

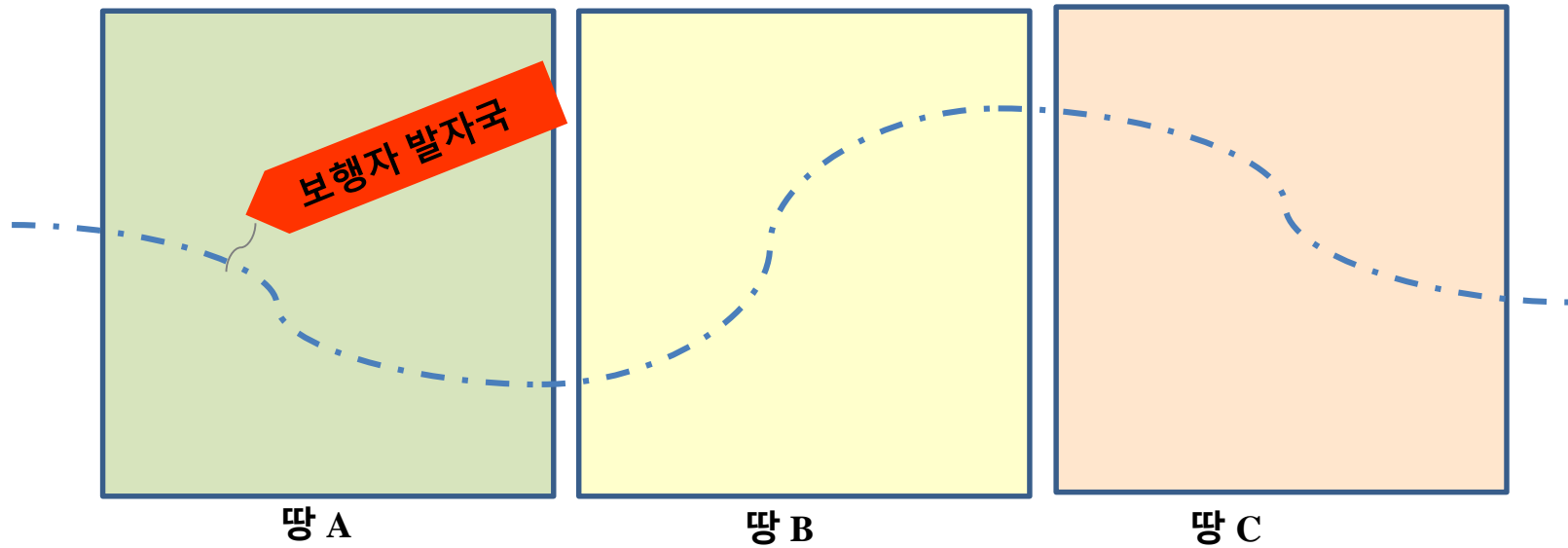
DID 기반의 전자증명 서비스와 마이 데이터

2019.11.

SKT 블록체인/인증 Unit 이미연

1. 마이 데이터 사업의 이슈들
2. DID란
3. DID 기반의 전자증명 서비스

발자국의 주인은 땅주인인가? 발주인인가?



“합법적으로 수집한 개인정보라면 비식별 조치 후 이용하는 것이 가능하고
이 경우 정보주체의 동의를 받지 않아도 된다.”

– 개인정보 가이드라인

현재는 사전 동의와 비식별화를 통해
땅주인(서비스 주체)이 개인정보를 활용하고 있음

규제도 문제이지만 개인이 자신의 정보에 접근/보관/처리
할 수 있는 **루트가 없는** 것이 더 큰 문제임

- “개인정보란 살아 있는 개인에 관한 정보로서 특정한 개인을 알아 볼 수 있는 정보 또는 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보를 의미한다.”
– 정보통신망법(제2조 제1항 제6호), 개인정보보호법(제2조 제1호)
- “개인정보의 처리란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄) 및 그 밖에 이와 비슷한 행위를 말한다.”
– 개인정보보호법(제2조 제2호)

개인이 사회생활을 하면서 다양한 기관들과 관계를 맺고 형성하게 되는 개인의 중요정보들은 각 기관의 데이터베이스에 존재하며, 필요시 각 기관-기관의 서버를 통해 공유되고 있음

서비스 이용정보의 종류

- 개인식별정보
(주민번호, CI, ID/PW)
- 서비스 가입정보
- 서비스 이용정보
- 개인위치정보
- 분석데이터
 - 고객 등급
 - 고객 취향
 - 구매 의향

