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