요구사항명세서

(Software Requirements Specification)

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

1. Introduction

1.1. Purpose

블록체인 DID를 활용한 아파트 출입 시스템개발을 위하여 요구되는 시스템기능 및 인터페이스를 명세하고, 성능 및 품질에 대한 기준을 마련하다. 이를 기반으로 서비스 제공자는 소프트웨어의 구조와 기능을 체계적으로 이해할 수 있으며, 개발자는 예상되는 제약 사항 및 발생 가능한 오류가 반영된 명확한 요구 사항을 토대로 높은 품질의 제품을 구현해 낼 수 있다.

1.2. Scope

신용기관이 사용자에게 DID를 발급하면, 사용자는 블록체인 시스템위에 올려져있는 DID를 활용해 verifier에게 자신임을 인증 할 수 있다. 이때, 블록체인 특성상, 이에 대한 정보가 다수의 동의가 없이는 조작되기 힘들다는 점을 이용하여, 신뢰성과 보안성을 높일 수 있다. 또한 DID의 특성으로, 원하는 정보만 줄 수 있다는 장점이 있다. 또한, 중앙관리자를 따로 두지않아, 서버관리에 드는 비용을 절감할 수 있다.

1.3. Definitions, acronyms, and abbreviations

블록체인(BlockChain) : 블록체인은 관리 대상 데이터를 '블록'이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장 환경에 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다.

분산 아이디(DID) : 분산아이디(Decentralized Identifier)는 기존 신원확인 방식과 달리 중앙 시스템에 의해 통제되지 않으며 개개인이 자신의 정보에 완전한 통제권을 갖도록 하는 기술이다.

이더리움(Ethereum) : 이더리움은 블록체인 기술을 기반으로 스마트 계약 기능을 구현하기 위한 분산 컴퓨팅 플랫폼이자 운영 체제다.

브라우니(Brownie) : 스마트 컨트랙트(Smart contract)의 Deploy와 Testing을 도와주는 도구

발급자(Issuer) : DID 자격증명을 발급해주는 발급자

검증자(Verifier) : DID 자격증명을 제출받아 검증하는 검증자

신원인증기관(CA) : 위의 발급자(Issuer)에 해당되며 믿을 수 있는 신원인증기관

QR코드 : QR 코드은 흑백 격자무늬 패턴으로 정보를 나타내는 매트릭스 형식의 이차원 바코드이다.

RSA : RSA 암호는 공개키 암호시스템의 하나로, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘으로

알려져 있다.

ECC : 타원곡선 암호(Elliptic curve cryptography)는 타원곡선 이론에 기반한 공개 키 암호 방식이다.

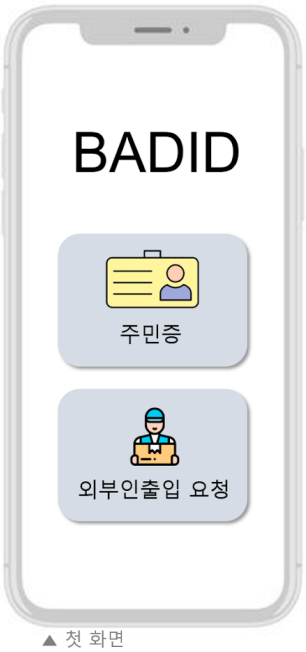
전자서명 : 전자서명이라 함은, 서명자를 확인하고 서명자가 당해 전자문서에 서명했다는 사실을 나타내는 데 이용하려고, 특정 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다.

1.4. References

- Web3j 공식 문서 : https://docs.web3j.io/
- Brownie 공식 문서 : https://eth-brownie.readthedocs.io/en/stable/
- 요구사항 일람표 : https://ko.wikipedia.org/wiki/%EC%9A%94%EA%B5%AC%EC%82%AC%ED%95%AD
- 솔리리티 공식 문서 : https://solidity-kr.readthedocs.io/ko/latest/
- 안드로이드 스튜디오 : https://developer.android.com/?hl=ko

