호화
기타	개인신용정보 (개인식별정보)	• 신용정보집중기관과 신용조회회사가 서로 개인식별번호를 제공하는 경우, 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화 • 신용정보회사등이 개인신용정보의 처리를 위탁하는 경우 개인식별번호를 암호화하여 수탁자에 제공

※ 출처 : 금융분야 개인정보보호 가이드라인, 금융위원회(2016.12.)

– **(업무용 단말기 저장 시 암호화)** 업무용 단말기 및 모바일 기기에 개인신용정보를 저장할 경우 상용 암호화 소프트웨어 또는 안전한 알고리즘을 사용하여 암호화한다.

응용프로그램에서 제공하는 암호 설정 기능

- 한컴 오피스 : 파일〉〉다른 이름으로 저장하기〉〉문서 암호 설정에서 암호 설정
- MS 오피스 : 파일〉〉다른 이름으로 저장하기〉〉도구〉〉일반옵션에서 암호 설정
- 어도비 아크로뱃 : 고급〉〉보안〉〉암호로 암호화 또는 인증서로 암호화
- MS Windows 폴더(파일) 암호화 : 암호화 폴더(파일) 선택하고 마우스 오른쪽 버튼 클릭〉〉속성〉〉일반〉〉고급에서 암호 설정

※ 출처 : 개인정보의 안전성 확보조치 기준 해설서

- **(통신구간 암호화)** 정보통신망을 통해 개인신용정보 및 인증정보를 송·수신할 때에는 보안서버 구축 등의 조치를 통해 암호화하여야 한다.

※ 단 전용회선등을 통해 개인신용정보등을 전송할 시에는 그렇지 아니하다.

- **(안전한 TLS 인증서 적용)** TLS1.3 버전 이상의 인증서를 적용하여 인터넷 기반으로 개인신용정보를 암호화하여 송·수신한다.

참고

〈 TLS 이용 시 고려사항 〉

분류	설명
공신력 있는 인증서 이용	공신력 있는 인증기관에서 발급한 TLS 인증서 이용 * 신뢰성이 높고, 기관 정보를 확인할 수 있는 EV(Extended Validation) 등급 인증서 사용)
상호인증	양방향TLS(Mutual TLS)을 적용하여 상호인증 수행
최신 버전의 TLS 이용	TLS1.3 이상을 적용하며 최신 업데이트(패치)를 유지
안전한 암호 알고리즘 이용	안전한 데이터 교환을 위한 암호 알고리즘(암호화 키 교관, 메시지 인증, 데이터 암호화 등)을 이용
인증서 및 키 관리	인증서 및 데이터 전송·암호화에 이용되는 키를 안전한 방법으로 저장·관리
접근통제	TLS 설정 등에 접근 가능한 기기·사용자 등 접근통제 수행
보안에 취약한 옵션 미사용	재생공격에 취약한 0-RTT 핸드쉐이크 옵션 미사용

☞ TLS를 안전하게 사용하는 경우에 한하여 API기반 개인신용정보 전송구간에서는 전용선이나 공중인터넷망 사용이 가능하다. 단, 정보제공자가 금융회사인 경우 중계기관과의 연결시 반드시 전용선 및 이에 준하는 연결을 하여야 한다.

☞ 안전한 TLS이용을 위해 TLS1.3을 이용하여야 하며 내부 여건으로 하위버전(1.2등)를 이용하는 경우에는 가급적 신속하게 업데이트하여야 한다.

- **(암호키 관리)** 암호화 키가 접근이 인가된 사용자 외에는 노출되지 않도록 관리하며 생성부터 폐기까지의 관리기준을 수립하여 안전하게 관리한다.

  ※ 금융부문 암호기술 활용 가이드, 금융보안원, 2019.1. 참고

다. 시스템 보안

- **(망분리)** 내부 업무용시스템, 전산실 내 위치한 정보처리시스템과 해당 시스템에 직접 접속하는 단말기에 대해서 망분리를 수행한다.

  - **(내부 업무용시스템 망분리)** 내부통신망과 연결된 내부 업무용시스템 등은 외부통신망과 분리차단할 수 있도록 망분리를 수행하여야 한다.

  - **(정보처리시스템 망분리)** 전산실 내 위치한 정보처리시스템과 해당 정보처리시스템에 직접 접속하는 단말기에 대해서 인터넷 등 외부통신망으로부터 물리적으로 분리하여야 한다.

관련법령

- **전자금융감독규정 제15조(해킹 등 방지대책)** ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

  1.,2. (생략)

  3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다)

  4. (생략)

  5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.)

- **(침입차단·탐지시스템 설치 및 운영)** 개인신용정보처리시스템에 침입차단시스템과 침입탐지시스템을 설치하고 운영하여야 한다.

  - **(침해위협 탐지·대응)** 내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응한다.

  ※ 가입자 수 100만명 이상의 마이데이터사업자는 가입자 100만명에 도달한 시점에서 1년 이내에 금융보안원 금융보안관제센터가 제공하는 보안관제 서비스에 가입해야 한다.

  - **(이상거래 탐지 및 대응)** 이상거래 시도를 포함한 보안사고 등을 모니터링 및 기록(IP주소, 인증 실패 횟수, 부정한 API 요구 등)하고 지원기관에 공유한다.

- **(백신소프트웨어 설치·관리)** 개인신용정보처리시스템 등 정보처리기기에 컴퓨터 바이러스, 스파이웨어 등 악성 프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치한다.

  - **(백신소프트웨어 갱신·점검)** 소프트웨어는 월 1회 이상 주기적으로 갱신·점검하고, 바이러스 경보가 발령된 경우 및 백신 소프트웨어 제작 업체에서 업데이트 공지를 한 경우 즉시 최신 소프트웨어로 갱신·점검한다.

