BIDaaS:

Blockchain Based ID As a Service

A64010 김현학

BIDaaS: Blockchain based ID as a service

JH Lee - IEEE Access, 2017 - ieeexplore.ieee.org

… The proposed blockchain-based ID as a service (**BIDaaS**) is explained with one practical example that shows how the proposed **BIDaaS** works as an identity and authentication …

☆ 저장 " 인용 134회 인용 관련 학술자료

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 29, 2017, accepted De
date of current version February 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2017.2782733

INVITED PAPER

BIDaaS: Blockchain Based ID As a Service

JONG-HYOUK LEE, (Senior Member, IEEE)
Department of Software, Sangmyung University, Cheonan 31066, South Korea
e-mail: jonghyouk@smu.ac.kr

This work was supported by the research grant from Sangmyung University.

ABSTRACT Blockchain technology has been known as the underlying technology of cryptocurrencies, but nowadays it is further considered as a functional technology for improving existing technologies and creating new applications previously never practical. In this paper, we are focused on utilizing blockchain technology to introduce a new ID as a service (IDaaS) for digital identity management. The proposed blockchain-based ID as a service (BIDaaS) is explained with one practical example that shows how the proposed BIDaaS works as an identity and authentication management infrastructure for mobile users of a mobile telecommunication company.

Contents

- Demand for a New Type of IDaaS
- Blockchain based ID as a Service 제안
  - Entities Involved
  - Procedures
- Discussion

Demand for a New Type of IDaaS

- 클라우드 컴퓨팅이 컴퓨팅 산업에 큰 변화를 가져옴.
- Identity & authentication management 를 IDaaS 형태로 클라우드에서 제공한다면 많은 장점을 가질 수 있음.
  - Reduced on-site infra
    - 개별 사이트 사용자 정보 저장 불필요 등
  - 클라우드 서비스와의 통합 관리
  - 사용 편의성
    - 사용자 개별 계정 생성 불필요 등
- IDaaS는 critical기능을 3rd party에 맡기는 일이므로 3rd party를 완전히 믿을 수 있어야 하며 투명한 체계가 필요함.

