블록체인 응용사례 #2

Blockchain Case Study - DID

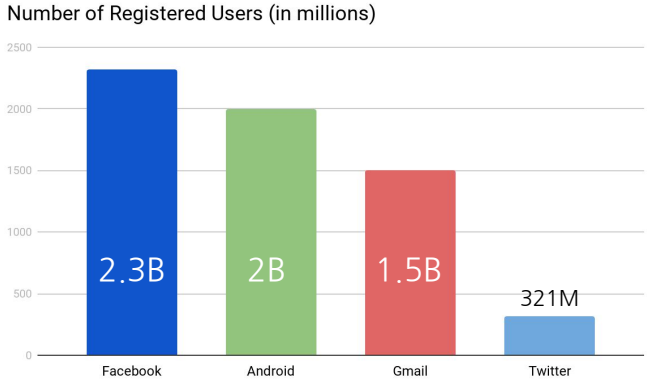
목차

목차

사일로(Silo)화된 중앙형 ID 시스템

인터넷은 사용자 중심으로 설계되지 않았음. 인터넷 사용자들은 서비스를 사용하기 위해 서비스가 생성하는 어카운트를 사용해야 하며 어카운트에 기록된 정보를 바탕으로 본인을 인증해야만 함.

- 현재의 ID 시스템은 사용자가 서비스/앱 별로 (서비스가 관리하는) ID를 빌리는 형태
- 서비스는 사용자의 개인정보를 DB에 저장하는데 서비스가 확장해감에 따라 사용자 정보가 누적되고 이것이 사일로화됨
- 사일로로 인해 해킹의 위협은 물론 데이터를 올바르게 관리해야하는 책임이 발생, 이는 곧 비용으로 이어짐
- 최근 서비스들이 사일로에 쌓인 데이터를 오용하는 사례가 다수 발생

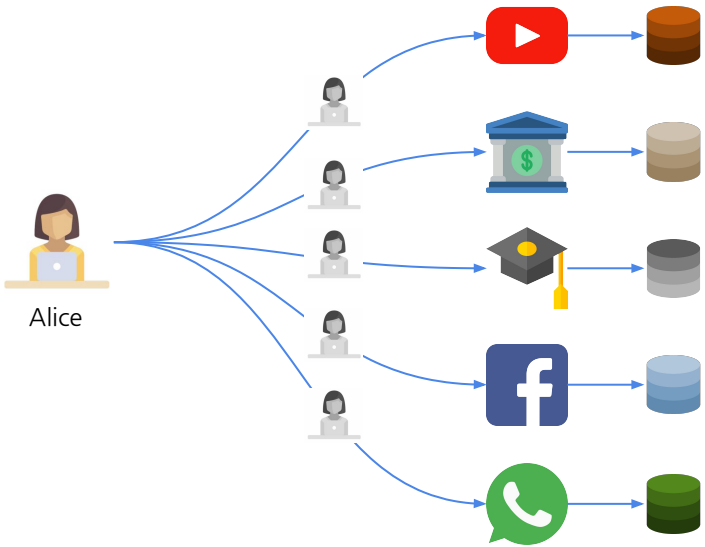


그래프 1. Facebook, Android, Gmail, Twitter가 사용자수. Android 사용자수는 Google Play Store 사용자 숫자로 대체

사일로의 문제

사용자 측면

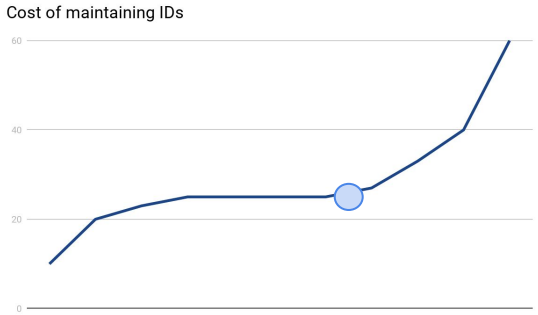
1. 데이터 파편화
2. 데이터 주권 행사 불가



서비스 측면

사용자 증가에 따라 다음과 같은 이유로 중앙화된 ID 시스템의 관리비용이 빠르게 증가:

1. 신규 사용자에 따른 비용
2. 데이터 보호, 관리 규제를 따르는데 발생하는 비용



그래프 2. 초기 어느 기간동안은 사용자 증가가 매출 증가로 이어지지만 데이터가 누적됨에 따라 해킹의 위협, 규제 대응으로 인한 비용이 크게 증가함.

