# 영지식 증명

https://youtu.be/6PCkqxn_L5A

# 영지식 증명

- Zero-Knowledge Proof, ZKP
- 주로 암호화폐에서 개인정보를 보호하는데 사용
- 증명자(Prover)는 검증자(Verifier)에게 **‘자신이 정보를 알고 있다’**라는 사실만을 검증 받음
- 대화형 증명 시스템에 기반

# 대화형 증명 시스템

- Interactive Proof System
- 증명자와 검증자로 구성됨
- 증명자는 특정 명제를 자신이 증명할 수 있다고 주장
- 검증자는 이에 대해 yes or no의 답변을 받아냄
- 증명자 계산량에는 제한이 없으나, 검증자 계산량에는 제한이 존재

# 대화형 증명 시스템

- 증명자 P는 명제 x에 대해 $x \in L$ 임을 증명
- P와 V가 명제 x를 받음
- P는 x에 대해 계산 후 결과 $\pi$를 V에 보냄
- V는 $\pi$를 보고 $x \in L$ 이라고 생각되면 yes, 아니면 no를 말함

# 대화형 증명 시스템

- 대화형 증명 시스템은 ‘완전성’과 ‘건전성’을 만족하여야 함

- 완전성 (Completeness)
  - $x \in L$일 경우, P가 보낸 $\pi$를 보고 V는 $x \in L$이라고 판단해야 함

- 건전성 (Soundness)
  - $x \notin L$일 경우, P가 무슨 시도를 해도 V는 $x \notin L$이라고 판단해야 함

# 대화형 증명 시스템

- ‘증명자와 검증자가 서로 메시지를 교환하는 계산’을 모델링한 추상적 컴퓨터 모델
- 증명자는 전능하며 무제한의 계산 자원을 가지고 있으나 신뢰할 수 없음
- 검증자는 제한된 자원을 가지고 있으나 신뢰할 수 있음

# 대화형 증명 시스템

- 대화형 증명 시스템에서는 주로 증명자가 악역을 담당한다고 가정

- 만약 검증자가 악역이라면?

# 영지식 증명

- 누구나 검증자가 정보를 누설하지 않는다는 것을 확인할 수 있는가?
- 검증자가 검증하는 과정에서 알고 있어야 하는 정보의 비중은 어느 정도인가?
- 증명자가 제공한 정보를 통해 검증은 가능하지만 정보 자체의 유추는 불가능해야 함

