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, 인증 요구를 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

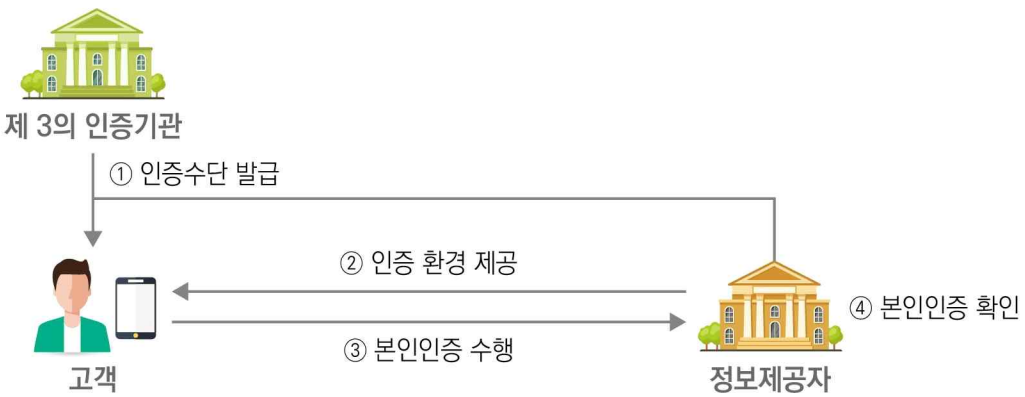
③ **(본인인증 수행)** 고객은 개인신용정보 전송요구를 위해 인증기관 또는 정보제공자가 제공하는 인증수단을 이용해 본인인증을 수행한 결과를 정보제공자에게 전달한다.

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.

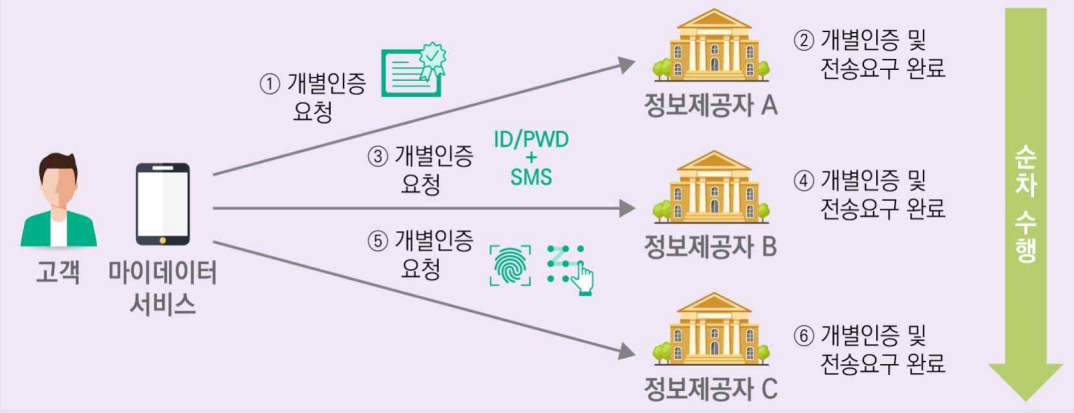
  * 개별인증의 특성에 따라 다수 정보제공자가 동일한 인증수단(예: 공동인증서 등)을 요구하는 경우에도 고객은 각 정보제공자별로 순차적으로 인증을 수행