라. 개발 보안

- **(보안 설계)** 마이데이터서비스 개발 및 변경 시 보안 요구사항을 도출하고 이에 대한 대책을 설계에 반영하여 개발한다.

  - **(API보안 설계)** 자격증명, 접근토큰 등 API 관련 중요정보가 처리과정 및 관리과정 중 노출되지 않도록 설계하고 이에 따라 개발한다.

- **(테스트데이터 활용)** 마이데이터서비스 개발시에는 개인신용정보가 아닌 가상의 테스트데이터를 활용해야 한다.

○ **(취약점 점검)** 마이데이터사업자는 고객에 마이데이터서비스를 제공하기 이전에 취약점 점검을 수행하여야 한다.

※ 금융보안원 또는 전문기관을 통해 취약점 점검 수행

마. 출력·복사 시 보호조치

○ **(출력·복사 보호 내부시스템 구축)** 개인신용정보취급자는 개인신용정보 출력·복사 시 보호조치를 위한 내부시스템을 구축한다.

○ **(출력항목 최소화)** 개인신용정보처리 시스템에서 개인신용정보를 출력(인쇄, 화면표시, 파일생성 등)할 경우 용도를 특정하여야 하며, 불필요한 개인신용정보가 노출되지 않도록 출력 목적에 따라 출력 항목을 최소화한다.

- **(불필요 정보 마스킹·삭제 처리)** 불필요한 정보가 노출되지 않도록 일부 정보를 마스킹하거나 삭제한다.

○ **(출력·복사 시 기록·관리)** 개인신용정보를 조회(출력, 복사 등)하는 경우 조회자의 신원, 조회일시, 대상정보, 목적, 용도 등을 기록하고 관리한다.

○ **(외부 전송 사전 승인)** 개인신용정보를 보조저장매체에 저장하거나 이메일 등의 방법으로 외부에 전송하는 경우 관리책임자의 사전 승인을 받아야 하며, 승인신청자에게 관련 법령을 준수하여야 한다는 사실을 알려야 한다.

www.fsec.or.kr

금융분야 마이데이터 기술 가이드라인

PART.

06

Q&A

6 Q&A

1. 개인신용정보 전송

궁금해요?

Q 기관간 개인신용정보 전송 요구 시 전송할 수 있는 데이터 범위는?

A 신용정보법 제33조의2②에 따르며 구체적인 내용은 신용정보원이 제공하는 금융분야 서비스 가이드라인 3.3.을 참고바랍니다.

Q 마이데이터사업자도 개인신용정보 전송요구에 응해야 하는지?

A 마이데이터사업자는 신용정보법 제33조의2에 따른 데이터정보제공·이용자등(정보제공자)에 포함되어, 동법 제33조의2②항에 해당하는 개인신용정보에 대해 고객의 개인신용정보 전송요구에 응하여야 합니다. 단, 타 정보제공자를 통해 수집한 정보는 전송의무를 가지고 있지 않습니다.

* 고객의 개인신용정보 전송요구에 응하여야 하는 기관 정보는 [참고1]정보제공자·정보수신자 범위 참고

Q 고객, 마이데이터사업자 외에도 개인신용정보를 전송받을 수 있는지?

고객, 마이데이터사업자 외에 신용정보법령에 따라 개인신용정보를 수신할 수 있는 금융기관은 고객의 개인신용정보전송 요구에 따라 개인신용정보를 수신할 수 있습니다.
* 고객의 개인신용정보 전송요구에 의해 개인신용정보를 수신가능한 기관 정보는 [참고1]정보제공자·정보수신자 범위 참고

A

Q 마이데이터사업자에게 API를 이용하여 개인신용정보를 전송할 경우, 중계기관을 이용하여 전송할 수 있는지?

신용정보업 감독규정(제23조의3③)에 정의된 기관 외의 기관은 중계기관을 이용하여 개인신용정보 전송 수행이 가능합니다. 다만 그 외의 기관은 자체적으로 시스템를 구축하여 개인신용정보를 전송하여야 합니다.

A

Q 개인신용정보 전송 요구 시 비밀계좌, 보안계좌 등이 표기되지 않는데, 고객은 이를 전송 요구할 수 없는지?

비밀계좌, 보안계좌 등과 같이 고객이 비대면 정보 조회 금지를 요청한 정보를 원칙적으로 개인신용정보 전송요구 대상에서 제외되어 전송요구시 표기되지 않습니다. 이 경우 고객이 금융회사 창구등을 통해 해당 정보에 대하여 일반계좌로 전환 시 개인신용정보 전송요구가 가능합니다.

A

Q 중계기관을 이용하여 개인신용정보를 전송할 경우 해당 개인신용정보는 중계기관에서 저장·보관하는지?

A 중계기관은 개인신용정보 전송을 중계할 뿐 해당 개인신용정보를 별도로 저장·보관할 수 없습니다.

Q 마이데이터사업자는 정보제공자에 정기적 전송을 요구할 수 있는데, 주기에 따른 전송 횟수 제한이 있는지?

A 개인신용정보의 정확성 및 최신성 유지를 위해 마이데이터사업자는 최대 1주 1회*에 한하여 동일한 내역의 개인신용정보를 정보제공자에 전송 요청 가능합니다. 단, 고객이 직접 개입한 경우(조회, 새로고침 등)는 횟수 제한 없이 전송 요청이 가능합니다.
*1주의 기준은 일요일에서 토요일로 함

Q 정기적 전송 중 개인신용정보 전송 지연이 발생하였을 때도 고객에게 지연고지를 하여야 하는지?

A 정기적 전송이 고객의 명시적인 요구 행위가 아닌점, 또한 정기적 전송이 통상 야간, 새벽등에 발생하여 지연고지 시 고객 불편이 발생할 수 있는 점 등을 고려하여 정기적 전송에 한해 고객에 지연고지 의무가 면제됩니다.