목차

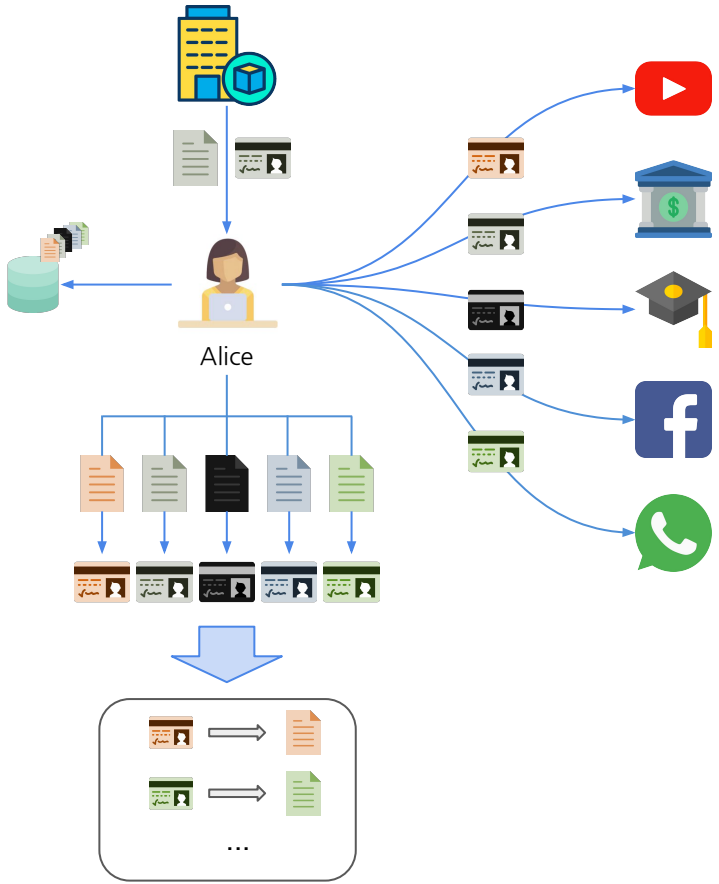
DID란?

Decentralized ID (DID)는 블록체인과 같은 탈중앙화된 네트워크에 등록된 유니크한 식별자(ID)로 **ID의 등록함에 있어서 중앙화된 서버를 필요로 하지 않고 그 자체로 검증 가능(Verifiable)한 특징을 가짐**. 등록과 사용과정에서 중앙화된 체계를 필요치 않기 때문에 탈중앙화(Decentralized) 되었다고 표현.

데이터 소유권자 Alice는 자신의 정보를 노출하지 않고 자신이 정보를 소유하고 있음을 DID를 사용하여 증명. Alice는 원하는 만큼 많이 DID를 생성 또는 기관으로부터 발급받을 수 있음.

DID는 정확히 DID 문서 (DID Document)의 식별자로써 기능. DID 문서는 DID가 가리키는 정보가 무엇인지, 문서의 검증은 어떻게 하는지 정해진 프로토콜에 따라 상세히 기술.

DID를 사용하면 **자기자신을 또는 자신의 정보를 인증하는 과정에서 실제 정보를 노출할 필요가 없어짐**. 유효한 운전면허증을 가지고 있다는 사실을 증명하는 것이지 운전면허증에 기재된 정보를 공개할 필요가 없는 것과 같은 맥락.