Blockchain based ID as a Service 제안

3 Entities Involved

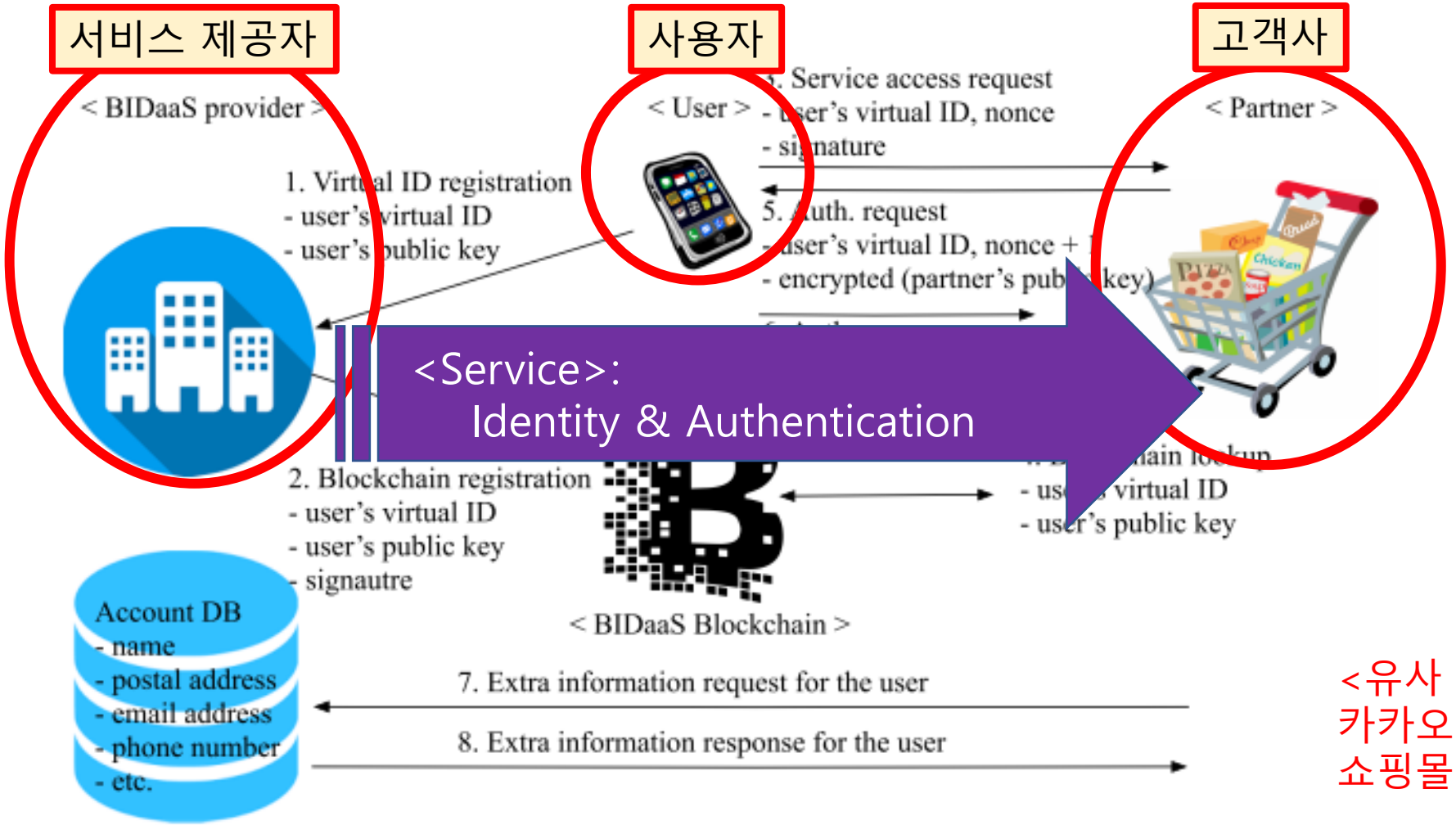


FIGURE 1. BIDaaS for a mobile user.

<유사 예시>:
카카오 계정으로
쇼핑몰 등에 로그인

Procedures

1) Virtual ID Creation

2) BIDaaS Blockchain Registration

3) Mutual Athentication

4) Extra Information Request

1) Virtual ID Creation

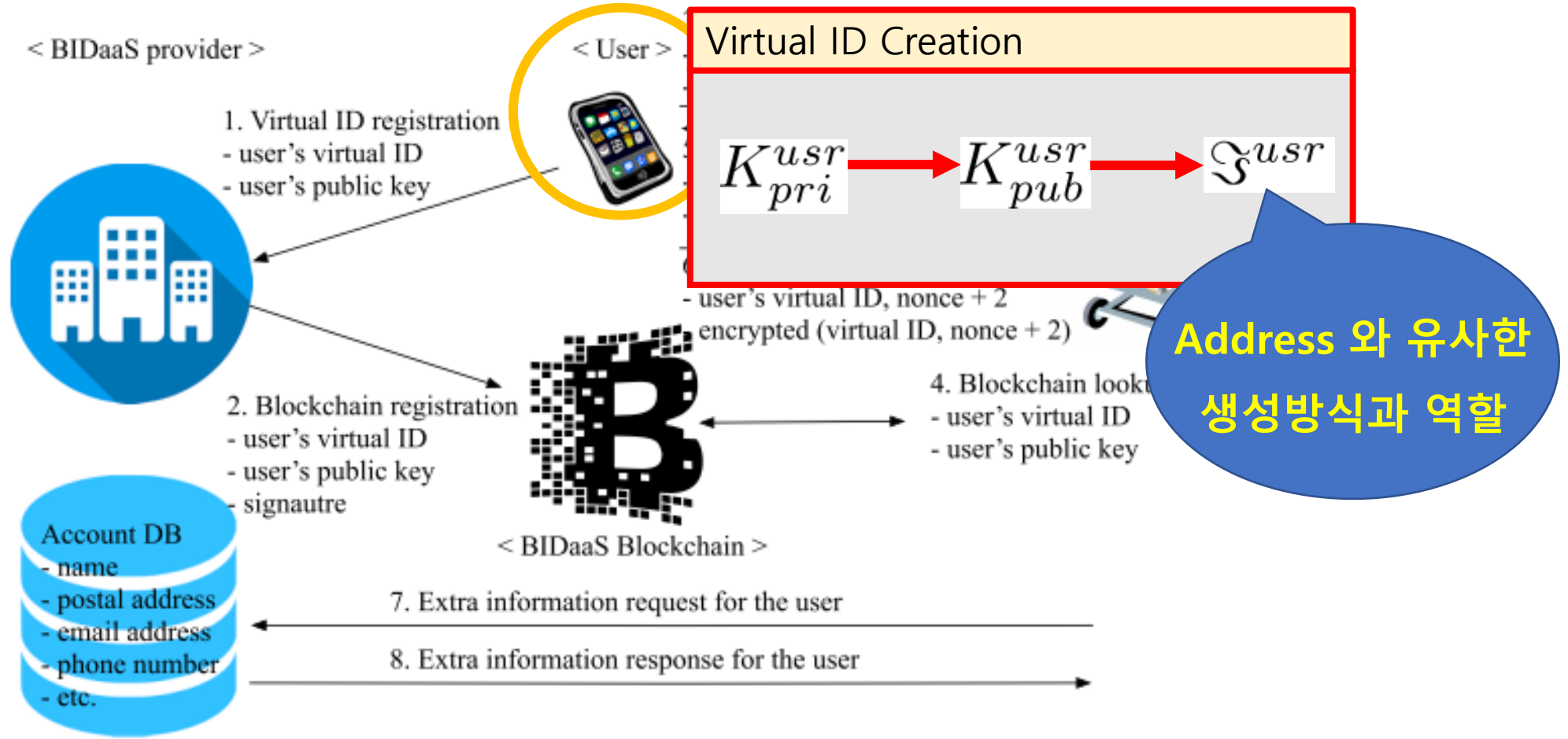


FIGURE 1. BIDaaS for a mobile user.