Q 지체없이 전송에서 지체없이의 의미는?

고객이 정보 전송을 요구하는 시점에서 정보제공자가 시스템의 처리시간에 따라 정보를 즉시 전송하는 것을 의미합니다.

A

Q 개인신용정보 전송요구시 별도의 동의절차가 있는지?

신용정보법령에서 요구하는 동의절차외에 별도로 지원기관이 정의하는 '알고하는 동의절차'를 적용해야 합니다.

A

2. 마이데이터서비스

궁금해요?

Q 마이데이터사업자 허가를 위한 절차는?

A 신용정보업 감독규정 별표1(본인신용정보관리업 허가 등의 절차) 또는 본 가이드라인의 [참고2] 참고바랍니다.

Q 마이데이터서비스는 모바일 앱만을 의미하며 브라우저를 통한 웹서비스는 해당되지 않는지?

A 기능확장, 정보보호·보안 등을 고려하여 현재는 모바일 앱서비스를 고려하여 가이드라인이 구성되어 있습니다. 다만, 통합조회등의 마이데이터서비스는 웹을 이용하여서도 제공이 가능합니다.

Q 가이드라인 내 용어를 필수적으로 이용하여야 하나요?

A 고객 편의성을 위하여 고객에게 익숙한 용어로 변경하여 이용가능합니다. (예, 개인신용정보 전송 철회 → 연동 해제 등)

Q 전용앱이 아닌 뱅킹 앱 등 별도서비스의 인앱(in-app)형태로 마이데이터 서비스를 제공할 경우도 별도의 마이데이터 서비스 회원가입/탈퇴 절차가 필요한가요?

A 전용앱이 아닌 인앱 형태로 마이데이터 서비스를 제공하는 경우에도 고객의 마이데이터 서비스 회원가입(또는 별도의 서비스 이용 동의)을 받아야하며, 마이데이터 서비스 회원탈퇴(또는 별도의 서비스 이용 해지) 기능을 제공하여야 합니다.

Q 마이데이터사업자의 영업 범위는 본인신용정보 통합조회 서비스로 한정되는지?

A 마이데이터사업자는 고유업무인 본인 신용정보통합조회 서비스 이외에 부수·겸영업무*에 속한 서비스 제공도 가능합니다.
* 부수업무: 수집한 개인신용정보를 기초로하는 데이터 분석 및 컨설팅 업무
* 겸영업무: 투자자문업 또는 투자일임업 등

Q 고객이 "전송을 요구하는 목적"을 특정할 시, 해당 내용을 고객이 직접문자열로 입력하는 형태가 아닌, 시스템에 기입력된 내용을 고객이 선택하는 방식으로 제공이 가능한지?

A 전송을 요구하는 목적 등 전송 시 특정사항은 신용정보원의 알고하는 동의 절차 및 기준을 준수하면 됩니다.

Q 통합인증을 통해 고객의 정보제공자 가입정보를 가져오고자 할 때, 한번에 선택할 수 있는 정보제공자 수가 제한되는지?

A 마이데이터 사업자는 고객편의, 전송요구 처리 부하등을 고려하여 최대 50개의 정보제공자를 고객이 한번에 선택할수 있도록 화면을 제공할 수 있습니다. 단, 고객은 마이데이터 사업자가 자율 구성한 정보제공자에 대해 개별적으로 추가·수정 선택할 수 있어야하며, 고객이 각 정보제공자를 개별적으로 추가 선택한 경우에는 50개 초과가 가능합니다.

Q 고객에게 두가지 인증수단(개별인증, 통합인증)을 모두 제공하여야 하나요?

A 마이데이터사업자는 통합인증을 반드시 제공하여야 하나, 개별인증은 제공여부를 선택가능합니다.

Q 기능적합성 심사 및 보안 취약점 정보에 대한 정보는 어디서 확인 가능한가요?

A 금융분야 마이데이터 테스트베드 내 자료실에서 확인 가능합니다.
*https://developers.mydatakorea.org

Q 웹, 모바일 등을 통해 수집한 개인신용정보를 이용하여 고객에게 대면 방식(금융창구 등)을 통한 마이데이터서비스 제공이 가능한지?

A 개인신용정보를 웹, 모바일 등을 통해 수집하였다 하더라도, 불완전 판매의 가능성이 있어 고객에게 대면 방식의 마이데이터서비스 제공은 할 수 없습니다.

Q 시행령 제18조의6제10항에 따라 연 1회 개인신용정보 전송 요구 내역을 탈퇴 고객에게도 통지하여야 하는지, 통지한다면 고객에게 통지하기 위해 탈퇴한 고객의 신용정보 전송요구내역에 관한 기록을 보관 가능한지?

A 1년 내 탈퇴한 고객에게도 통지하여야 합니다. 다만, 탈퇴 전 통지를 하였고 연 1회 통지 요건을 충족시킨 경우 통지하지 않아도 됩니다. 또한, 마이데이터사업자가 시행령 제18조의6제10항에 대한 통지 의무 이행을 위하여 기록을 보관하는 것은 법령상 의무 이행을 위하여 보관하는 것이므로 탈퇴 고객의 정보임에도 통지 시까지 신용정보 전송 내역 기록을 보관할 수 있습니다. (단, 수집한 개인신용정보는 탈퇴시 모두 삭제하여야함)

※ 서비스 가이드라인 Q&A의 Q20, Q21 참조(122p)

3. API

궁금해요?

Q 정보제공자가 고객에게 직접 개인신용정보를 전송할 때에도 API를 이용하여야 하는지?

A 고객이 요구한 개인신용정보를 정보제공자가 직접 전송할 시에는 PDS방식 등 별도로 정하는 바에 따릅니다.

Q 일시적인 API 요구 증가 등 망부하로 인해 전송요구에 응대가 어려울 경우 문제가 되는지?

