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

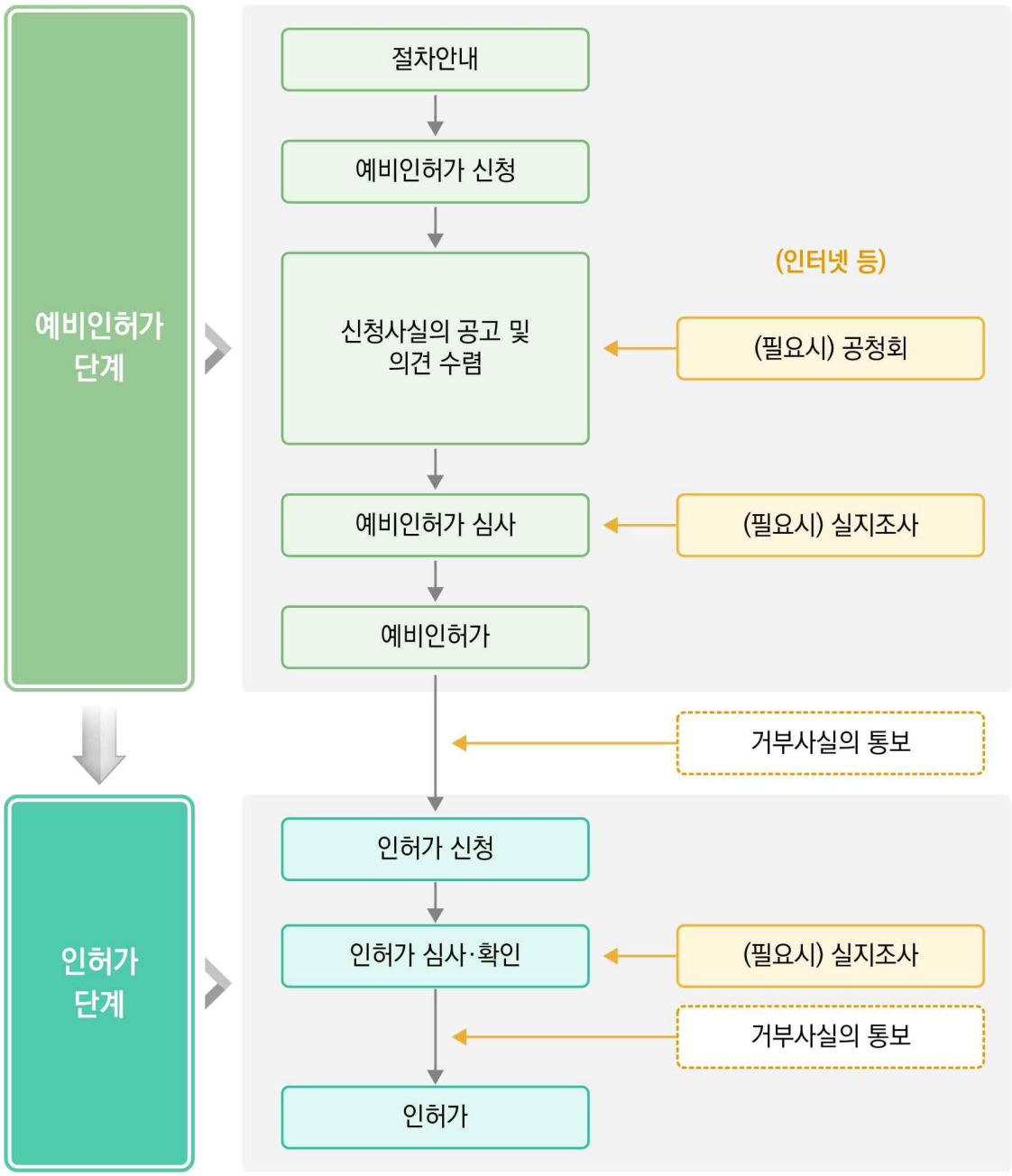
참고 2. 본인신용정보관리업자 허가요건 및 절차

- 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)	