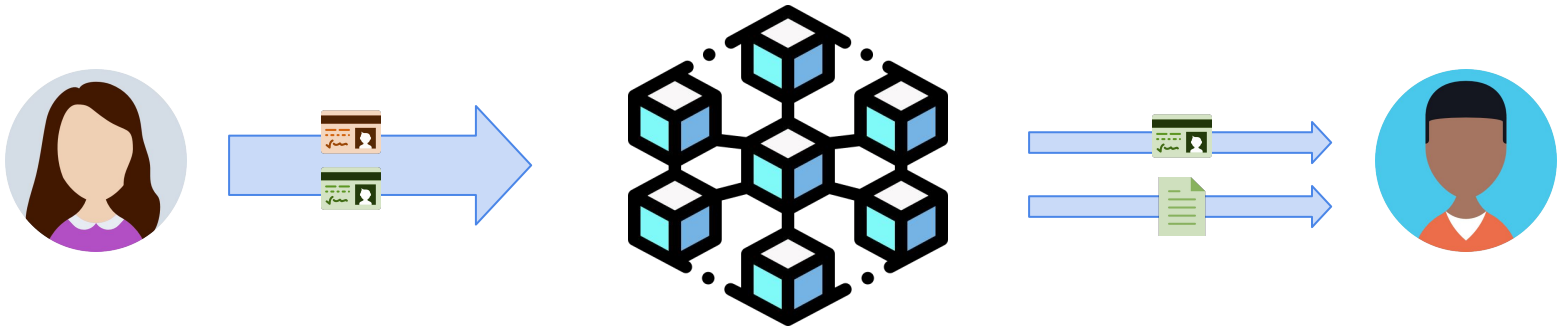
DID와 블록체인의 관계

퍼블릭 블록체인은 (1) 누구나 쓰고 읽을 수 있고 (2) 한번 쓰여진 기록은 위변조가 어려움.

이러한 성질을 사용하여 다음을 블록체인에 기록:

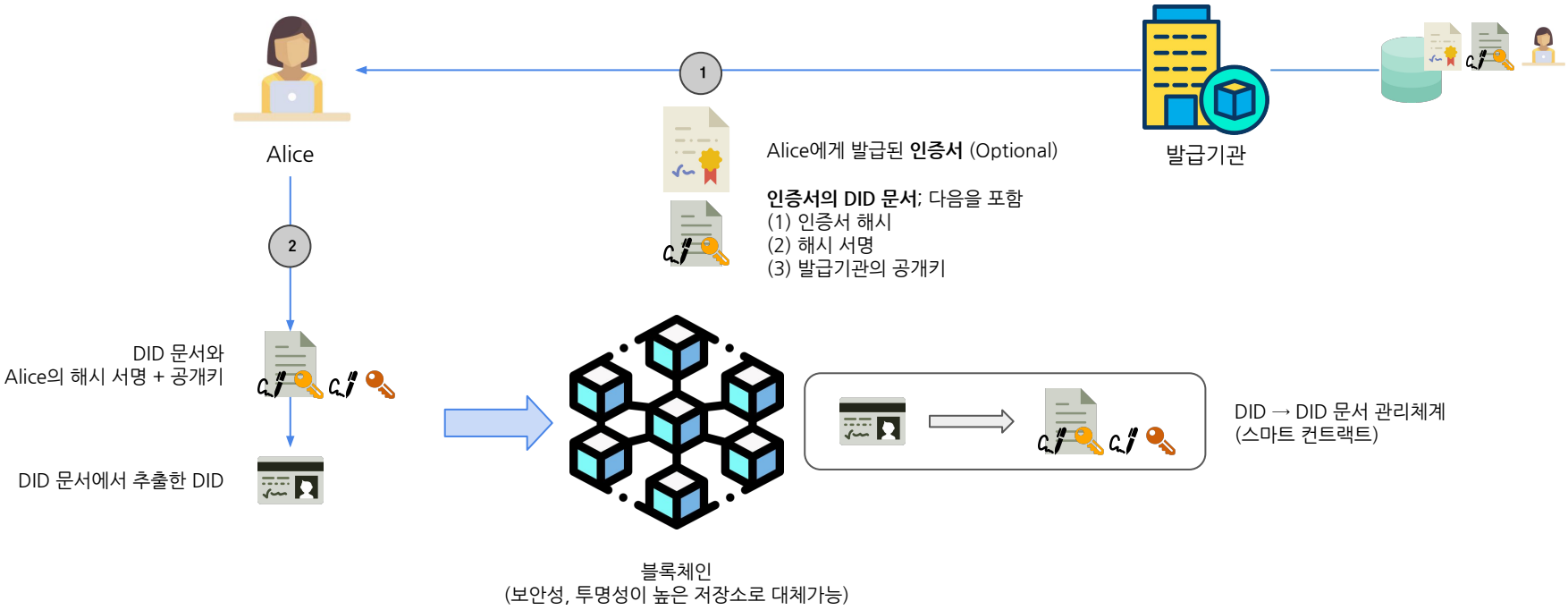
- (사용자 또는 기관 등이) 발급한 DID를 검증할 수 있는 공개키
- DID와 DID 문서

블록체인에 위 정보를 기록함으로써 신뢰할 수 있는 제 3자의 필요성을 없애고
누구든지 **DID의 (1) 진위여부와 (2) 소유권 확인**을 할 수 있도록 한다.