A 일시적인 API 요구 증가로 인한 망부하로 인해 전송이 지연될 경우, 고객 에게 지연 사유를 통지하고 지연사유가 해소된 즉시 전송을 재개할 수 있습니다.

Q API전송구간은 전용망을 사용해야하는지?

A 규격에 따라 안전한 방식의 TLS를 활용할 경우 전용망이 필수는 아닙니다. 다만 더욱 안전한 전송을 위해 전용망 이용은 자율적으로 결정 할수 있습니다.

Q 정보제공자의 API시스템 구축 및 운영업무를 위수탁할 수 있는지?

A 금융기관 업무위탁 규정에 따라 정보제공자는 본질적 업무가 아닌 경우 외부업체와 위수탁계약을 맺어 업무수행이 가능합니다. 다만, 수탁사가 중계기관과 같이 다수의 정보제공자와 위수탁관계를 맺어 동일한 인터페이스로 다수의 마이데이터서비스 제공자에게 개인신용정보를 전송하는 형태는 불가합니다. (수탁 시스템이 계약을 맺는 위탁자만을 위한 전용시스템인 경우에 한해 가능)

Q 정보제공자는 접근토큰관리(발급, 인증 등)를 직접 수행하여야 하는지?

A 정보제공자등은 접근토큰 발급·인증 등 전반적인 접근토큰 관리는 직접 수행합니다. 발급된 접근토큰 내역은 종합포털에 전송되어 고객의 개인신용정보 전송요구 내역에 대한 통합 관리 지원에 이용됩니다.

Q 자격증명과 접근토큰의 차이가 무엇인지?

A 자격증명은 API 호출 시에 정보제공자와 마이데이터사업자간의 API 호출 자격을 인증하고 서로를 식별할 수 있도록 하는 것으로 종합포털이 정보제공자와 마이데이터 사업자에게 발급합니다. 반면 접근토큰은 마이데이터사업자가 개인신용정보 전송 요청 권한을 획득하기 위한 것으로 정보제공자가 마이데이터사업자에게 발급합니다. 접근토큰은 최대 유효기간이 1년이며 개인신용정보 전송 요구 변경·연장 시에 기발급된 접근 토큰을 폐기하고 재발급받아야 합니다.

Q API로 개인신용정보를 조회하는 경우 조회기간에 제한이 있는지?

정보수신자가 API방식을 통해 개인신용정보를 조회하는 경우 과도한 전송트래픽 집중, 정보제공자 API서버 과부하, 전송지연 등을 방지하기 위해 일(Date) 기준 API는 최대 31일, 월(Month) 기준 API는 최대 3개월로 조회기간(From/To)을 설정하여 요청하여야 합니다.

A

Q API규격에 따른 개발을 지원할수 있는 시스템이 있는지?

금융분야 마이데이터 테스트베드를 통해 테스트, 검증 등을 수행할 수 있습니다.
*https://developers.mydatakorea.org

A

Q 테스트베드에 대한 이용절차, 매뉴얼등이 있는지?

금융분야 마이데이터 테스트베드를 통해 확인 가능합니다.
*https://developers.mydatakorea.org

A

Q 토큰이 중복발급되었을 때 그 처리 절차는?

토큰이 중복발급되었을 경우, 해당 사실을 사업자에 통보하고 토큰 삭제 및 오전송 개인신용정보 유무 여부 확인 등 금융보안원이 정하는 후속 절차를 따라야 합니다.

A

4. 본인인증

궁금해요?

Q 정보제공자는 자사가 관리하는 특정한 인증수단 만을 제공해도 되는지?

A 정보제공자는 통합인증을 반드시 제공하여야 하며 개별인증 제공 여부는 선택가능합니다.

Q 정보제공자는 개별인증수단을 별도로 개발하여야 하는지?

A 정보제공자는 별도 자체 개발 또는 타 인증기관이 제공하는 인증방법(예:기존계좌활용 인증(1원 이체 등), 휴대폰 본인확인 등)을 이용하여 고객에 개별인증수단을 제공할 수 있습니다.

Q 중계기관을 이용하여 개인신용정보를 전송할 경우 본인인증 주체는?

A 정보제공자가 중계기관을 이용하여 개인신용정보를 전송할 경우, 중계기관이 정보제공자의 업무(본인인증)를 위탁하여 수행합니다. 이때, 고객이 통합인증을 이용하여 본인인증을 수행할 경우는 중계기관이, 개별인증을 이용하여 본인인증을 수행할 경우는 정보제공자가 본인인증을 수행하여야 합니다.

Q 정보제공자 또는 마이데이터사업자도 통합인증 수단 제공기관이 될 수 있는지?

A 통합인증을 위해서는 공통된 개인식별자(CI) 활용이 필요하며 CI활용에 문제가 없는 인증사업자는 가능합니다. 현재로서는('21년 2월) 적법하게 CI 제공이 가능한 정통망법상 본인확인기관과 전자서명법상 전자서명인증사업자(평가·인정 완료)등이 통합인증기관으로 참여 가능하며, 추후 개별법에 따라 CI활용이 가능한 경우 참여자격이 부여될 수 있습니다.

Q 개별인증 수단으로 휴대폰/신용카드 본인확인서비스 한가지만 적용 가능한지?

A SMS 인증 방식의 휴대폰 본인확인서비스는 다중요소 인증기준을 충족한다고 보기 어려우므로 추가적으로 지식 또는 특징 기반의 인증수단 적용이 필요합니다. 그 외 휴대폰 본인확인서비스 방식 및 신용카드 본인확인서비스 방식의 경우에는 다중요소 인증기준의 충족 여부와 안전성 등을 자율적으로 검토하시어 적용여부를 판단하시기 바랍니다.

Q 개별인증 수단으로 공동인증서, 또는 사설인증서 한가지만 적용 가능한지?