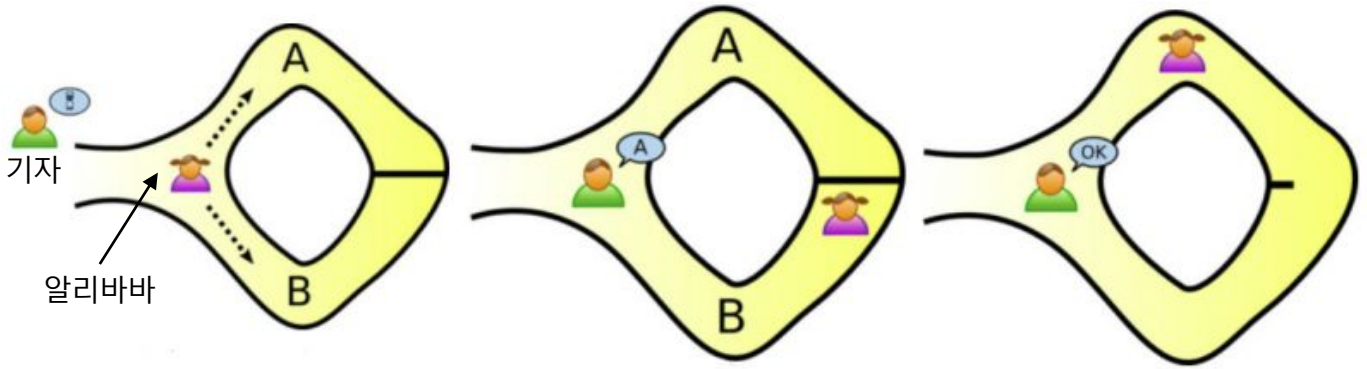
-> 이것에 대한 해결책으로 영지식 증명 등장

# 영지식 증명의 조건

- 완전성 (Completeness)
  - 조건이 참일 경우, 검증자는 증명자의 증명을 납득할 수 있어야 함
- 건전성 (Soundness)
  - 조건이 거짓일 경우, 증명자는 검증자를 절대 납득시킬 수 없음
- 영지식성 (Zero-Knowledge)
  - 조건이 참일 경우, 검증자는 그 조건이 참이라는 것 외의 아무 정보도 알 수 없음

# 알리바바와 동굴

- 알리바바는 증명자, 기자는 검증자