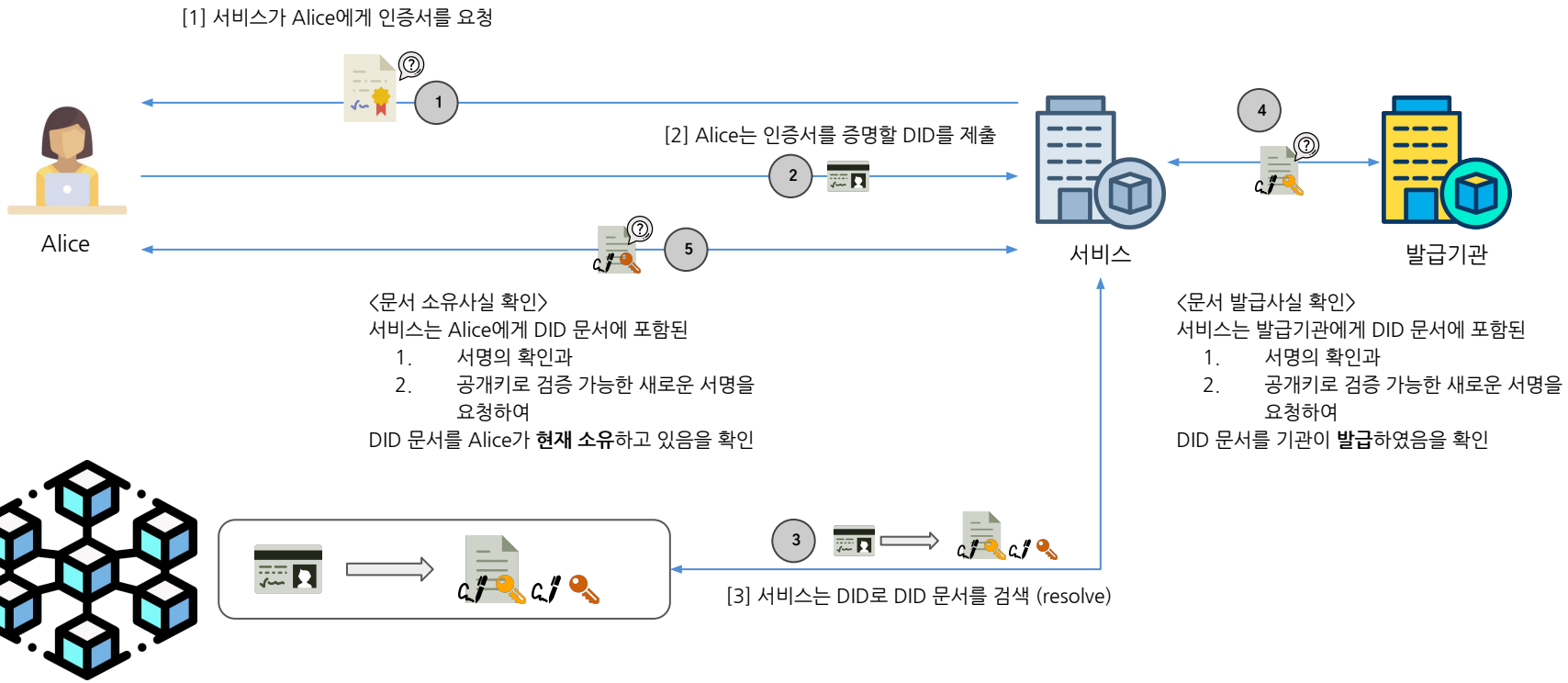


목차

예 1-1: 기관이 발급한 DID의 배포 (Publishing)