A 개별인증 수단으로는 다중인증, 다중요소 공개키인증서, 비대면실명확인 방식 활용 등을 적용 가능합니다. 공동인증서 및 일반적인 사설인증서는 다중요소 공개키인증서에 해당하므로 다른 인증수단 없이도 적용 가능합니다. 다만, 각 인증서 발급기관에 대한 신뢰성 및 안전성을 충분히 검토하시어 선정 및 적용하시기 바랍니다.

Q 개별인증 수단으로 사설인증서 적용시 반드시 전자서명법상 인정받은 전자서명인증사업자만 선정 및 적용하여야 하는지?

A 통합인증시에는 CI 제공·활용을 위해 사설인증기관의 경우에는 전자서명법상 인정받은 전자서명인증사업자 지위가 필요하지만, 개별인증시에는 CI 제공·활용이 필수가 아니기 때문에 필수 요건이 아닙니다. 다만, 전자서명법상 전자서명인증사업자의 평가·인정 여부는 사설인증기관 선정시 신뢰성 및 안전성 검토에 활용 가능합니다.

Q 통합인증에 따른 전자서명을 정보제공자 및 마이데이터 사업자가 저장·관리하여야 하는지?

A 전송요구내역의 보관 기준에 따라 저장·관리하여야 합니다.

Q 통합인증을 위한 사설인증서 적용시 별도 기준이 존재하는지?

A 마이데이터사업자는 공동인증서 외에 통합인증수단으로 포함된 사설인증서를 1개 이상 적용하여야 하며, 정보제공자는 통합인증처리를 위해 모든 통합인증수단(공동 및 사설인증서)을 허용하여야 합니다.

Q 고객이 기존에 발급받은 개별인증수단을 이용하는 중에 통합인증수단으로 본인인증 방식을 바꾼 후, 기발급된 개별인증수단도 계속 이용할 수 있는지?

A 개별인증수단은 각 정보제공자가 발급하는 인증수단으로 계속하여 이용 가능합니다.

5. 정보보호시설·보안

궁금해요?

Q 마이데이터사업자가 해외에 있는 상용클라우드를 이용할 수 있는지?

A 클라우드 사업자 안정성 평가 등 전자금융감독규정의 요건(제14조)을 지키는 경우에 한하여 이용이 가능합니다. (단, 개인신용정보는 국내에서 저장되어야 함)

Q 마이데이터사업자가 해외에 위치한 전산센터(IDC)를 이용할 수 있는지?

A 마이데이터사업자는 국내에 위치한 전산센터만 이용 가능합니다.

Q 망분리의 범위는 어디까지인지?

A 개인신용정보를 처리하는 서버, 서버에 접속하는 주요단말, 개인신용정보 관련 업무를 담당하는 담당자의 PC가 망분리 요건에 해당합니다.

Q 물리적 망분리 외에 논리적 망분리도 허용하는지?

서버와 서버에 접속하는 주요단말은 물리적 망분리, 업무PC는 물리적, 논리적 망분리를 적용하여야 합니다.

A

Q 정보제공자와 마이데이터사업자는 보안수준진단을 받도록 되어 있는데 구체적으로 어떠한 형태의 진단인지?

정보제공자와 마이데이터 사업자는 개정 신용정보법상 의무적으로 받아야하는 상시평가를 수행하면 보안수준진단을 수행하는 것으로 인정합니다.

A

Q 보안수준 진단을 위한 금융권 정보보호 상시평가는 평가를 담당하는 지정기관이 있는 것인지?

신용정보 감독규정 제45조의2에 따라 상시평가 점검 대상은 금융보안원에 점검 결과를 제출하여야 합니다.

A

Q 개보법상 개인정보보호책임자가 신정법상 신용정보관리·보호인을 겸임할 수 있는지?

A 개보법상 개인정보보호책임자가 신정법상 신용정보관리·보호인을 겸임하여 역할을 수행할 수 있습니다.

Q 마이데이터사업자는 주민등록번호를 처리할 수 있는지?

A 개정 신용정보법 시행령에 따라 주민등록번호 처리가 가능합니다. (신용정보법 시행령 제37조의2⑤항 참고)

Q 가입자 100만 이상의 마이데이터사업자가 금융보안원의 보안관제 서비스를 받기 위한 절차는?

A 금융보안원 사원가입을 통해 보안관제 서비스를 받을 수 있습니다.
※ 문의:02-3495-9122

Q 마이데이터 업무에 필요한 전산설비는 기존 업무에 필요한 전산설비와 구분하여 별도로 구축하여 운영해야 하는지?

A 정보보호에 미치는 영향을 자체검토하여 사업자 자율로 운영이 가능합니다.

Q 마이데이터서비스에 대한 보안취약점 점검 방법, 절차는?

마이데이터서비스는 서비스제공 이전 시점에서 보안취약점 점검을 받아야합니다.
(마이데이터 테스트베드 자료실 내 보안취약점 점검 안내서 참고)

A

Q 정보제공자간 API 호출 시 반드시 전용선(또는 VPN)을 의무사용해야하는지?

TLS를 안전하게 사용하는 경우(P.82 참조)에 한하여 전용선이 아닌 TLS를 사용가능합니다, 단, 정보제공자가 금융회사인 경우 중계기관과의 연결시 반드시 전용선 및 이에 준하는 연결을 하여야 합니다.

A

Q 안전한 TLS이용을 위해 특별히 요구되는 버전이 있는지?

안전한 TLS이용을 위해 TLS1.3을 이용하여야 합니다. 내부 여건으로 1.2를 이용하는 경우에는 가급적 신속하게 업데이트 하여야 합니다.

A

www.fsec.or.kr

금융분야 마이데이터 기술 가이드라인

PART.

