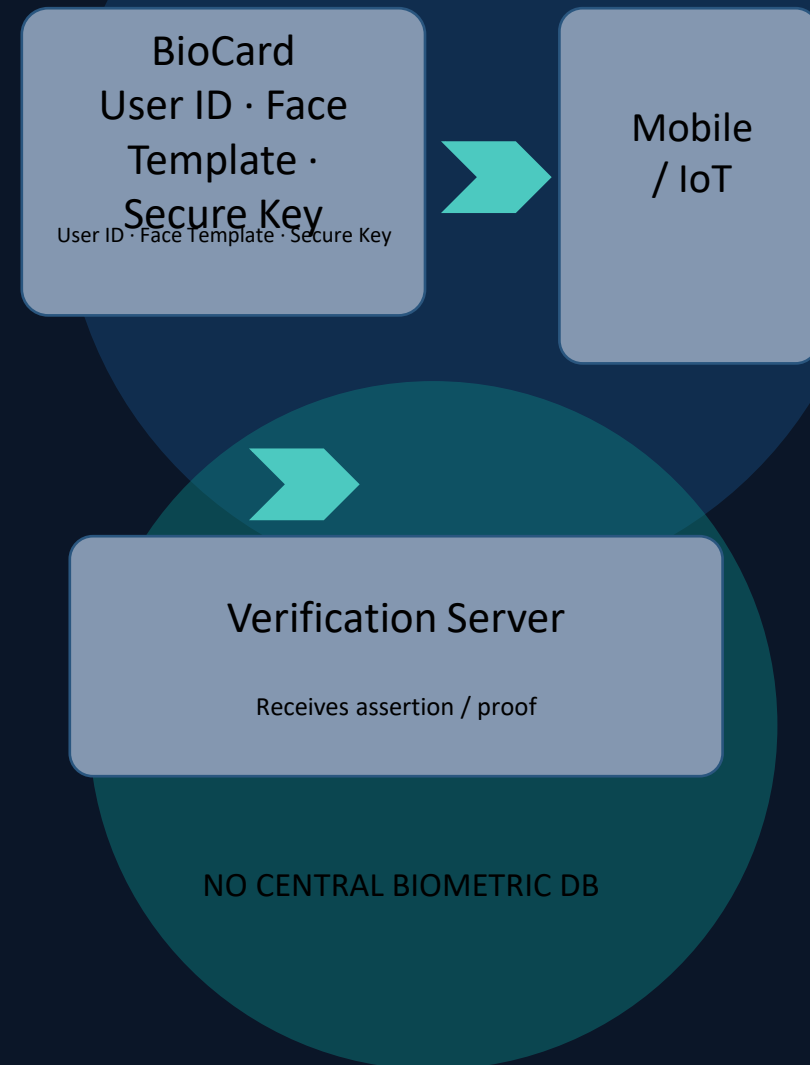


BIOCARD

Zero Trust Face Authentication

얼굴인식 기술을 Zero Trust 구조에 적용한
Privacy-First Biometric Authentication

기술 소개 자료



왜 Zero Trust에 얼굴인증이 필요한가?

핵심은 얼굴인식의 정확도만이 아니라, 인증 과정에서 생체정보와 신뢰를 어떻게 분리하는가입니다.