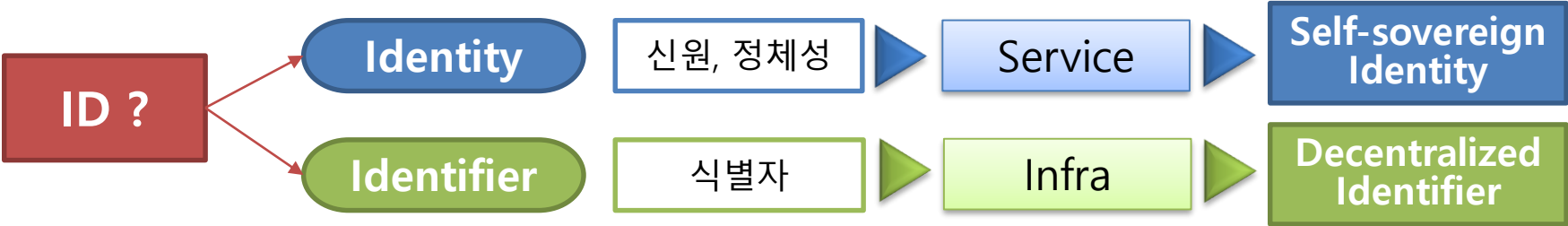
개인정보 취급처

- 정부 (부처)
- 지자체
- 공공기관, 협회
- 소속학교
- 소속회사
- 은행
- 병원
- 각종 서비스 회사
- ...

**개인정보를 각 기관끼리 알아서 전송/공유/활용하고 있다
→ 개인의 정보주권을 개인에게!!**

1. 마이 데이터 사업의 이슈들
2. DID란
3. DID 기반의 전자증명 서비스

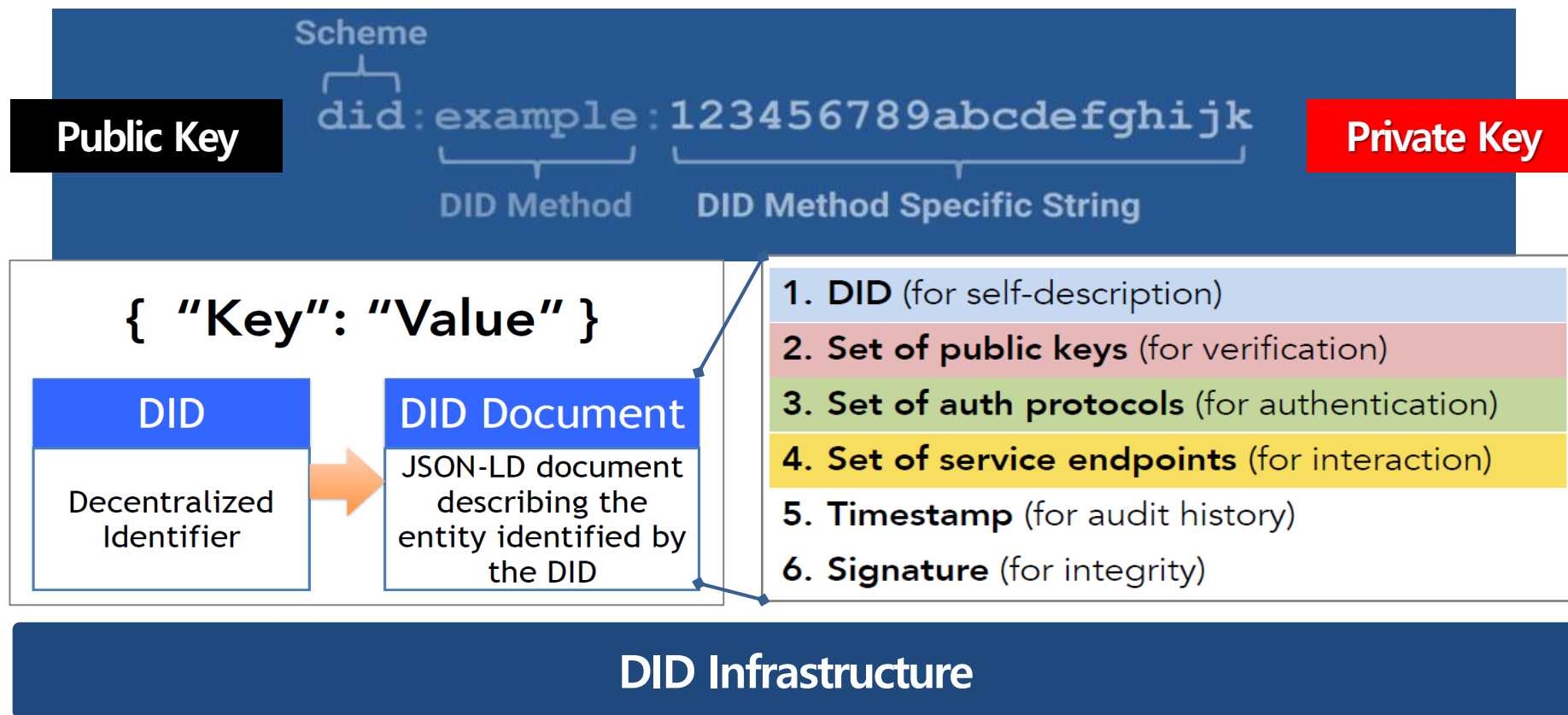
ID와 Identifier(식별자)