2) BIDaaS Blockchain Registration

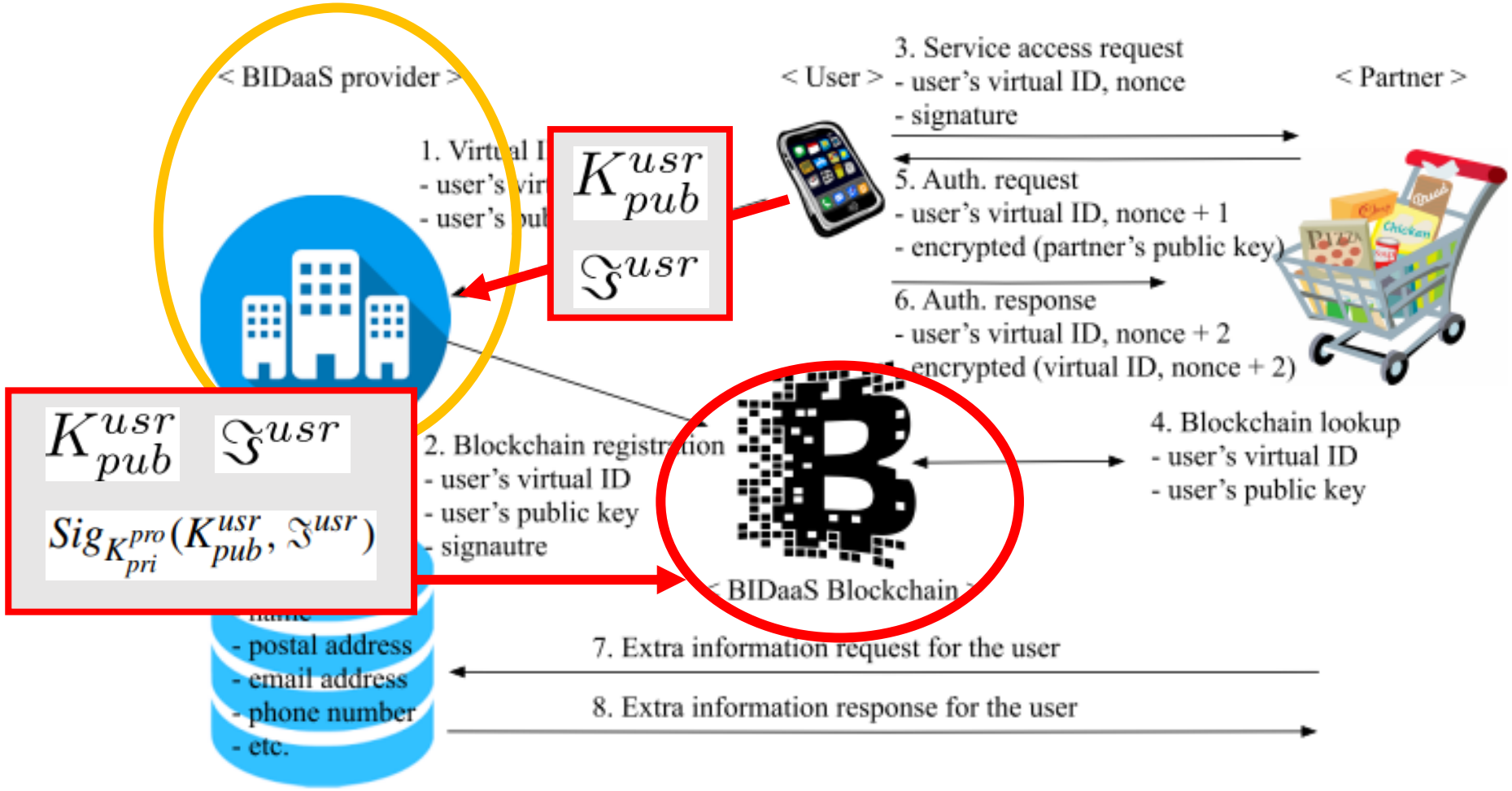


FIGURE 1. BIDaaS for a mobile user.