07

참고

7 참고

참고 1. 정보제공자·정보수신자 범위

가. 정보제공자* 범위

* 신용정보법에 따라 고객의 개인신용정보 전송 요구에 응하여야 하는 자

① 금융기관

은행법에 따라 인가를 받아 설립된 은행, 금융지주회사, 한국산업은행, 한국수출입은행, 농협은행, 수협은행, 중소기업은행, 한국주택금융공사, 금융투자업자·증권금융회사·종합금융회사·자금중개회사 및 명의개서대행회사, 상호저축은행과 그 중앙회, 농업협동조합과 그 중앙회, 수산업협동조합과 그 중앙회, 산림조합과 그 중앙회, 신용협동조합과 그 중앙회, 새마을금고와 그 연합회, 보험회사, 여신전문금융회사, 기술보증기금, 신용보증기금, 신용보증재단과 그 중앙회, 한국무역보험공사, 예금보험공사 및 정리금융회사, 공제조합, 국채등록기관, 한국농수산식품유통공사, 신용회복위원회, 근로복지공단, 소프트웨어공제조합, 엔지니어링공제조합, 정리금융회사, 체신관서, 전기공사공제조합, 주택도시보증공사, 중소벤처기업진흥공단, 중소기업창업투자회사 및 중소기업창업투자조합, 중소기업중앙회, 한국장학재단, 한국자산관리공사, 국민행복기금, 서민금융진흥원, 금융위원회에 등록한 대부업자, 자본재공제조합, 소상공인시장진흥공단, 금융위원회에 자산유동화계획을 등록한 유동화전문회사, 농업협동조합자산관리회사

② 공공기관

행정안전부, 국세청, 관세청, 고용노동부, 보건복지부, 조달청, 공무원연금공단, 주택도시공사, 주택금융공사, 근로복지공단, 신용회복위원회, 지방자치단체 및 지방자치단체조합, 국민건강보험공단, 국민연금공단

③ 전자금융업자
④ 한국거래소, 예탁결제원
⑤ 신용정보회사, 채권추심회사, 본인신용정보관리회사
⑥ 겸영여신업자
⑦ 기간통신사업을 등록한 전기통신사업자
⑧ 한국전력공사
⑨ 한국수자원공사

나. 정보수신자* 범위

* 신용정보법에따라 고객의 개인신용정보 전송 요구에 의해 개인신용정보를 수신받을 수 있는 자

① 신용정보주체 본인
② 본인신용정보관리회사
③ 금융기관

은행법에 따라 인가를 받아 설립된 은행, 금융지주회사, 한국산업은행, 한국수출입은행, 농협은행, 수협은행, 중소기업은행, 한국주택금융공사, 금융투자업자·증권금융회사·종합금융회사·자금중개회사 및 명의개서대행회사, 상호저축은행과 그 중앙회, 농업협동조합과 그 중앙회, 수산업협동조합과 그 중앙회, 산림조합과 그 중앙회, 신용협동조합과 그 중앙회, 새마을금고와 그 연합회, 보험회사, 여신전문금융회사, 기술보증기금, 신용보증기금, 신용보증재단과 그 중앙회, 한국무역보험공사, 공제조합, 국채등록기관, 한국농수산식품유통공사, 신용회복위원회, 근로복지공단, 소프트웨어공제조합, 엔지니어링공제조합, 정리금융회사, 체신관서, 전기공사공제조합, 주택도시보증공사, 중소벤처기업진흥공단, 중소기업창업투자회사 및 중소기업창업투자조합, 중소기업중앙회, 한국장학재단, 한국자산관리공사, 국민행복기금, 서민금융진흥원, 금융위원회에 등록한 대부업자, 자본재공제조합, 소상공인시장진흥공단, 금융위원회에 자산유동화계획을 등록한 유동화전문회사, 농업협동조합자산관리회사