	인식방식	소유증명 방식	생성방식	사용 방식	활용 예
기존 ID	Human readable, memorable	Password로 소유 증명	중앙에서 생성 관리	직접 입력	단순 로그인
DID	Machine readable	Private key로 소유 증명	분산환경에서 스스로 생성	Wallet을 통해 제시	로그인, 전자서명, message 암호/복호화

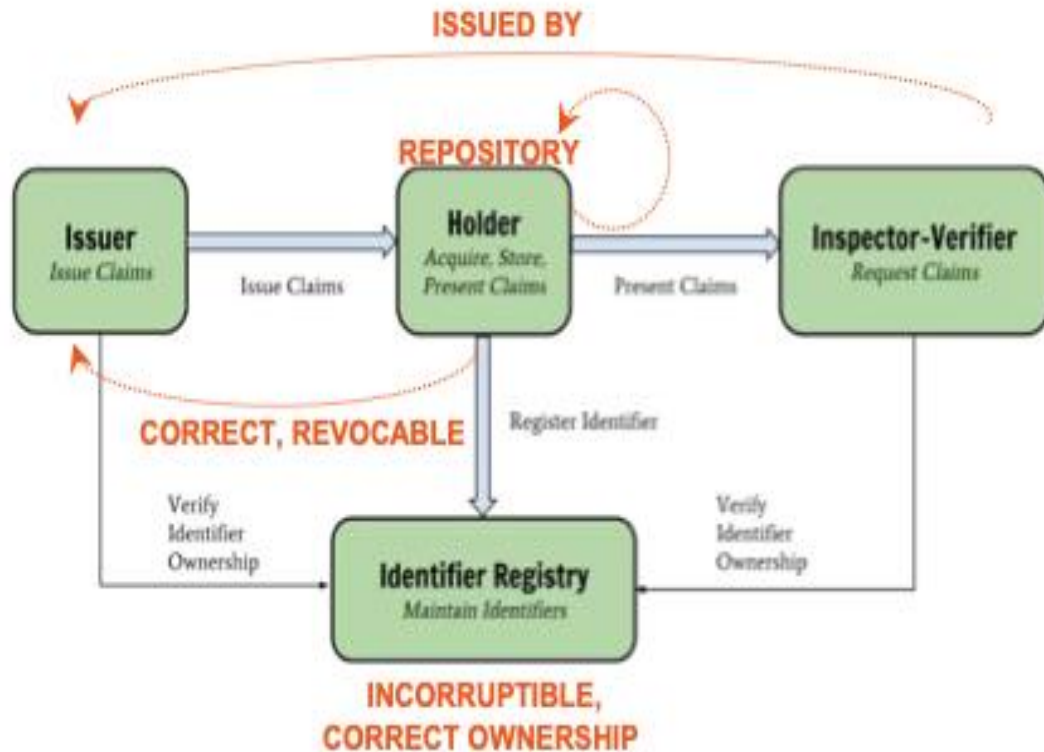
분산 식별자(DID-Decentralized Identifier) 'DID'란?

'분산 식별자(DID)'란 공개키 인프라를 기반으로 하는 새로운 유형의 고유 식별자로서 탈중앙화 방식의 신원 관리를 지원 하며 개인뿐만 아니라 기관과 사물의 식별에도 적용 가능



DID 메커니즘

다양한 증명정보 발급기관과 정보이용기관이 개인을 매개로 N:1:N으로 연계, 확장성을 담보함
사업자와 출입보안회사 간의 DB 연동을 끊고, 개인이 자신의 정보를 단말에 보관하며 필요시 제3자(출입보안회사)에게 정보를 전송하는 방식으로 정보의 흐름을 바꿈