3) Mutual Athentication

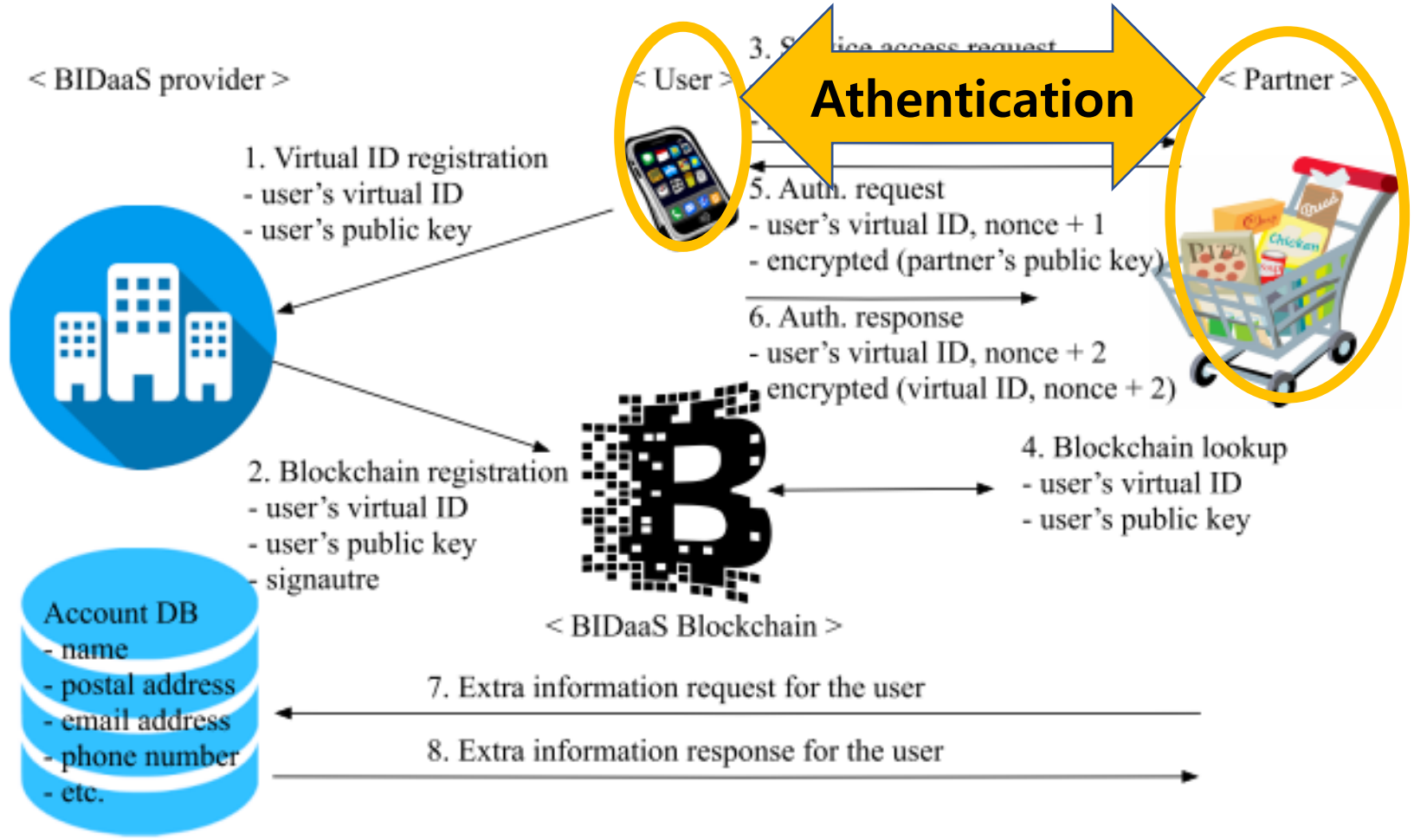


FIGURE 1. BIDaaS for a mobile user.

