유스케이스 명세서

(Usecase Specification Document)

과제명	블록체인 기반 자기주권형 분산 신원 증명 연구

조	9 조
지도교수	류재철 교수님 (서명)
조원	201502015 권재승 201502122 조성락 201601155 오하늘

Table of Contents

Introduction

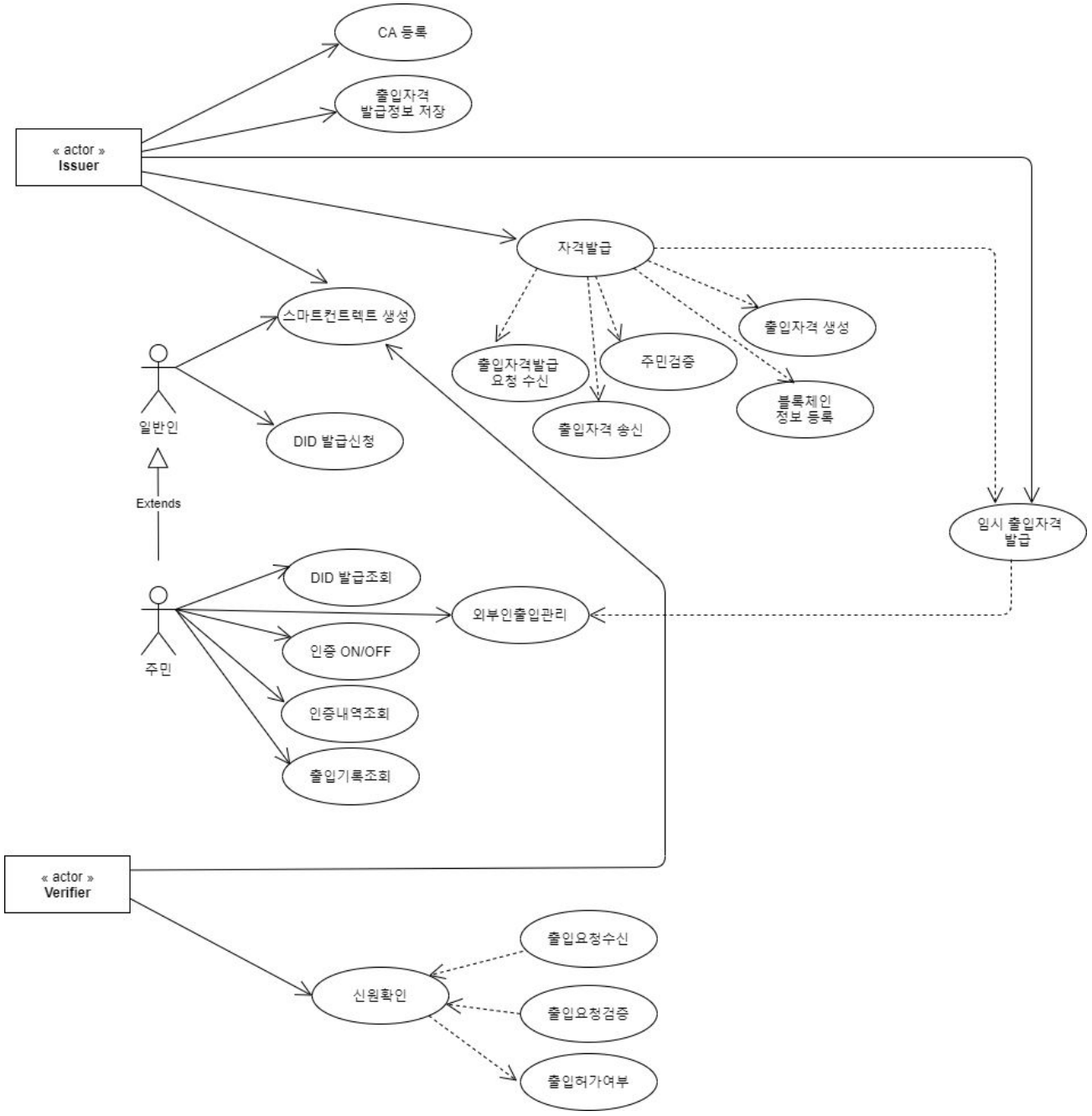
1.1. Objective

이 문서는 블록체인 DID를 이용한 아파트 출입시스템의 기능과 요구사항을 명세하고있다. 요구사항을 상세하게 표현하기 위한 유스케이스 다이어그램과 각 유스케이스에 대한 명세를 포함한다.