증명정보 발급기관과 정보이용기관 간
시스템 연계를 끊고,

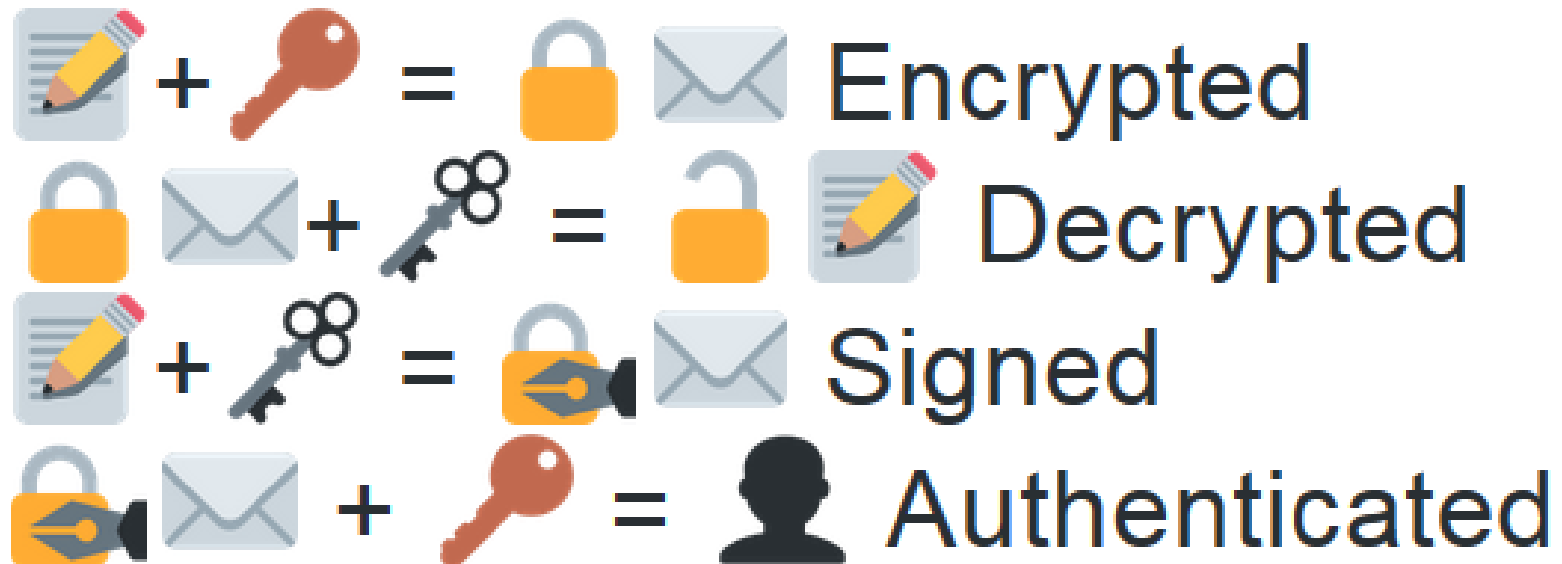
개인이 자신의 중요정보를
단말에 직접 보관하고 관리하고,

개인이 제3자에게 제시하는 정보에
대해 검증할 수 있는 도구와 체계를
블록체인 상에서 오픈하여 제공한다

진본임을 수학적으로 증명하는 방식

내가 제출한 데이터가 원본임을 증명하는 방식으로 PKI¹⁾ 방식(비대칭 전자서명) 같은 암호학적인 증명방식을 활용

 Public Key
 Private Key
 Message



1) Public Key Infrastructure 공개키 기반 구조

블록체인 원장 내 저장 내역

블록체인 원장에는 증명발급기관(Issuer)가 발행한 증명서(Credential)를 누구나 검증할 수 있도록 검증에 필요한 데이터들이 저장하고 공유

DID Document

DID의 공개키(Public Key), 서비스 엔드포인트(Service Endpoint), PKI Meta Data 등

Schema Definition

증명서(Credential) 내 Claim의 속성 스키마(Attribute Schema) 정의 (여러 증명발급기관 간 공통으로 사용 가능)

Credential Definition

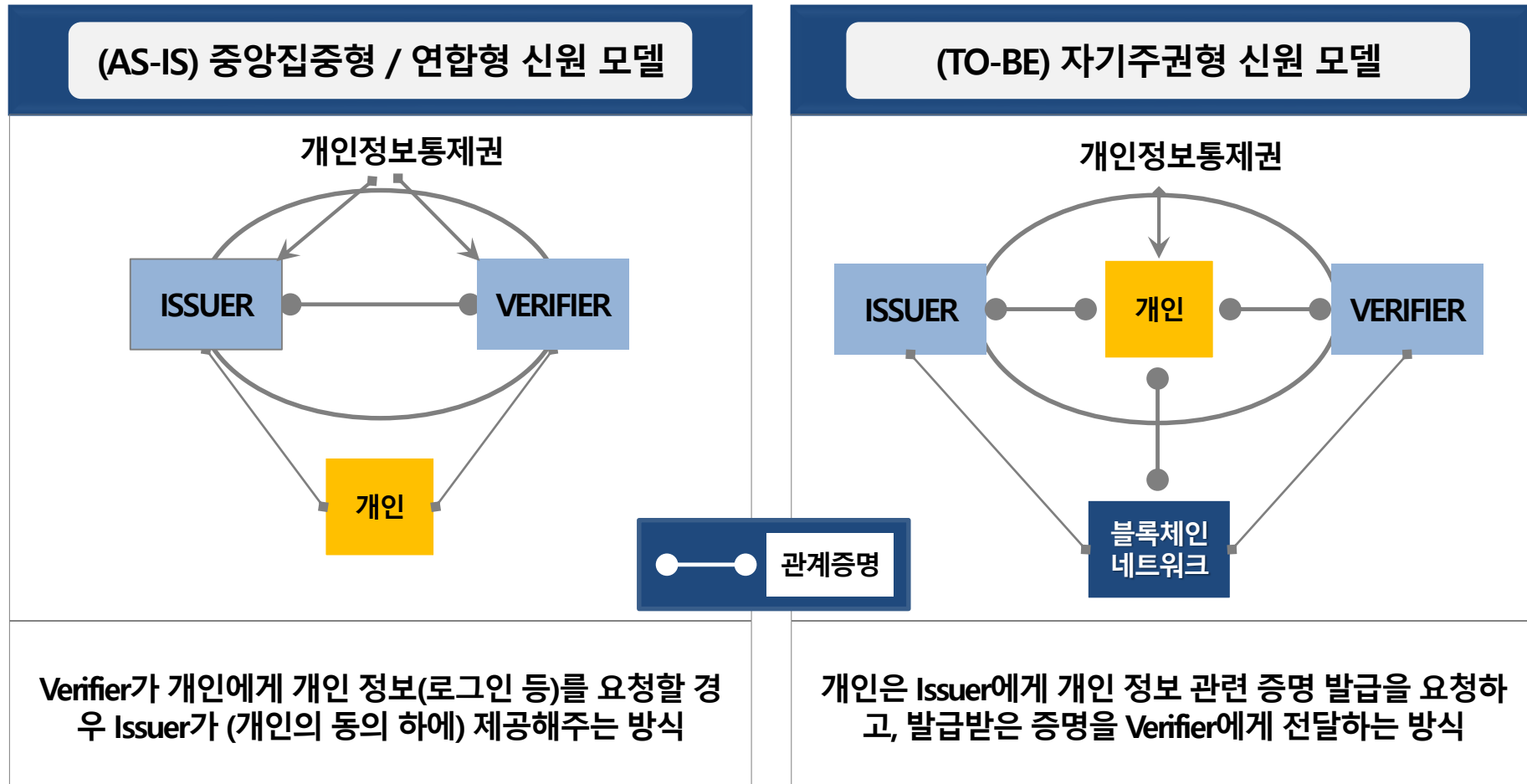
증명발급기관(Issuer)가 발행하는 '검증가능한 증명서(Verifiable Credential)'에 대한 정의로서 동일한 스키마를 사용하더라도 Issuer는 각 Credential Definition 생성 필요