④ 개인신용평가회사
⑤ 개인사업자신용평가회사

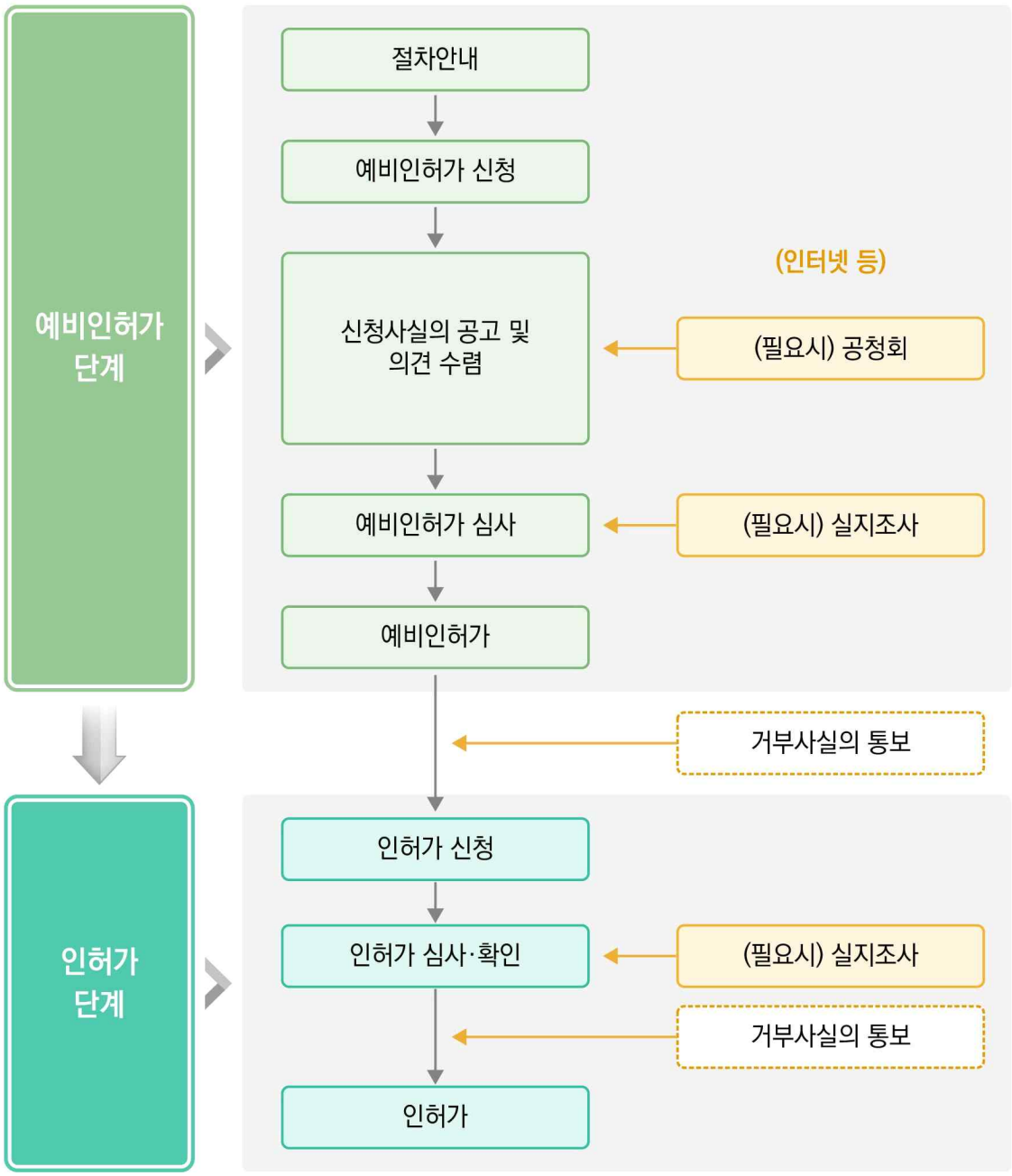
참고 2. 본인신용정보관리업자 허가요건 및 절차

- 본인신용정보관리업자는 해당 업의 수행을 위해 다음의 요건을 구비하여 금융위원회로부터 허가를 받아야 함(신용정보법 제4조)

본인신용정보관리업 허가에 필요한 정보처리·정보통신설비 요건
(신용정보업감독규정 별표2)

구성	세부 요건
시스템 구성	1. 시스템 구성에 다음 항목을 포함할 것 가. DB서버, 통신서버, 웹서버, 보안서버 등 서버 시스템 나. 저장장치, 단말기 등 기타 주변장치 다. 해당업무 영위를 위한 각종 S/W 프로그램 2. 백업 및 복구시스템을 갖출 것 3. 내외부 네트워킹 등 통신시스템 구성 등을 갖출 것
보안체계	1. 침입차단시스템, 침입탐지시스템, 이동식저장장치 통제 프로그램, 바이러스 및 스파이웨어 탐지 및 백신프로그램을 갖출 것 2. 업무 위탁 및 외부 시설·서비스의 이용 시 보호대책을 마련할 것 3. 직무분리 기준을 수립할 것 4. 안전한 비밀번호 작성 규칙을 마련할 것 5. 비상계획, 재해복구 훈련 실시 체계를 갖출 것 6. 서버, 단말 등에 대한 접근통제 방안을 마련할 것 7. 전산실, 자료보관실 등에 대한 출입통제 절차를 마련할 것 8. 주요 데이터에 대한 접속기록 유지할 것 9. 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위한 대책을 마련할 것(「전자금융감독규정」 제15조제1항제3호 및 제5호를 준용하고, 클라우드컴퓨팅서비스 이용과 관련하여 같은 규정 제14조의2 제1항·제2항·제8항을 준용한다.) 10. 안전한 물리적 보안설비(통신회선 이중화, CCTV 등)를 갖출 것 11. 안전한 백업대책을 갖출 것 12. 안전한 데이터 암호화 처리방침 및 암호처리 시스템 구축 할 것 13. 외부에서 정보처리시스템 접속 시 안전한 접속 및 인증수단(VPN 등)을 적용할 것

본인신용정보관리업 허가 등의 절차
(신용정보업감독규정 별표1)



※ 예비인허가, 인허가 시 구비 서류는 신용정보업감독규정「별표1의2. 신용정보업, 본인신용정보관리업, 채권추심업 및 신용정보집중기관 허가 등의 신청서류(제5조제2항 관련)」 참조

참고 3. 주요 인증 규격(가이드라인)의 인증 수준 요구 현황

○ 미국 NIST, 디지털 신원 가이드라인(SP 8000-63-3)

- 인증을 통해 개인정보에 접근 가능한 경우 등에는 다중 인증에 해당하는 AAL 2 이상에 해당하는 인증 수단 적용

보증 수준	허가 인증 수단 (예시)
AAL* 3 (높음)	• OTP + 다중 요소 공개키 인증서(예: 전자서명 생성시 비밀번호 요구) • 공개키 인증서(보안 영역에 저장) + 비밀번호 • 다중 요소 공개키 인증서(보안 영역에 저장) • OTP + 공개키 인증서 + 비밀번호
AAL 2	• 다중 요소 OTP(예: OTP 생성시 비밀번호 요구) • 다중 요소 공개키 인증서 • 비밀번호 + 보안카드/OTP/공개키 인증서
AAL 1 (낮음)	• 비밀번호, 보안카드, OTP, 다중 요소 OTP, 공개키인증서 등

* AAL(Authentication Assurance Level) – 인증 보증 수준

○ EU, PSD2 하위 강력한 고객인증(SCA) 등에 대한 규제기술표준(RTS)