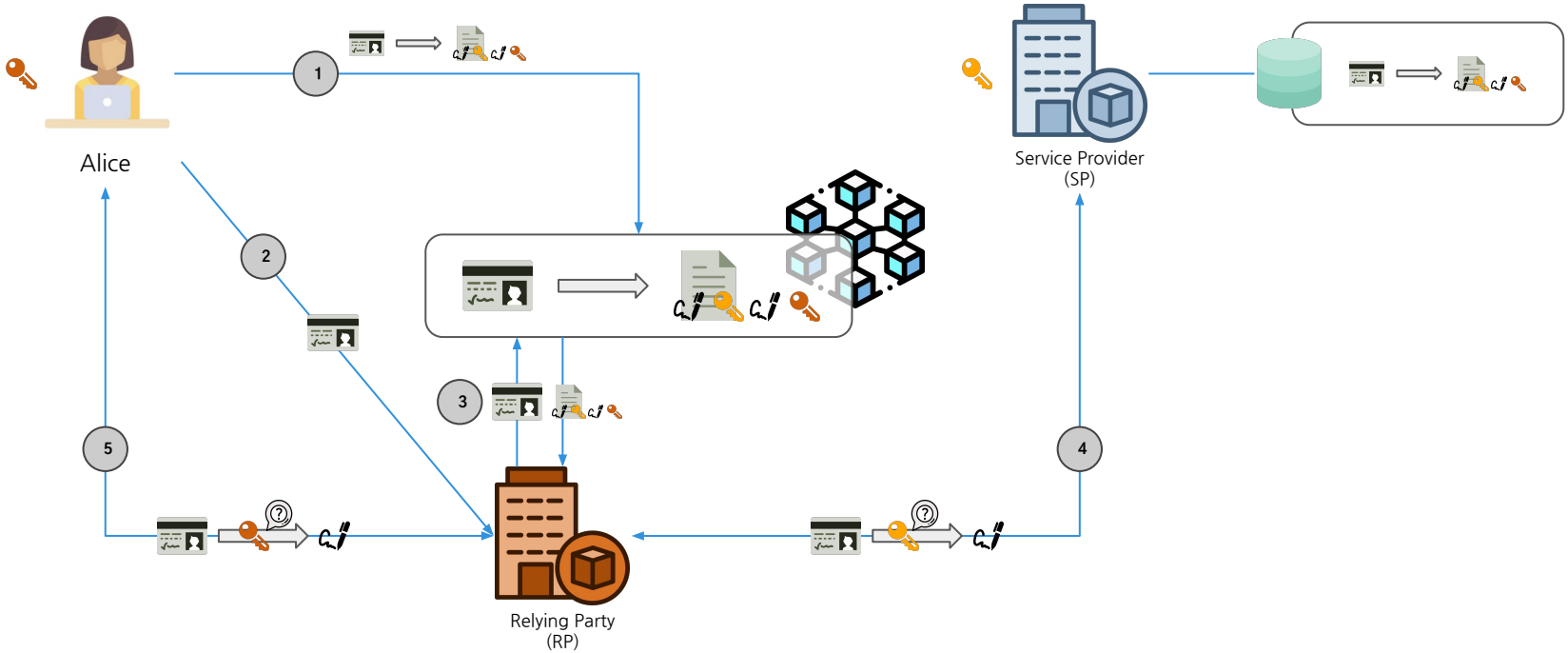


예 1-2: 기관이 발급한 DID의 사용 (Validating)

