금융인증서란

■ 금융인증서

- 금융결제원(YesKey) 기반의 클라우드 저장 방식 전자인증서

- 온라인 금융거래에서 본인 확인과 전자서명(법적 효력)을 제공하는 서비스
    * 기존의 PC 저장형(공동)인증서보다 발급·사용·갱신이 간편하도록 설계되어 있고, 은행 앱 등에서 바로 발급·관리할 수 있음

■ 설치(발급) 방법 — 모바일/PC

A. 모바일(은행/증권 앱)에서 발급

* 은행 앱 실행 → 메뉴(인증/보안 · 인증센터) → 금융인증서 발급/사용등록 선택
* 본인확인 : 주민등록·계좌번호·휴대폰 인증 등(은행마다 요구사항 약간씩 다름)
* 비밀번호(보통 6자리 PIN) 설정 – 인증서용 PIN이 생성되어 클라우드에 묶임
* 발급 완료 – 인증서(및 공개키 관련 정보)는 금융결제원의 안전한 클라우드(YesKey)에 저장
* 이후 동일 계정(또는 등록한 기기)에서 PIN으로 간편 로그인/서명 가능

B. PC(인터넷뱅킹)에서 발급

* 은행 인터넷뱅킹 접속 → 인증센터 → 금융인증서 발급 메뉴 선택
* 본인확인(휴대폰·보안매체 등) 후 인증서 발급 → 클라우드 등록(또는 기존 모바일 인증서를 연동)

■ 구조(어떻게 구성되어 있나) — 구성요소 요약

- 개인키(Private key)
    * 사용자 고유의 전자서명 키

- 금융인증서
    * 사용자 개인키를 금융결제원의 클라우드 암호화 저장소에 안전하게 보관하고, 사용 시 PIN·단말 인증으로 그 키를 사용해 서명하도록 제공됨

- 공개키/인증서(Certificate)
    * 공개키와 사용자 식별정보, CA(금융결제원 또는 위탁 CA)의 전자서명이 포함된 전자문서(인증서). 상대방(서비스)은 이 인증서를 통해 서명이 진짜인지 검증함

- 인증 서버(클라우드)
    * 금융결제원(YesKey)의 클라우드 저장소가 핵심 역할 – 키 보관, 인증 요청 처리, 서명대행(키 사용 시) 등

- PIN / 기기 인증
    * 사용자는 PIN(또는 생체인증)을 통해 클라우드에 저장된 개인키를 이용한 서명을 허가함
    * 기기·세션 기반 추가 본인확인이 들어가기도 함

■ 동작 원리 — PKI 기반 플로우

- 발급(초기)
    * 사용자가 본인확인 정보를 제출하면, 인증기관(CA)이 사용자 고유의 공개/개인키 쌍을 생성하거나 사용자의 키를 등록함
    * 공개키와 사용자 정보에 CA의 서명을 붙여 인증서를 발급하고, 개인키는 암호화되어 클라우드에 저장됨

- 서명(서비스에 로그인하거나 거래 승인할 때)
    * 사용자가 서비스에서 인증(또는 거래서명)을 요청하면, 서비스는 금융결제원의 인증 서버로 서명 요청을 보냄
    * 사용자는 PIN/생체로 본인승인 → 금융결제원(클라우드)에서 개인키로 디지털 서명 수행 → 서명 결과가 서비스로 전달되어 거래 성립

- 서비스
    * 금융결제원 또는 CA의 공개키로 서명의 원본(데이터 해시)과 인증서의 유효성을 검증 (서명 검증 = 본인·데이터 무결성 확인)

- 검증과 유효성
    * 서비스는 인증서의 만료기간·폐지목록(CRL)·OCSP(온라인 상태 확인) 등을 검증하여 인증서가 유효한지 확인

■ 금융인증서 vs 공동인증서(주요 차이)

- 저장 방식
  - * 금융인증서 = 클라우드 저장(YesKey)
  - * 공동인증서 = PC·USB 등에 파일로 저장(사용자 보관)

- 설치·사용 편의성
  - * 금융인증서가 훨씬 간편(모바일 발급, PIN 인증) – 플러그인·보안프로그램 설치가 덜 필요

- 보안성
  - * 클라우드 보관은 분실 위험을 줄여주지만, 클라우드 운영 주체에 대한 신뢰/보안이 중요
  - * 반면 사용자 로컬 보관은 유출 위험(PC 해킹, 분실)이 존재