- 지급자(고객)가 자신의 온라인 지급계좌에 접근(지급지시, 거래내역 조회 등)하는 경우 다중 인증을 적용하도록 규정

ISO/IEC:29115 실체 인증 보증 프레임워크 표준

- 민감 개인정보 및 개인 경제활동 정보 접근시 다중 인증에 해당하는 LoA 3 이상에 해당하는 인증 요구사항 적용

보증 수준	인증 요구사항
LoA* 4 (높음)	• H/W 암호화 기반 인증수단 (전자서명 적용) • 대면인증 필수 또는 이에 준하는 수준의 신원확인
LoA 3	• 지식인증과 소유인증 필수 • 일반적인 수준 이상의 엄밀한 신원확인
LoA 2	• 소유 기반 인증 또는 이에 준하는 보안수단 필수 • 신원의 신뢰성 있음(일반적인 수준의 신뢰수준)
LoA 1 (낮음)	• ID/PW, 단일 요소 인증 • 신원확인절차가 없거나 신원의 신뢰성을 요하지 않음

* LoA(Level of Assurance) – 인증 보증 수준
※ 출처 – 공공웹사이트 인증 수단 소개서(행정안전부, 2018.9.)

참고 4. 비대면 실명확인 방식

① **실명확인증표 사본 제출** : 고객이 실명확인증표(원본)를 사진촬영 또는 스캔 후 컴퓨터 또는 모바일 기기를 통해 이메일, 파일 업로드 등의 방식으로 제출

② **영상통화** : 금융회사 또는 금융회사 직원이 영상통화 등을 통해 실명확인증표상 사진과 고객의 얼굴을 대조

* 고객이 위협이나 강박상태에 있는 등 의심할 만한 정황이 있는 경우 다른 비대면 방식을 통한 추가 확인이나 대면확인 요구 가능

③ **접근매체 전달과정에서 확인** : 본인만 수취할 수 있는 우편 등을 통해 고객에게 현금카드, 통장, OTP, 보안카드 등 접근매체 전달과정에서 실명확인증표 확인

④ **기존계좌 활용** : 타 금융회사에 이미 개설되어있는 고객의 기존계좌로부터 금융회사가 소액이체를 받는 등의 방식*을 통해 고객이 동 계좌에 대해 사용권한이 있는지 확인

* 예 : ❶고객이 금융회사가 지정한 금액을 이체, ❷금융회사가 기존 계좌에 소액이체 후 고객이 해당 자금을 금융회사에 재이체, ❸고객의 기존 계좌에 대해 금융회사가 소액이체 등의 방식을 통해 1회용 인증번호 등을 전송하고 고객이 해당 인증번호를 입력하는 방법 등

⑤ **기타 이에 준하는 방법*** : 금융회사에 생체정보**(이하 “바이오정보”라 한다)를 등록한 고객은 사전에 대면·비대면 등으로 등록한 바이오정보와 비교를 통해 확인

* 바이오정보 외에 새로운 방식의 실명확인 방안에 대한 금융위원회의 승인은 불필요하고, 금융회사가 자체적으로 판단하여 적용 가능

** 지문, 정맥, 얼굴(안면), 홍채, 음성, 서명, 키스트로크, 보행 등 개인의 신체적 또는 행동적 특징을 디지털화한 정보

⑥ **타 기관 확인결과 활용** : 신용카드, 공동인증서, 아이핀(I-PIN), 휴대폰과 같이 인증기관 등에서 신분확인 후 발급한 파일, 아이디·비밀번호, 전화번호 활용

⑦ **다수의 고객정보 검증** : 고객이 제공하는 정보(예 : 전화번호, 주소, 이메일, 직장정보 등)와 신용정보회사 등이 보유한 정보를 대조

참고 5. 마이데이터 정보제공자용 접근토큰 관리 자체점검표

점검항목		점검결과 (O/X)
1.규격 및 유효기간	1-1. 접근토큰 표준 규격(JWS)을 준용	
	1-2. 리프레시토큰의 유효기간을 실제 전송요구 종료시점과 같거나 길게 설정하여 발급	
	1-3. 정보제공API 접근토큰의 유효기간을 90일 이내로 설정하여 발급	
	1-4. 정보제공API 리프레시토큰의 유효기간을 1년 이내로 설정하여 발급	
	1-5. 지원API 제공용 접근토큰의 유효기간을 1년 이내로 설정하여 발급	
	1-6. 접근토큰 발급·재발급 시 전송요구 동의기간을 참고하여 유효기간을 알맞게 설정하여 발급	
2.발급관리	2-1. 실제로 전송을 요구한 정보주체에 해당하는 접근토큰과 리프레시토큰을 발급	
	2-2. 정보주체별로 중복된 접근토큰과 리프레시토큰이 발급되지 않도록 발급시 확인・관리	
	2-3. (개별인증 시) 인가코드 발급 시 client_id, redirect_uri 검증을 수행	
	2-4. (개별인증 시) 인가코드의 유효시간 10분 이내로 설정	
	2-5. 동일 정보제공자라 하더라도 복수개의 업권에 대해서 각 업권별로 접근토큰을 발급·관리	
3.갱신 및 폐기관리	3-1. 전송요구 유효기간 동안 리프레시토큰을 무단 변경하지 않음 (갱신·삭제 등)	
	3-2. 전송요구 변경에 따라 새로운 접근토큰과 리프레시토큰 발급 시 기존 접근토큰과 리프레시토큰을 즉시 폐기	
	3-3. 전송요구 철회시 접근토큰과 리프레시토큰을 즉시 폐기	
4. 정보제공	4-1. 정보제공 API 응답시 타인의 정보가 제공되지 않도록 접근토큰 중복여부, 유효성을 검증	
	4-2. 전송요구 기한 만료 이후 정보제공 API 응답이 이루어지지 않도록 전송요구 종료시점을 검증(40106 에러코드 관련)	

금융분야 마이데이터 기술 가이드라인

발 행 일 2021년 2월 23일

발 행 처 금융보안원
(16881) 경기도 용인시 수지구 대지로 132
T. 02-3495-9000

디자인·인쇄 경성문화사
T. 02-786-2999