Revocation Accumulator

증명서(Credential) 유형별로 증명서 폐기(Revocation) 여부 검증을 위해 증명발급기관(Issuer)이 계산하여 갱신하는 값으로서, 증명서 폐기 상황 발생시마다 재계산 후 갱신

Self-Sovereign Identity 'SSI'란?

자기주권신원 모델이란 기업이 개인정보를 보관하고 유통하는 방식에서, 개인이 직접 개인정보와 본인에 대한 증명을 유통하는 방식



나의 중요 증명정보를 내 손 안에!

나의 '생애이력정보'

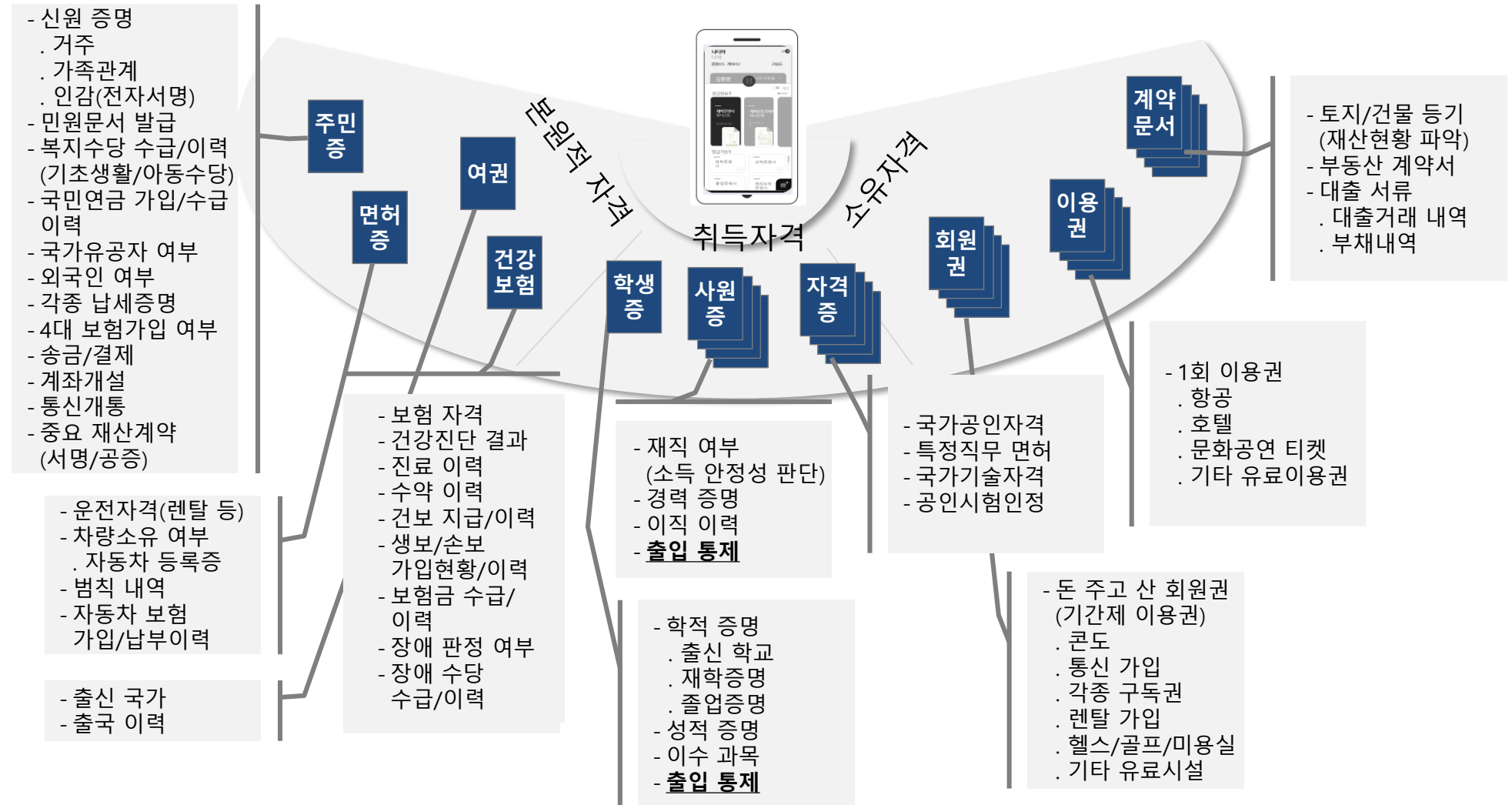
- 출생
- 가족
- 주소
- 재학/학력
- 재직/경력
- 납세이력,
대출상환이력
- 재산 명의정보
(동산/부동산)
- 주거래 계좌정보
- 자격증, 면허증
- 건강기록
- 상벌사항