기존 중앙집중형 얼굴 인증

- 1 사용자 얼굴 / 생체 Template
- 2 중앙 서버 DB에 생체정보 저장
- 3 침해사고 발생 시 생체정보·인증 정보가 집중

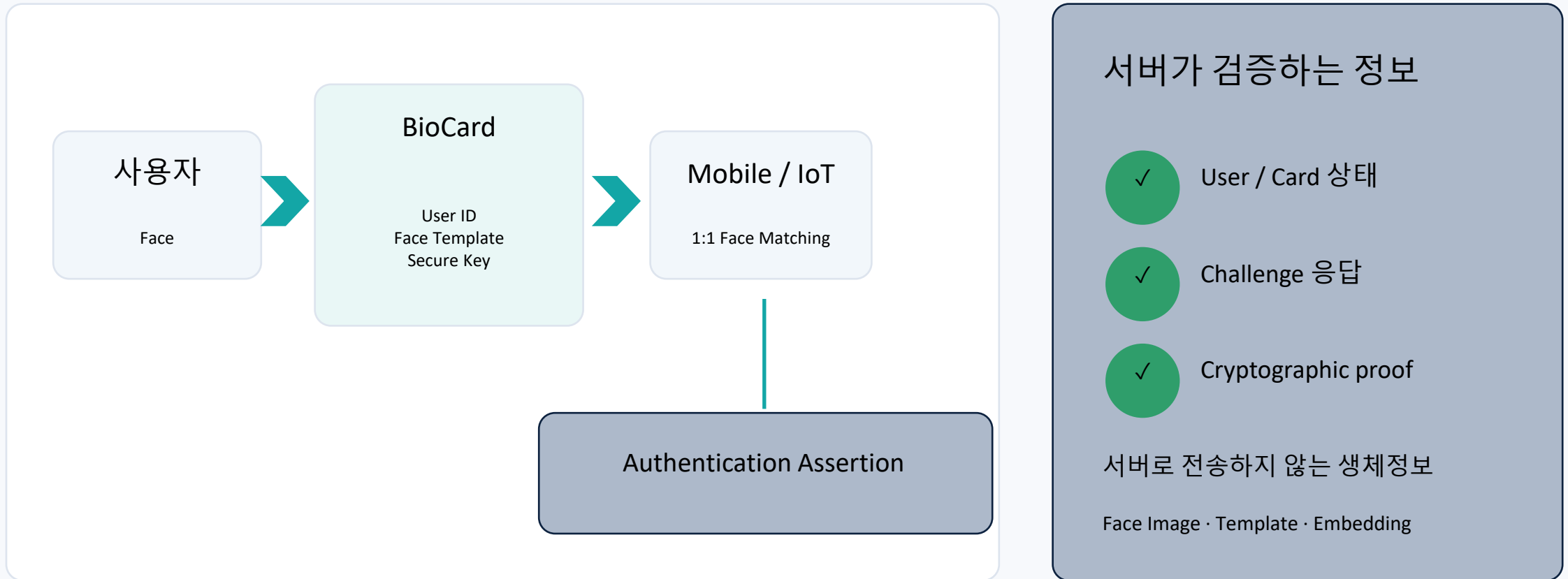
Zero Trust 관점의 요구사항

- 사용자·기기·인증요청을 기본적으로 신뢰하지 않고 검증
- 얼굴정보와 서비스 서버의 데이터 경계를 분리
- 고위험 접근에는 다중 요소 기반의 강한 인증 적용
- 인증 결과는 서버에서 검증 가능한 증명 형태로 전달

핵심 질문: “얼굴을 서버가 보유하지 않아도 사용자를 검증할 수 있는가?”

BioCard 기반 Zero Trust 인증 구조

얼굴 Template은 사용자 측에 보관하고, 서비스 서버에는 검증 가능한 인증 결과만 전달합니다.



Zero Trust를 구성하는 4개의 기술 요소

얼굴인식 자체보다 Identity, 보유 요소, 암호학적 검증, 데이터 경계를 함께 설계합니다.

1

BIOMETRIC

ARE

얼굴을 이용한 1:1 사용자 검증

2

POSSESSION

HAVE

BioCard 및 Secure Key를 이용한
보유 요소 검증

3

CRYPTO

CHALLENGE / PROOF

Challenge에 대한 암호학적 응답
으로 인증 요청의 유효성 검증

4

DATA BOUNDARY

NO CENTRAL BIOMETRIC
DB

얼굴 이미지·Template·Embedding
을 서비스 서버와 분리

핵심 구조: Face + Card + Cryptographic Proof를 결합하여 신뢰를 검증

Tap → Face → Challenge → Verified

사용자 인증은 NFC 기반 카드 접촉, 1:1 얼굴검증, 서버의 Challenge 검증 순서로 구성됩니다.