3) Mutual Athentication

서비스 접근 요청
사용자 V-UID 전달

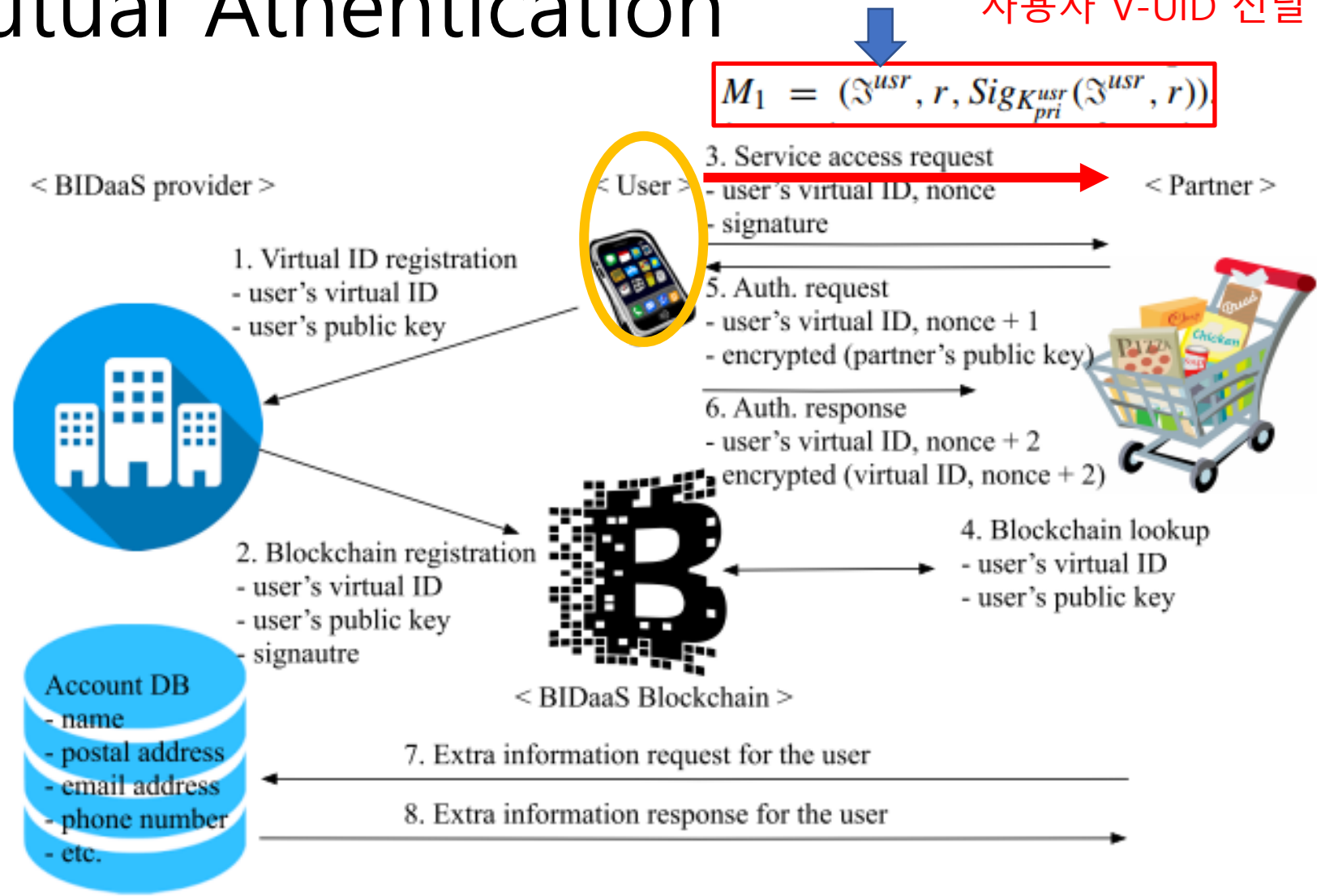


FIGURE 1. BIDaaS for a mobile user.