....



내 정보를
제공/판매하는 주체도
'나'

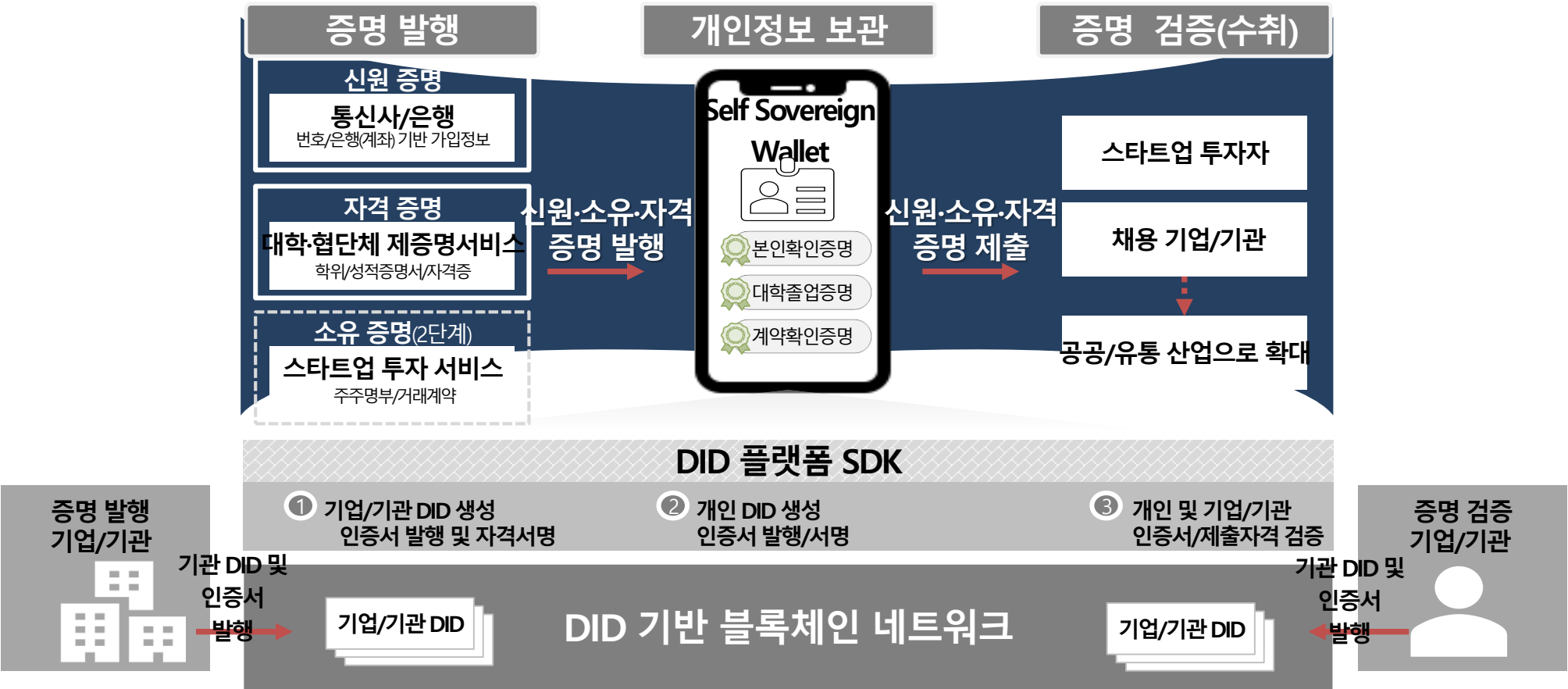
'증' 기반의 다양한 증명정보들



1. 마이 데이터 사업의 이슈들
2. DID란
3. DID 기반의 전자증명 서비스

전자증명 서비스의 개요

전자증명 서비스는 DID 기술 기반의 블록체인 네트워크와 플랫폼 SDK를 통해 다양한 증명서의 발행과 검증을 지원하는 서비스로 구성



SKT 전자증명 서비스 주요 기능

자기주권 지갑 서비스는 다양한 증명서를 모바일 단말에 발급받고 제출하는 기능으로 구성되며, DID 서명 기능을 활용한 전자계약서 서비스도 지원

1. 전자증명서

발급 완료한 증명서의 자세한 내용 및 상태를 조회하고 관리 가능

2. 증명서 선택