2. Usecase Diagram

블록체인 기반 자기주권형 분산 신원 증명 플랫폼을 사용한 아파트 출입통제 시스템에서 수행하는 기능들에 대한 유스케이스 다이어그램은 다음과 같다.

그림 1. 아파트 출입통제 시스템에 대한 유스케이스 다이어그램



3. Usecase Specification

3.1. 스마트 컨트렉트 생성

Usecase 이름	스마트 컨트렉트 생성
ID	1
간략 설명	스마트 컨트렉트 생성 절차에 대한 명세이다.
Actor	일반인, 주민, Issuer, Verifier
Pre-Conditions	- 서비스 사용자는 이더리움 프라이빗 네트워크에 속해있어야 한다.
Main Flow	1) 사용자 어플리케이션에서 출입자격 발급, 정보 조회 등의 기능을 사용한다. 2) 정보 조회 또는 정보 전송을 위해 스마트 컨트랙트 생성자를 생성한다.
Post-Conditions	- 스마트 컨트랙트 생성자가 생성된다.
Alternative Flow	

3.2. 자격발급

Usecase 이름	자격발급
ID	2
간략 설명	아파트 출입자격을 발급해준다.
Actor	Issuer, 주민, 일반인
Pre-Conditions	- 자격을 발급받을 사용자가 자격발급을 요청해야한다. - Issuer가 신원 인증기관(CA)으로 등록되어있어야 한다.
Main Flow	1) 사용자 어플리케이션에서 자격발급 버튼을 클릭한다. 2) 출입자격을 발급받기 위해 필요한 정보를 입력하고 정보를 전송한다. 3) Issuer는 전달받은 정보를 검증하여 신원인증을 한다. 4) 신원인증이 완료되면 전달받은 사용자 공개키를 포함하여 출입자격을 발급한다. 5) 발급한 출입자격에 Issuer의 서명을 포함하여 다시 사용자 어플리케이션에게

	전달한다.
Post-Conditions	- 요청받은 출입자격을 발급한다.
Alternative Flow	3-1) 신원인증에 실패한다. Issuer는 출입자격을 발급하지 않는다.

3.3. 신원인증기관(CA) 등록

Usecase 이름	신원인증기관(CA)등록
ID	3
간략 설명	아파트 출입자격을 발급해줄 신원인증 기관을 등록한다.
Actor	Issuer
Pre-Conditions	- 신뢰할 수 있는 인증기관이여야 한다. - 이더리움 사설 네트워크 관리자이어야 신원 인증 기관(CA)을 등록할 수 있다.
Main Flow	1) 블록체인 기반 DID 플랫폼 관리자는 신뢰할 수 있는 신원인증기관을 선정한다. 2) 아파트 관리사무소의 인증서와 그 서명을 검증할 수 있는 공개키를 등록한다. 3) 신원인증기관(CA)로 등록된다.
Post-Conditions	- 신원인증기관(CA)로 등록된다.
Alternative Flow	

3.4. 출입자격 발급정보 저장

Usecase 이름	출입자격 발급정보 저장
ID	4
간략 설명	블록체인에 출입자격 발급정보를 저장한다.
Actor	사용자, Issuer

Pre-Conditions	- 데이터 서명을 위한 키 생성
Main Flow	1) Issuer 또는 사용자는 서명을 위한 개인키는 자신이 가지고, 공개키를 블록체인에 넣어 저장한다. 2) Issuer의 경우, 출입자격을 발급한 후 해당 발급과 관련된 정보들(유효기간, 권한, 서명값)을 블록체인에 올린다.
Post-Conditions	- 출입자격을 검증하기 위한 정보들이 블록체인에 저장된다.
Alternative Flow	

3.5. 출입자격 발급요청 수신

Usecase 이름	출입자격 발급요청 수신
ID	5
간략 설명	주민 또는 일반인으로부터 출입자격 발급요청을 수신한다.
Actor	Issuer, 주민, 일반인
Pre-Conditions	- 출입자격을 요청하는 사용자가 블록체인 사설 네트워크에 참가된 상태이어야한다.
Main Flow	1) 사용자 어플리케이션에서 자격발급 버튼을 클릭한다. 2) 출입자격을 발급받기 위해 필요한 정보를 입력하고 정보를 전송한다. 3) Issuer는 전달받은 정보를 수신한다.
Post-Conditions	- Issuer가 출입자격을 수신한다.
Alternative Flow	