- 알리바바는 자신이 문의 비밀번호를 알고 있음을 증명하고 싶지만, 비밀번호는 알리고 싶지 않음
- 알리바바는 A와 B 둘 중 하나로 들어간 다음 기자를 부름
- 기자는 갈림길까지 간 다음 알리바바를 특정 방향으로 나오라고 지시
- 알리바바가 그 방향으로 나옴



# 알리바바와 동굴

- 확률이 1/2밖에 되지 않음
  - 이 예시의 경우만 그럼

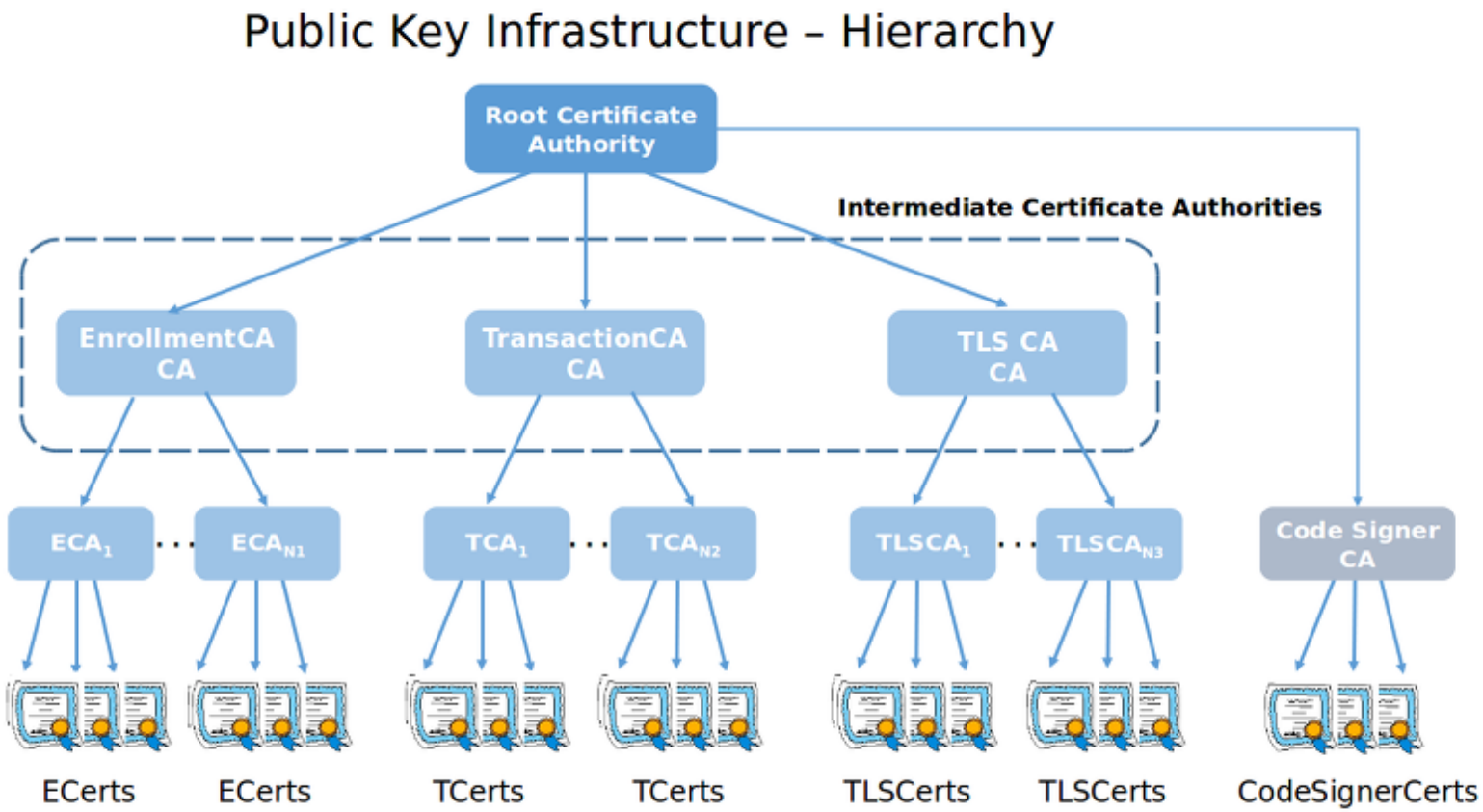
- 알리바바가 갈림길에서 A로 갔는데 기자가 A로 나오라고 할 수도 있음
  - 검증을 여러 번 반복함으로써 확률을 높임
  - 검증을 40번만 하여도 틀릴 확률은 1조 분의 1 이하가 됨