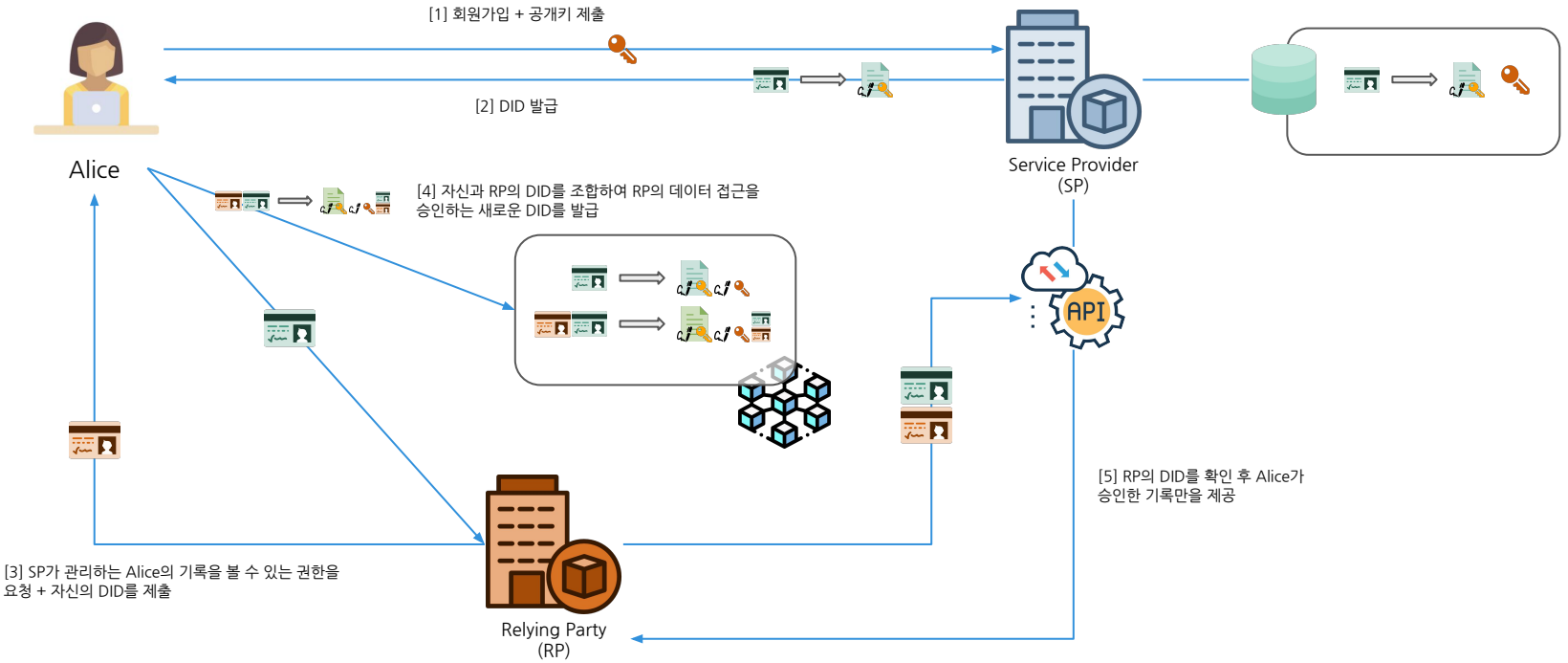


예 2-1: DID로 구현된 Authentication (AuthN)

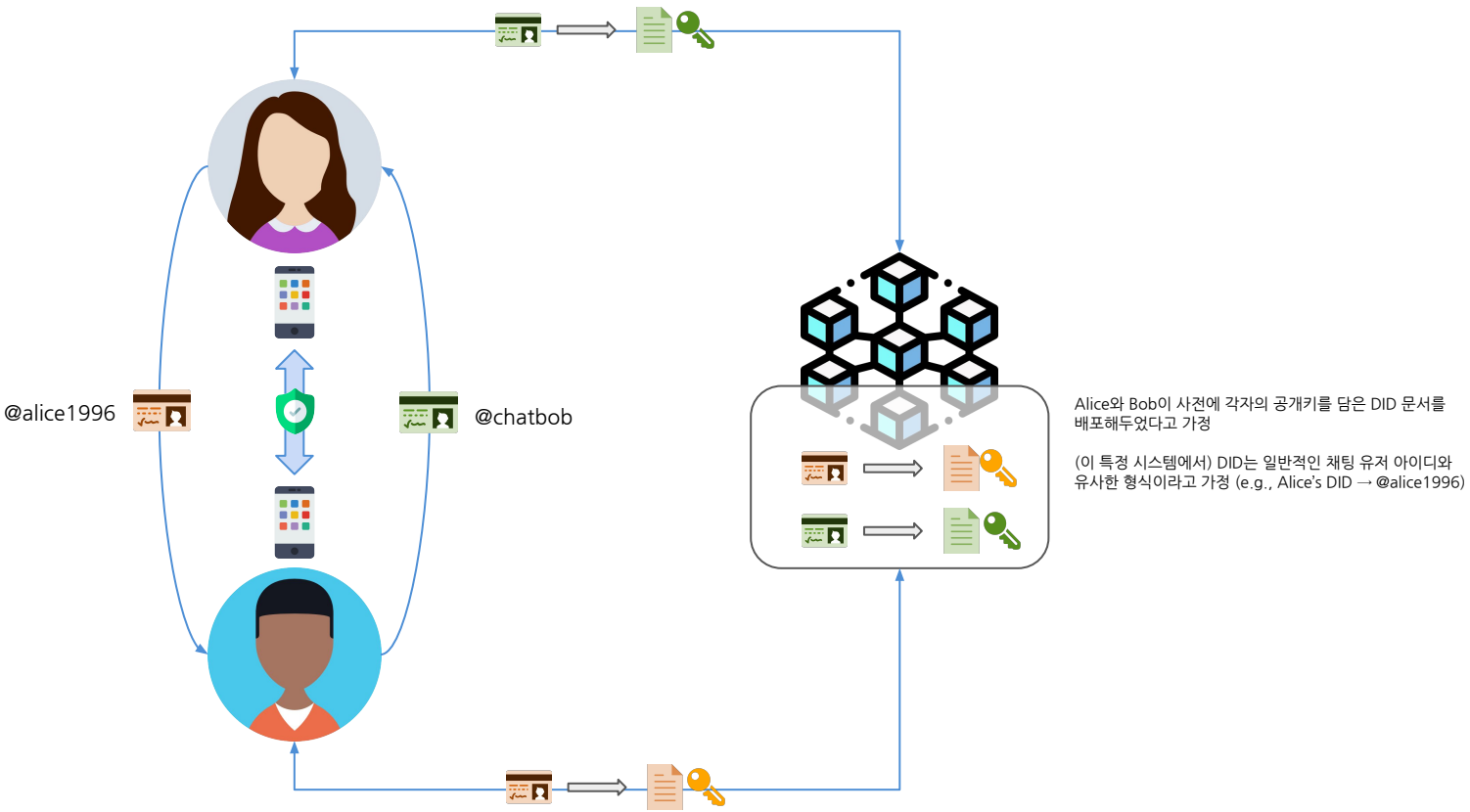
DID를 사용할 경우 공개키 기반의 소유권 증명(attestation)으로 AuthN을 구현하여 기존의 OpenID를 대체