3.6. 주민 검증

Usecase 이름	주민 검증
ID	6

간략 설명	출입자격을 발급하기 위해 주어진 정보에 해당되는 주민이 맞는지 검증한다.
Actor	Issuer
Pre-Conditions	- 주민이 출입자격을 Issuer에게 요청해야한다. - 주민의 정보를 Issuer가 받아야한다.
Main Flow	1) Issuer는 출입자격 발급을 위해 주민으로부터 정보를 수신한다. 2) 정당한 아파트 주민인지 검증한다.
Post-Conditions	- 아파트 주민인지 여부가 결정된다.
Alternative Flow	

3.7. 출입자격 생성

Usecase 이름	출입자격 생성
ID	7
간략 설명	아파트 출입을 위한 출입자격을 생성한다.
Actor	Issuer
Pre-Conditions	- 출입자격을 요청한 사용자가 아파트 주민이거나 허락받은 출입자이여야한다.
Main Flow	1) 출입자격을 요청한 사람이 검증한다. 2) 검증된 요청자의 출입자격을 생성한다. 3) 생성된 출입자격에 Issuer의 개인키로 서명한다.
Post-Conditions	- 출입자격이 생성된다.
Alternative Flow	

3.8. 출입자격 송신

Usecase 이름	출입자격 송신
ID	8
간략 설명	생성한 출입자격을 요청자에게 송신한다.
Actor	Issuer
Pre-Conditions	- 출입자격이 생성된다.
Main Flow	1) 생성된 출입자격에 Issuer의 개인키로 서명한다. 2) 요청자에게 출입자격을 송신한다.
Post-Conditions	- 출입자격을 정상적으로 송신된다.
Alternative Flow	

3.9. 신원확인

Usecase 이름	신원확인
ID	9
간략 설명	신원확인 절차에 관해 명세한다
Actor	사용자,Verifier
Pre-Conditions	- 사용자의 did가 블록체인에 등록되어있어야한다. - verifier는 스마트컨트렉트를 생성해야한다.
Main Flow	1) 사용자가 출입시스템에 신원확인 요청을 한다. 2) verifier는 출입요청 수신을 통해 사용자의 DID정보를 받는다. 3) 블록체인에 등록되어있는 사용자의 DID정보를 이용하여 출입요청검증을 진행한다. 4) 출입허가여부를 결정한 후, true이면 문을 열어주고 false이면 경고문을 출력한다.
Post-Conditions	

Alternative Flow	

3.10. 블록체인에 정보 등록

Usecase 이름	블록체인에 정보 등록
ID	10
간략 설명	블록체인에 출입자격을 등록하는 과정을 자세히 명세한다.
Actor	Issuer, 사용자
Pre-Conditions	-사용자는 오픈키를 가지고 있어야한다
Main Flow	1) issuer는 사용자의 did에 서명을 하여 사용자에게 전달한다 2) 사용자는 이에 자신의 오픈키와 서명을 첨부하여 블록체인에 등록한다.
Post-Conditions	- 사용자의 출입자격이 블록체인에 등록된다
Alternative Flow	

3.11. 임시 출입자격 발급

Usecase 이름	임시 출입자격 발급
ID	11
간략 설명	외부인 출입을 위한 임시 출입자격 발급에 관해 자세히 명세한다
Actor	사용자, issuer, 일반인
Pre-Conditions	- 사용자는 블록체인에 자격증명이 되어있어야한다
Main Flow	1) 일반인이 사용자에게 임시출입권한을 요청한다. 2) 사용자는 이 정보를 issuer에게 전달하며 임시출입자격발급을 요청한다. 3) issuer는 이 정보를 이용하여 임시출입자격을 생성하고 블록체인에 등록한다.

Post-Conditions	- 일반인의 출입자격이 기간제로 부여받는다.
Alternative Flow	

3.12. 출입요청 수신

Usecase 이름	출입요청 수신
ID	12
간략 설명	주민으로부터 출입 요청을 받음
Actor	주민, Issuer
Pre-Conditions	- 주민이 출입요청을 함
Main Flow	1) 주민으로부터 출입요청을 받음
Post-Conditions	
Alternative Flow	

3.13. 출입요청 검증

Usecase 이름	출입요청 검증
ID	13
간략 설명	검증에 필요한 정보를 사용하여 출입에 허가된 사용자인지 검증함
Actor	Verifier
Pre-Conditions	사용자로부터 출입요청을 수신받음
Main Flow	1) 사용자로부터 받은 자격에 대해 자격을 발급해준 CA를 검증한다. 2) 사용자로부터 받은 자격에 대해 사용자가 주민인지 검증한다.
Post-Conditions	