# 알리바바와 동굴

- 완전성
  - 모든 검증을 통과하면 기자는 알리바바가 비밀번호를 안다고 생각할 수밖에 없음
- 건전성
  - 알리바바가 비밀번호를 모를 경우, 언젠가는 틀리기 때문에 비밀번호를 안다는 것을 증명할 수 없음
- 영지식성
  - 기자는 알리바바가 비밀번호를 안다는 사실을 알더라도 비밀번호에 대한 정보는 얻지 못함

# 하이퍼레저 패브릭과 영지식 증명

- 하이퍼레저 패브릭 1.x 버전에서는 ECerts와 TCerts 사용



# 하이퍼레저 패브릭과 영지식 증명

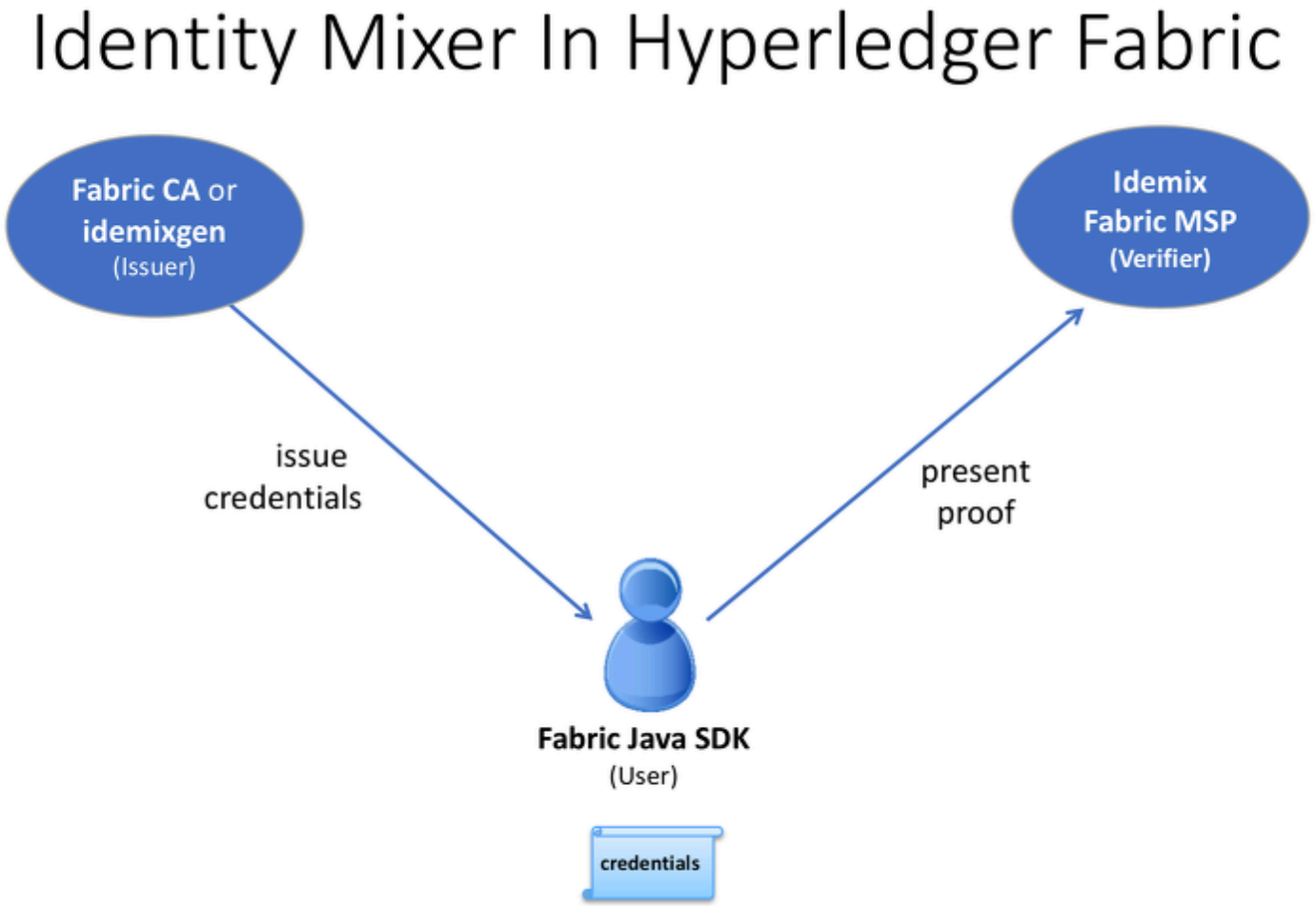
- Enrollment CA를 통해 네트워크에 사용자를 등록
- Transaction CA를 통해 사용자가 트랜잭션을 요청
- ECerts는 CA가 각각의 멤버 컴포넌트에게 등록에 사용하게끔 발행하는 인증서 자체
- TCerts는 CA가 사용자들이 트랜잭션 요청에 사용하게끔 발행하는 인증서 자체

# Identity Mixer

- 하이퍼레저 패브릭 1.x에서 사용되는 ECert의 사용자에 대한 신원증명서는 X.509 형식으로 구성
- 해당 정보를 CA로부터 발급받는데 세부정보가 전부 노출되어 있음
- 해당 신원증명서를 통해 트랜잭션을 호출하면 자신의 정보가 모두 노출될 가능성
- 신원증명의 일부를 제거하고 보내면 CA의 서명이 의미가 없어짐