3) Mutual Athentication

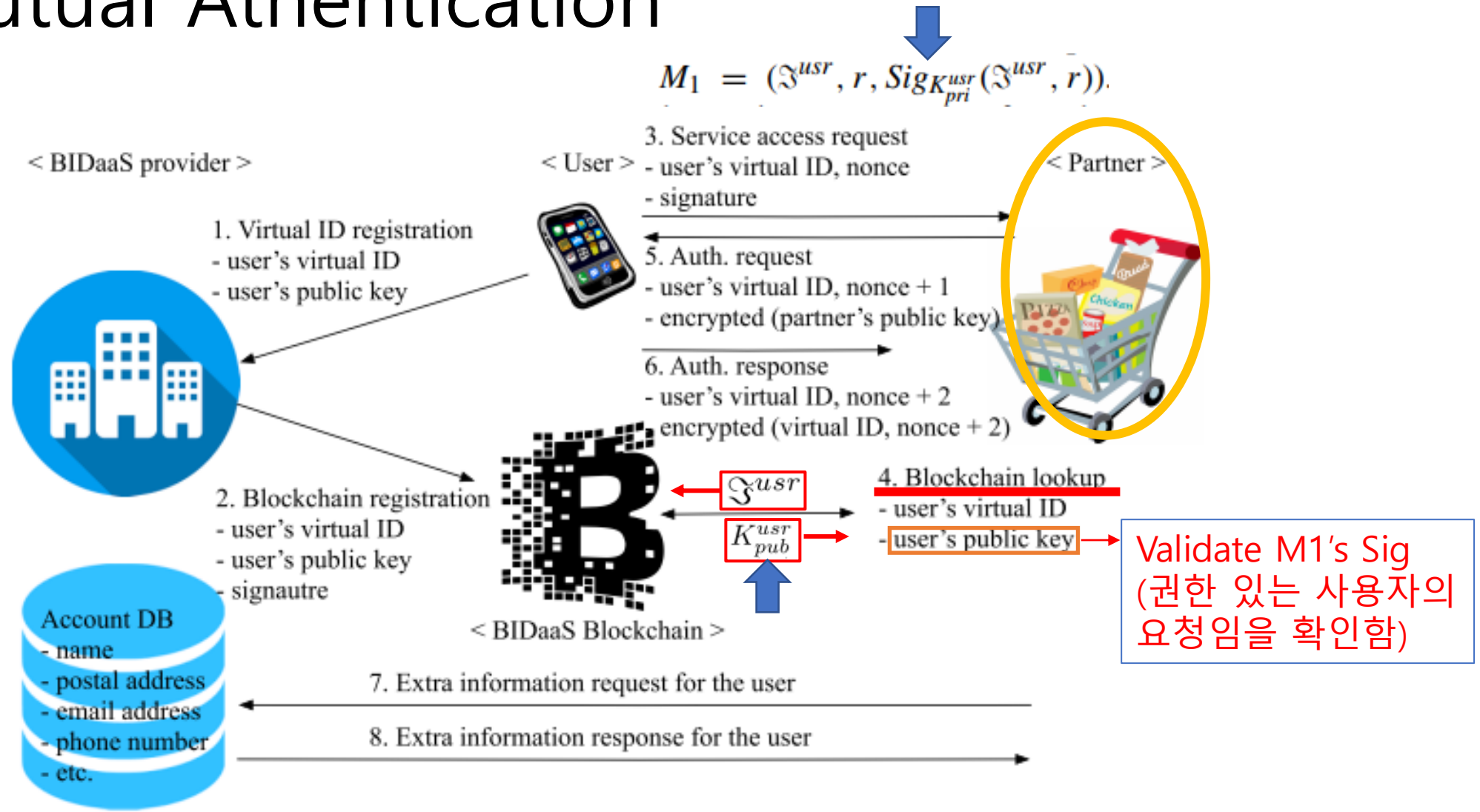


FIGURE 1. BIDaaS for a mobile user.

3) Mutual Athentication

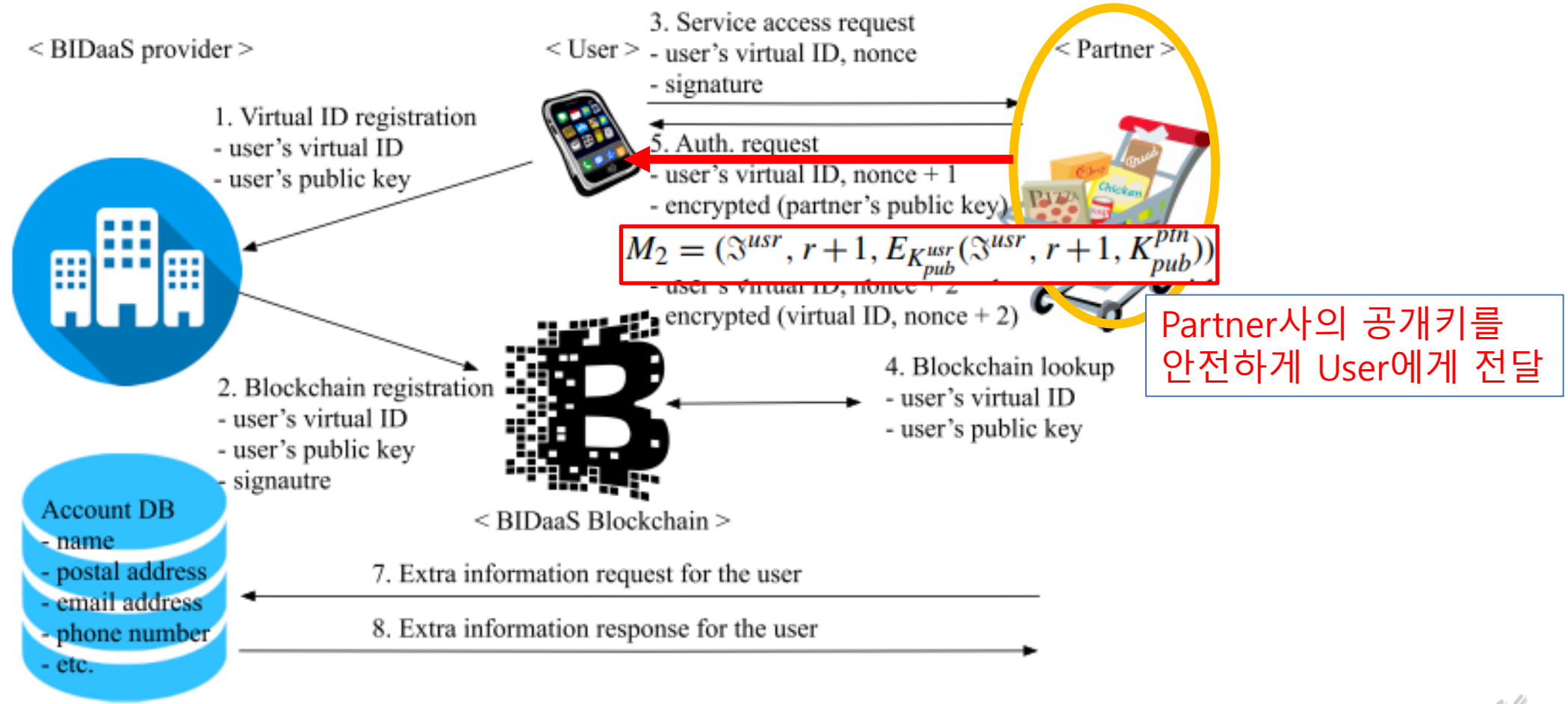


FIGURE 1. BIDaaS for a mobile user.