필요한 증명서를 선택하여 발급 신청하는 기능

3. 발행기관 선택

기관을 선택하여 발급이 가능한 증명서를 신청하는 기능



4. QR 스캔

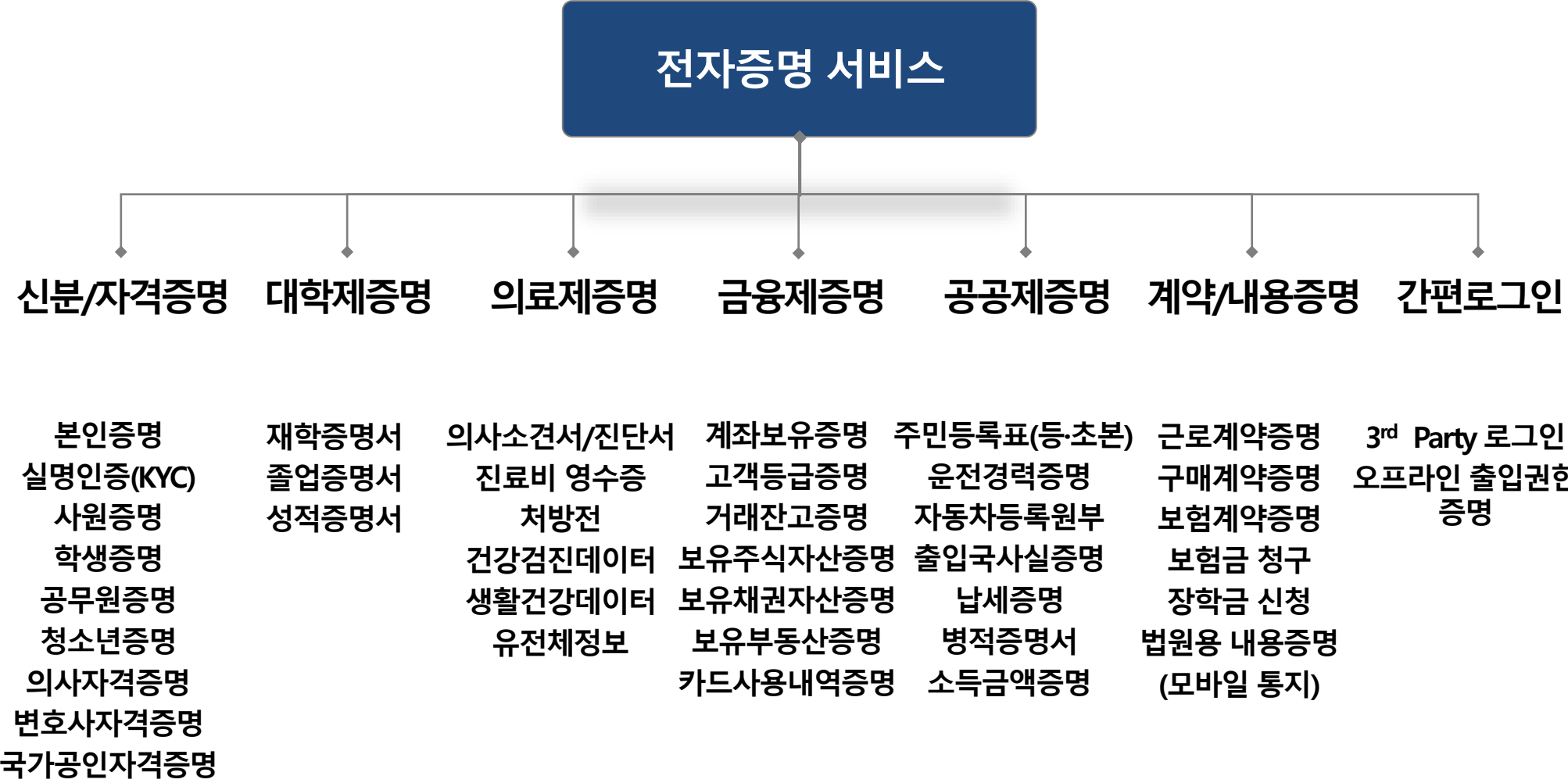
QR스캔 기능으로 기관과 연결하여 증명서를 발급/제출하는 기능

5. 전자계약서

전자계약서를 DID로 서명 후 모바일 내에서 관리 기능

6. 리워드 쿠폰

행위에 따라서 OTX로 교환 가능한 리워드 발행 기능



은행

- 주요 기업 재직증명 기반의 대출상품 서비스
- 전문가 자격증명 기반의 대출상품 서비스

카드

- 은행 보유자산 기준 우수고객등급 대상 VIP 카드발급 서비스
- 전문가 자격증명 기반의 VIP 카드발급 서비스
- 통신사 간편 신용증명 기반의 카드로론 서비스