-> Identity Mixer를 통해 이러한 문제 해결

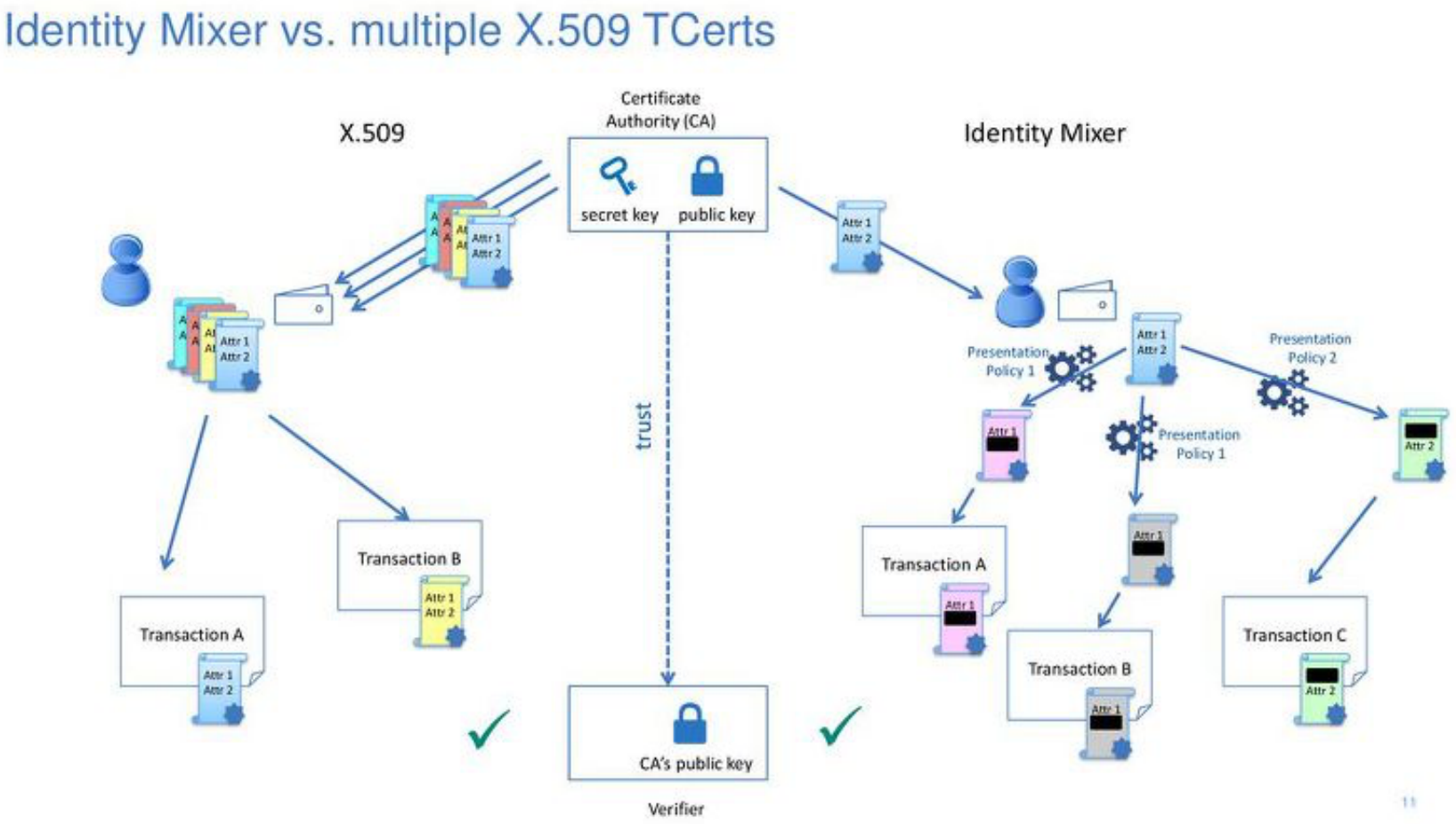
# Identity Mixer




크리덴셜 [kridénʃəl]
대략 "아이디(사용자명/계정) + 패스워드"
애플리케이션 등에서 사용하는 암호학적 개인 정보
https://zetawiki.com/wiki/%ED%81%AC%EB%A6%AC%EB%8D%B4%EC%85%9C

# Identity Mixer

- X.509 인증서는 매 트랜잭션마다 필요
- Identity Mixer는 한 번 받은 크리덴셜로부터 트랜잭션 실행



# Q & A