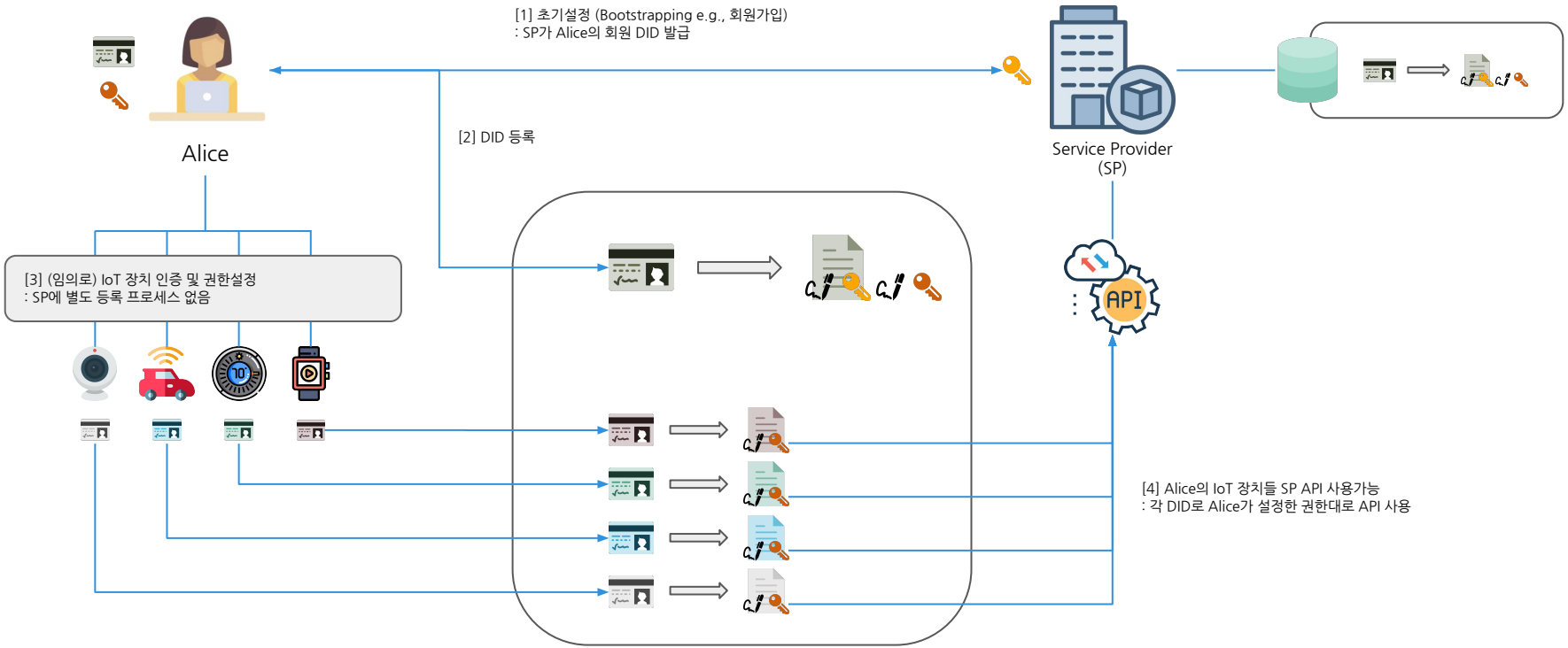
예 2-2: DID로 구현된 Authorization (AuthZ)