3) Mutual Athentication

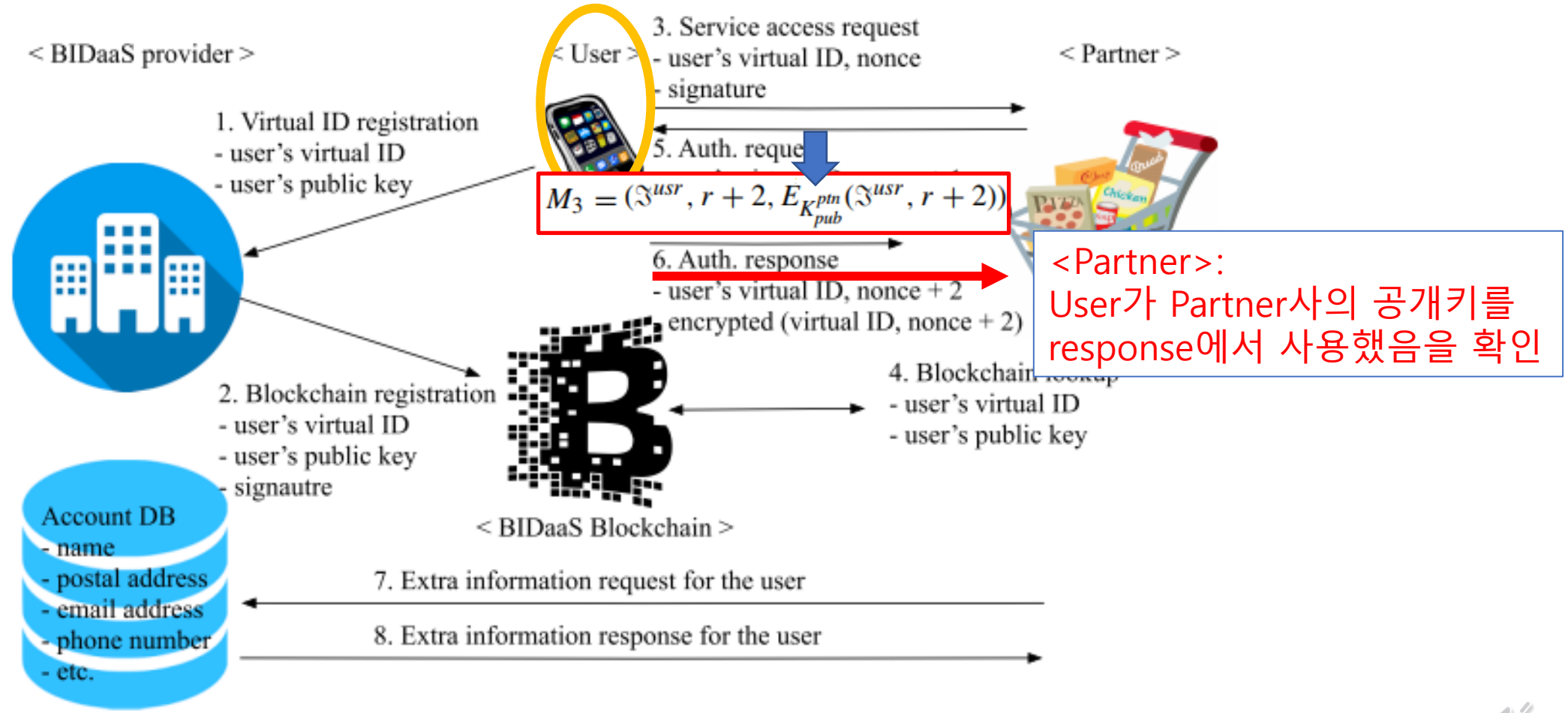
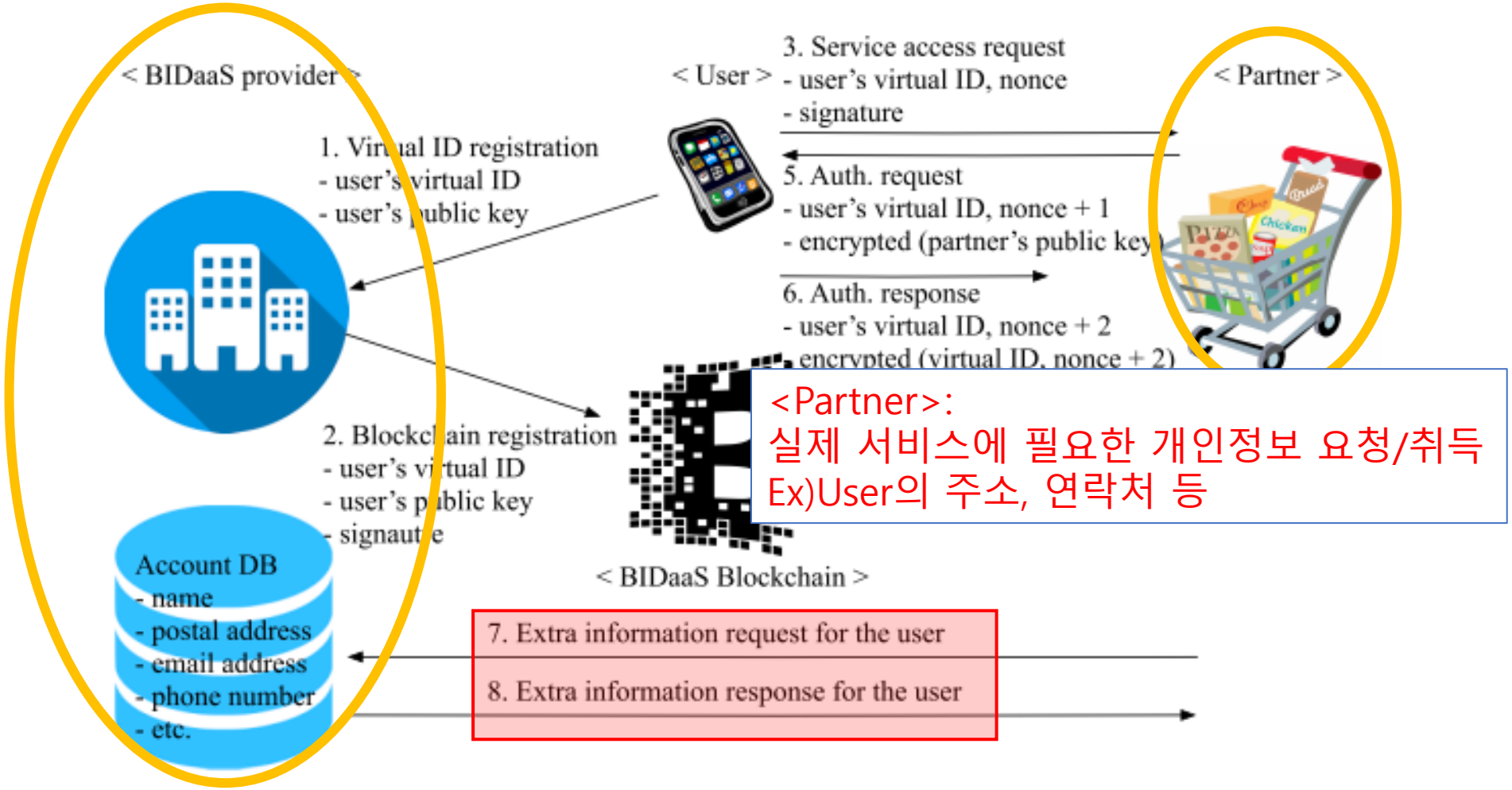