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

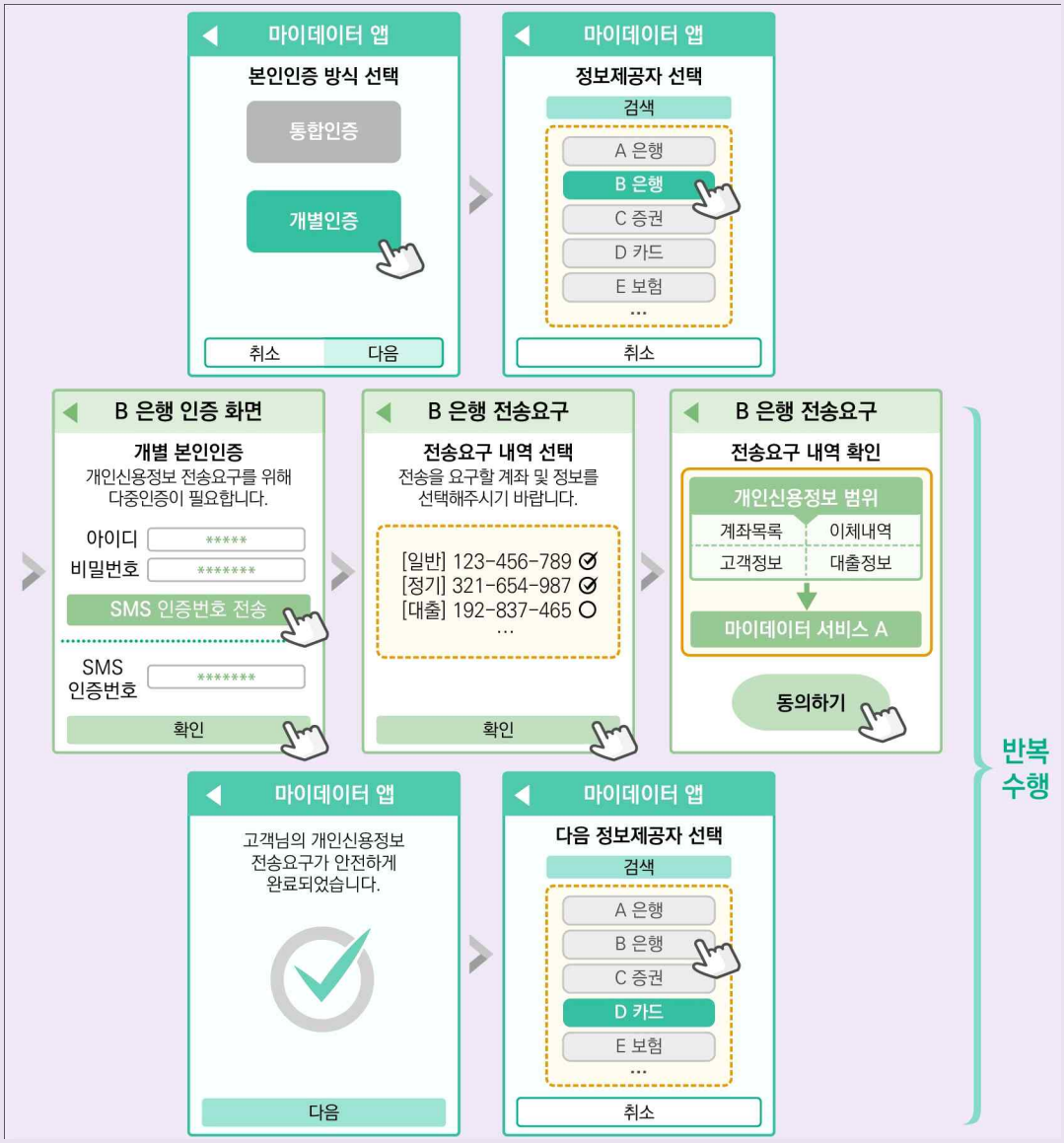
  * 인증 인터페이스의 유형(웹 화면, 별도 앱 등)은 각사가 자율적으로 결정할수 있으며, 반드시 인터페이스 호출을 위한 표준 API를 제공하여야 한다.(「금융분야 마이데이터 표준 API 규격」 참조).

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

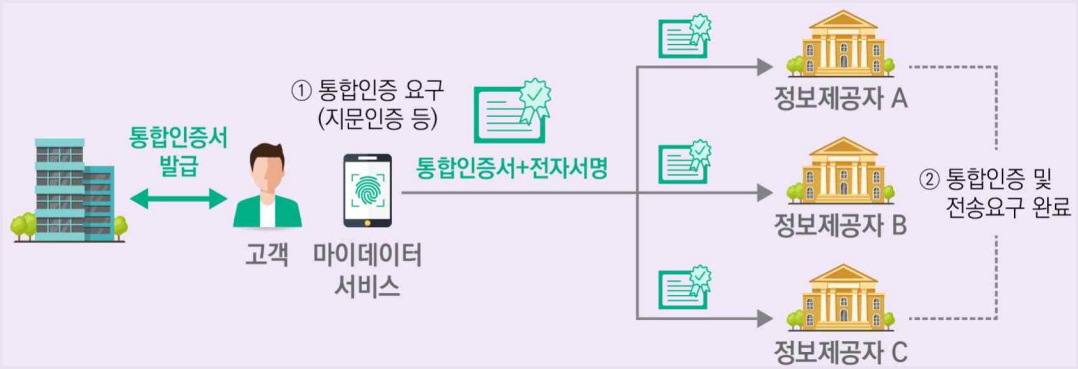
** 정보제공자는 마이데이터사업자가 인증수단을 전송할 수 있도록, 인증기관은 정보제공자가 인증수단의 검증·확인 등을 요청할 수 있도록, 통합인증을 위한 표준 API를 제공하여야 한다.(「금융분야 마이데이터 표준 API 규격」 참조).