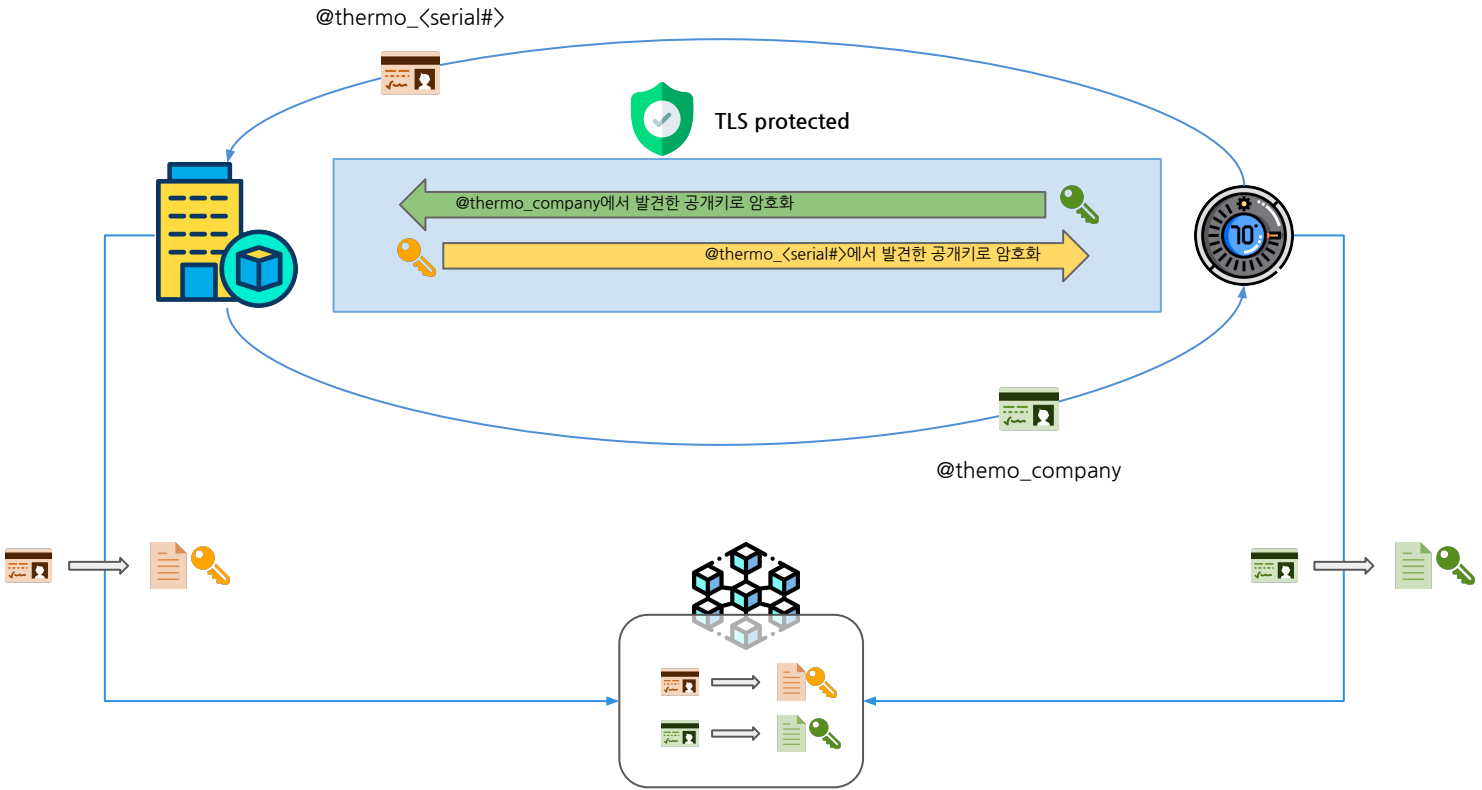
예 3: DID를 사용한 안전한 P2P 통신을 위한 키 교환



예 4: IoT AuthN + AuthZ using DID



예 5: TLS Certificates for IoT Clients (예3의 IoT사례)



End of Document