Alternative Flow	

3.14. 출입 허가 여부

Usecase 이름	출입 허가 여부
ID	14
간략 설명	검증된 사용자에 대한 출입허가 여부를 판단한다.
Actor	Verifier
Pre-Conditions	사용자가 제출한 자격에 대해 검증을 완료
Main Flow	1) 자격 검증의 결과에 따라 사용자의 출입할 자격이 있는지 판단한다.
Post-Conditions	
Alternative Flow	

3.15. DID 발급 신청

Usecase 이름	DID 발급 신청
ID	15
간략 설명	DID 발급 신청
Actor	사용자,Issuer
Pre-Conditions	- 사용자의 신원이 CA에서 인증되어 있어야함. - 사용자의 공개키가 발급되어야 함.
Main Flow	1) 사용자는 어플리케이션에 발급신청을 누른다. 2) 어플리케이션은 사용자정보를 Issuer에게 전달한다. 3) Issuer는 발급받은 사용자 정보를 이용해 자격발급을 진행한다. 4) 사용자는 받은 자격발급에 서명을해 공개키를 블록체인에 등록한다.

Post-Conditions	- 사용자는 회원으로 등록된다.
Alternative Flow	

3.16. DID 발급 조회

Usecase 이름	DID 발급 조회
ID	16
간략 설명	DID발급 내역 조회 절차를 명세한다.
Actor	사용자,일반인,Issuer
Pre-Conditions	- 이전에 발급신청을 해야한다
Main Flow	1) 사용자,일반인은 발급내역 조회 버튼을 누른다. 2) 어플리케이션은 issuer에게 발급내역정보를 요청한다. 3) issuser는 발급내역정보를 어플리케이션에 전달한다 4) 사용자에게 발급내역정보를 출력한다.
Post-Conditions	- 발급 내역을 출력한다
Alternative Flow	

3.17. 인증 ON/OFF

Usecase 이름	인증 ON/OFF
ID	17
간략 설명	인증 on/off기능에 대해 명세한다
Actor	사용자,verifier
Pre-Conditions	- 사용자의 자격이 블록체인에 등록되어 있어야한다.

Main Flow	1) 사용자가 ON/OFF버튼을 누른 후 출입시스템에 태그한다. 2) 어플리케이션에서 Verifier에게 자격정보를 전달한다 3) Verifier는 전달받은 자격정보를 블록체인에 등록된 오픈키를 확인하여 신원을 확인한다. 3-1) 신원이 확인되면 문이 열린다. 3-2) 신원이 확인되지 않으면 오류문구와 함께 문이 열리지 않는다
Post-Conditions	
Alternative Flow	

3.18. 외부인 출입관리

Usecase 이름	외부인 출입관리
ID	18
간략 설명	외부인 출입관리에 관한 절차를 명세한다
Actor	사용자,Issuer,외부인
Pre-Conditions	- 외부인은 미리 발급받은 DID를 가지고있어야한다.
Main Flow	1) 사용자는 외부인 출입관리 버튼을 누른다. 2) 어플리케이션은 Issuer에게 외부인에 관한 정보를 전달한다. 3) issuer는 외부인에 관한 정보를 블록체인에 등록하여 임시로 자격을 부여한다. 4) 외부인은 권한을 획득한다.
Post-Conditions	- 외부인에게 임시 출입권한을 부여한다.
Alternative Flow	

3.19. 인증내역 조회

Usecase 이름	인증내역 조회

ID	19
간략 설명	출입기록을 조회에 관한 절차를 명세한다
Actor	주민
Pre-Conditions	- 인증내역을 보는 사람은 신원이 인증된 본인이여야 한다
Main Flow	1) 사용자가 인증내역조회 버튼을 누른다 2) database에 기록된 사용자의 인증내역을 조회하여 목록으로 나열한다. 3) 보고싶은 인증기록을 선택한다. 4) 자격 인증한 일시, 날짜, 신원정보를 출력한다.
Post-Conditions	-자격인증 내역이 출력된다.
Alternative Flow	

3.20. 출입기록 조회

Usecase 이름	출입기록 조회
ID	20
간략 설명	출입기록을 조회에 관한 절차를 명세한다
Actor	주민
Pre-Conditions	- 출입기록을 보는 사람은 신원이 인증된 본인이여야 한다
Main Flow	1) 사용자가 출입기록조회 버튼을 누른다 2) databse에 기록된 사용자의 출입기록을 조회하여 목록으로 나열한다. 3) 보고싶은 출입기록을 선택한다. 4) 출입한 일시, 날짜, 신원정보를 출력한다.
Post-Conditions	- 출입기록이 목록에 출력된다.
Alternative Flow	