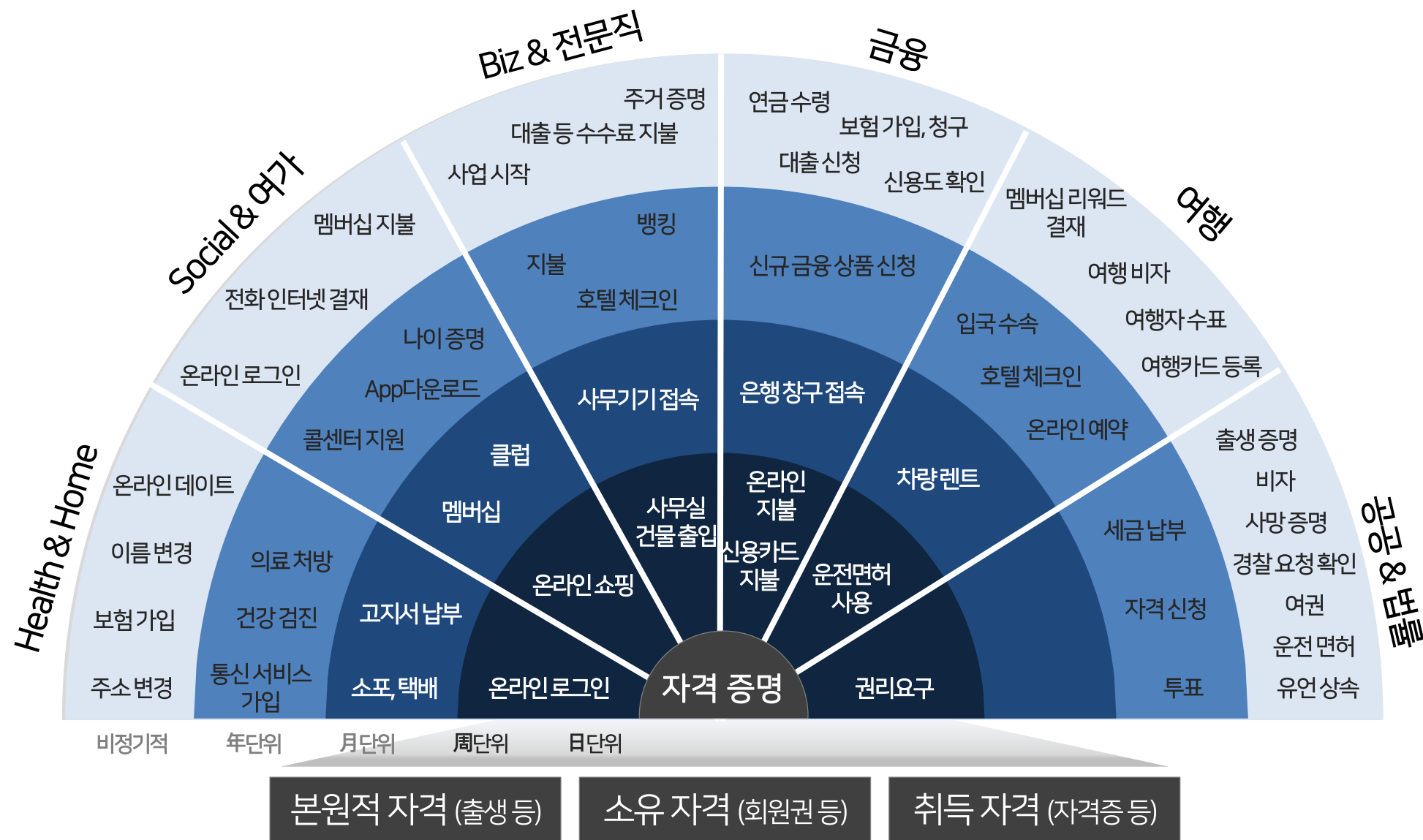
증권

- 은행 보유자산 기준 우수고객등급 대상 WM(Wealth Management) 상품 Offering
- 투자자의 투자선호/ 포트폴리오 증명 기반의 금융투자상품 Offering

보험

- 모바일 병원/약국 영수증 및 처방전 기반의 보험금 신청/지급 서비스
- 건강증진활동 증명 기반의 건강보험 할인 서비스

DID 기반의 증명(Credential) 혁신 시대의 개막



감사합니다.