개발자가 연동하는 인증 인터페이스 예시

`authenticate()` `authorize(transaction)`

얼굴인식 소프트웨어의 기술 적용 영역

동일한 인증 구조를 온라인·모바일·Enterprise·물리적 접근 환경에 확장할 수 있습니다.

01

Enterprise Zero Trust

VPN · 관리자 · 서버 · ERP

중요 자원 접근 시 사용자 Identity를 추가 검증

02

Financial / Transaction

고액송금 · 중요거래 · 기업금융

로그인 이후 거래 주체를 다시 검증

03

Medical / Sensitive Data 환자·의료진 본인확인

민감정보 접근에 강한 Identity 검증 적용

04

IoT / Physical Access

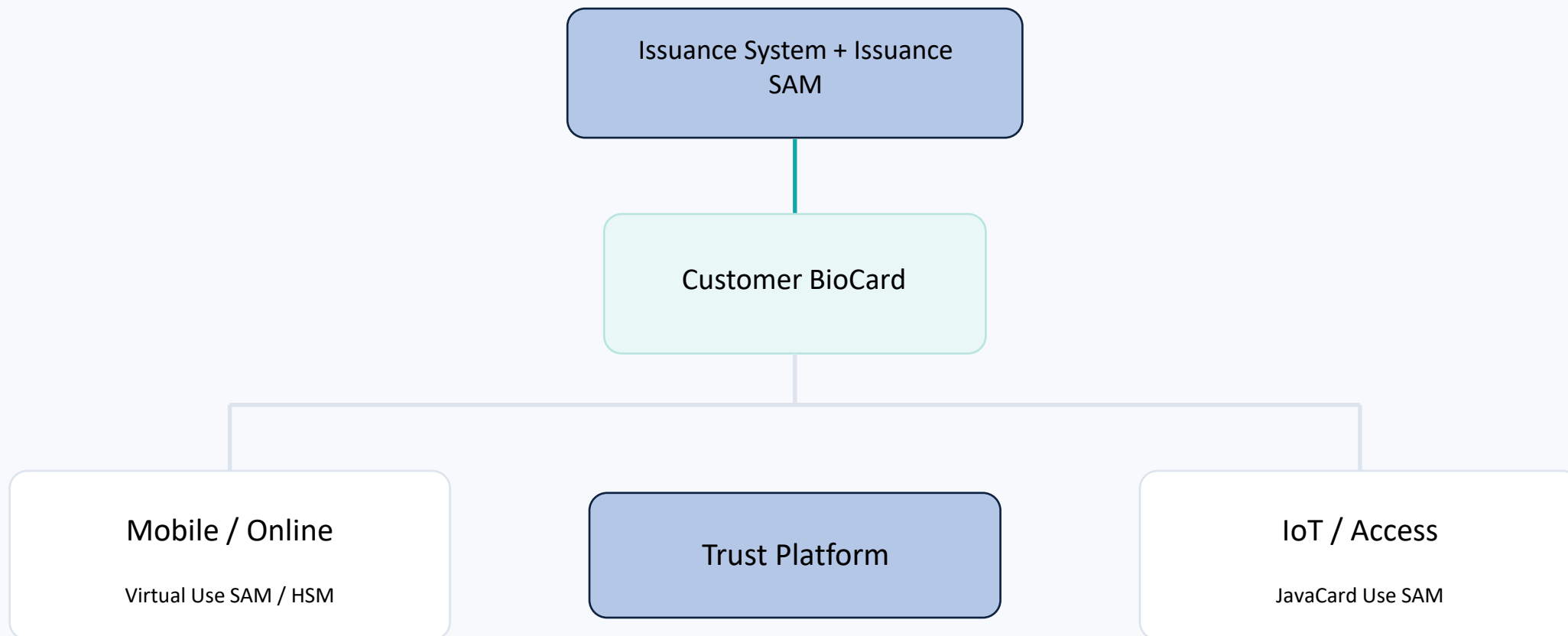
데이터센터 · 연구소 · 차량 · 출입통제

디지털 Identity를 물리적 접근으로 확장

공통 기술 목표: 사용자·기기·요청마다 인증 상태를 검증하고 최소 권한으로 서비스를 허용

발급과 사용을 분리한 Trust Infrastructure

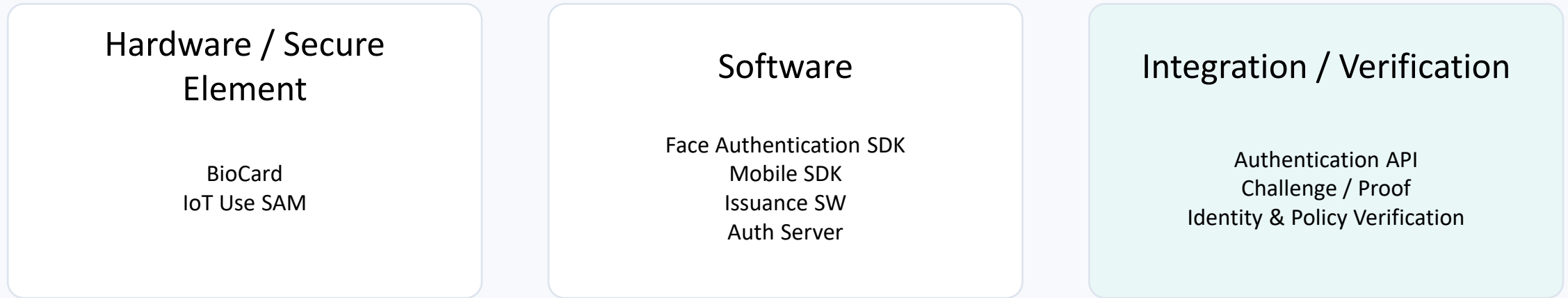
발급 영역과 사용 영역의 키·보안 역할을 분리하여 Mobile, Online, IoT 환경에 동일 Identity를 적용합니다.



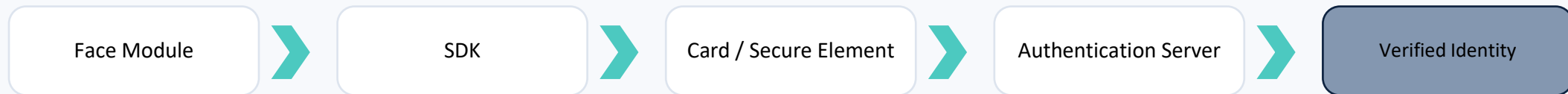
기술적 핵심: 발급키와 사용키의 역할을 분리하고, 인증에 필요한 키와 생체정보의 경계를 관리

소프트웨어 구성 요소와 연동 계층