FIGURE 1. BIDaaS for a mobile user.

4) Extra Information Request



<Partner>:
실제 서비스에 필요한 개인정보 요청/취득
Ex)User의 주소, 연락처 등

FIGURE 1. BIDaaS for a mobile user.

Discussion

- CONSENSUS ALGORITHM
  - Private blockchain, PBFT algorithm 제안(PoW에 비해 효율적)
- CONSORTIUM BLOCKCHAIN
  - 컨소시엄 블록체인으로 구성할 수 있음
- SERVICE LEVEL AGREEMENT
  - 서비스 제공자와 파트너가 간에 SLA가 필요할 수 있음.
  - 이는 서비스 제공자의 수익원을 창출하게 함.
- PROVIDED USER INFORMATION
  - 부가적 사용자 정보가 사용목적에 한해 일시적으로 제공되지만,
  - 파트너사의 코드에 따라 해당 정보가 저장되거나 다른 목적으로 사용될 여지가 있음.
  - 프라이버시 문제를 위해 이를 탐지하고 방지하는 Scheme이 필요

Discussion

- USE OF VIRTUAL IDs
  - may be used per service or per partner
  - same virtual ID may be used for all partners
  - depending on the user's decision (a degree of user privacy)
- TIMESTAMP INSTEAD OF A NONCE
- PRIVATE KEY OF A USER
  - must be safely stored and managed
  - eSIM or TEE

Discussion

- BENEFITS TO THE BIDaaS PROVIDER
  - 새 수익원 창출
- BENEFITS TO THE PARTNER
  - 인증 관리 구조를 실행/관리할 필요 없음.
  - 사용자 개인정보를 저장할 필요 없음.
- BENEFITS TO THE USER
  - 수많은 계정을 만들고 관리할 필요 없음
  - ID, 패스워드를 기억할 필요 없음.
- .....카카오ID 등 O-auth/OpenID를 사용하는 이유

끝.

감사합니다.