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

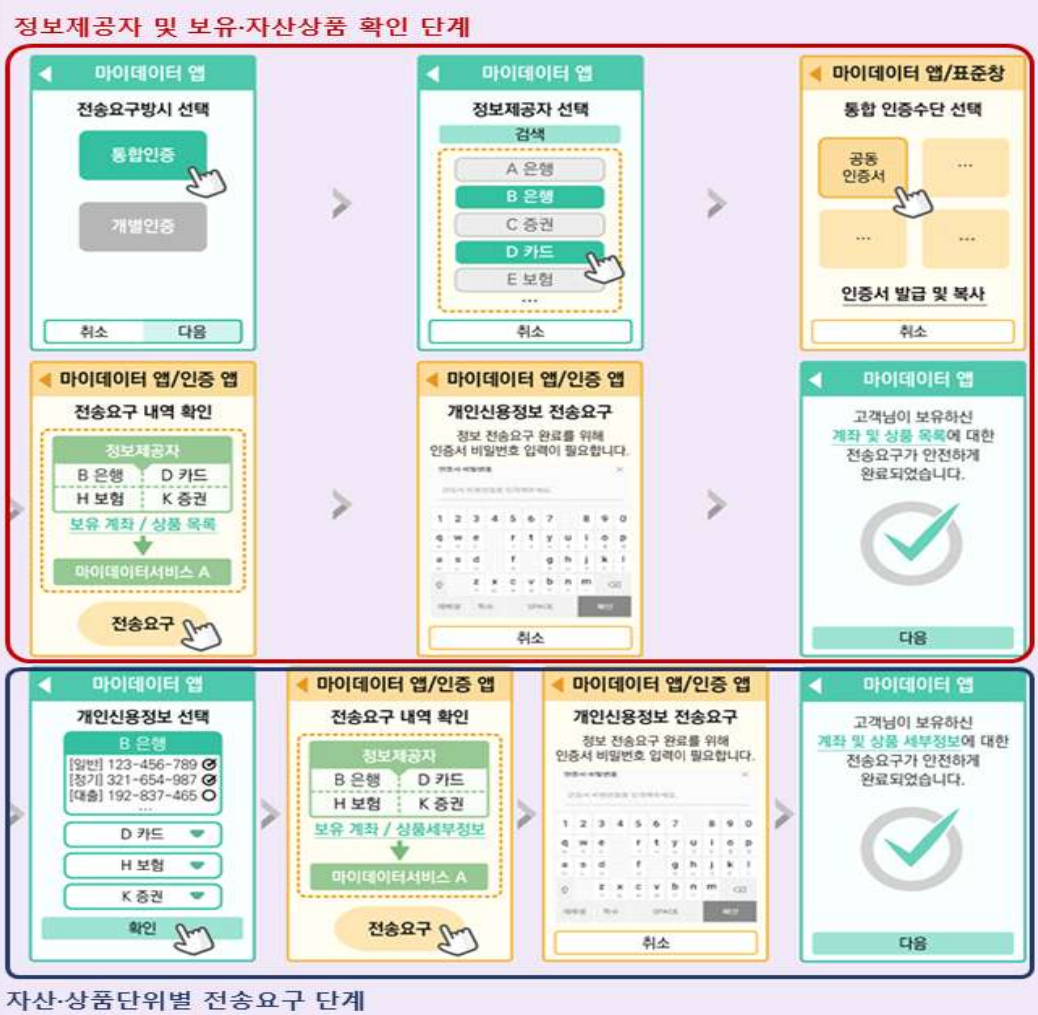
○ **(통합 본인인증 절차)** 통합 본인인증은 고객이 가입한 정보제공자 및 보유자산·상품을 확인하는 단계와 자산·상품단위별 전송요구를 하는 단계로 구성된다.

- **(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.