얼굴인식 모듈, Mobile SDK, 발급 시스템, 인증 서버가 각각의 역할을 수행하도록 계층화합니다.



Integration Flow



구성 요소를 분리함으로써 기존 애플리케이션에 얼굴인증·Zero Trust 계층을 단계적으로 통합할 수 있습니다.

기술 검증을 위한 PoC 구성

기존 인증 시스템을 유지한 상태에서 얼굴인증과 Zero Trust 검증 계층을 추가하여 기술 적합성을 검증합니다.

Phase 1

Identity Verification

Face 1:1 Matching
Card / Secure Key
Challenge / Proof

Phase 2

System Integration

Mobile SDK
Authentication API
IAM / Access Control

Phase 3

Operational Verification

인증 성공률
응답시간
통합 난이도
보안·개인정보 요구사항

PoC에서 확인할 핵심 항목: 얼굴 1:1 검증 → Card 검증 → Challenge/Proof → 서버 정책 검증의 전체 체인

BIOCARD

Zero Trust Face Authentication

얼굴정보를 중앙에 모으지 않고도 Identity
를 검증하는 기술 구조

✓

Face Template을 사용자 측에 보관

✓

Face + Card + Cryptographic Proof 결합

✓

서버에는 검증 가능한 Assertion을 전달

BioCard · Privacy-First Biometric Identity Platform

TECHNICAL POC

Face Authentication
Zero Trust

Mobile · Online · IoT · Access