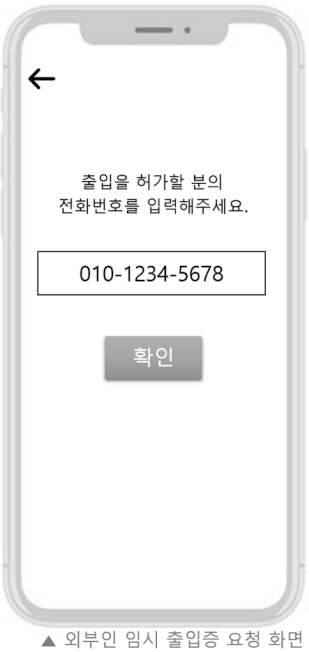
2. External Interface Requirements

2.1. 사용자 인터페이스 (User Interface)



▲ 첫 화면

▲ 발급받은 주민증



▲ 외부인 임시 출입증 요청 화면

사용자는 위와 같은 어플리케이션을 통해 시스템을 사용한다. 첫 번째 사진은 처음 보여지는 화면으로 각 버튼은 다음과 같은 기능을 수행한다.

주민증 버튼을 통해 발급을 요청할 수 있다. 휴대폰 인증으로 자기 자신을 인증하면 디지털증명서 발급기관인 아파트관리사무소로부터 주민증을 발급을 받는다. 주민증을 이미 발급받은 사람은 주민증 버튼을 통해 자신의 주민증을 볼 수 있다(두 번째 사진). 주민증에는 간단한 개인정보(이름, 주소)가 보이고 하단에 바코드와 QR코드가 들어있다. 바코드와 QR코드로 출입 시스템에 출입을 요청한다.

주민은 외부인출입 요청 버튼을 통해 외부인 출입허가를 요청할 수 있다. 출입을 허거할 외부인의 전화번호를 입력하여 전달하면 시스템에서 디지털증명서 발급기관에게 해당 번호의 사람에게 임시 주민증을 발급해준다. 주민증이 발급된 주민에 한해서만 이 기능을 사용할 수 있고 주민이 아닌 경우에는 주민증을 발급받으라는 알림을 받는다.

2.2. 하드웨어 인터페이스 (Hardware Interface)

1. 라즈베리파이3+

   Verifier 역할을 수행하기위한 하드웨어. 사용자로부터 데이터를 읽고, 서버와 통신해, 블록체인에

있는 정보를 읽고, 비교하여 신원을 검증한다.

2. 안드로이드 스마트폰

   DID 발급 및 관리, 출입시스템 이용을 위한 어플리케이션 구동을 위한 하드웨어이다. 안드로이드 시스템의 최신버전 OS가 권장된다.

2.3. 소프트웨어 인터페이스 (Software Interface)

1. 이더리움

   프라이빗 블록체인 네트워크 구성을 위한 블록체인 플랫폼이다.

2. remix

   솔리디티로 작성된 스마트컨트렉트를 컴파일하여 DApp을 만들 수 있도록 하는 개발도구이다. 스마트 컨트렉트로 DID를 작성하여, 출입 검증 및 DID발급을 담당하는 DApp을 컴파일한다.

3. geth

   이더리움 플랫폼에 참여하기 위한 네트워크 플랫폼이다. go언어로 작성되어있으며, 마이닝, 블록생성등을 할 수 있다.

4. 안드로이드스튜디오

   안드로이드 어플 개발 IDE로써, 이를 활용하여, 블록체인 DID 아파트 출입시스템 이용을 위한 사용자 어플리케이션을 제작한다.

5. android sdk

   안드로이드 어플 개발에 필요한 다양한 도구가 포함된 개발도구이다.

6. 솔리디티

   스마트 컨트렉트를 작성하기위한 언어.

2.4. 통신 인터페이스 (Communication Interface)

1. web3.js

   어플리케이션과, 이더넷 프라이빗 네트워크의 송수신을 위해 필요하다. 자바스크립트로 작성되어있는 통신 프로토콜이다.

2. rpc

   블록체인을 구성하기위해, 블록끼리 통신하기위한 프로토콜

3. 시리얼통신

라즈베리파이와, 현관문과의 통신을 위해 시리얼통신이 사용된다.

4. NFC

   핸드폰의 어플의 DID정보를 NFC방식을 통하여, Verifier인 라즈베리파이로 데이터를 전송한다

3. System Features

3.1 블록체인 플랫폼 시스템 (System Feature 1)

3.1.1 설명 및 우선순위 (Description and Priority)

블록체인 플랫폼 시스템			
식별자	**기능**	**설명**	**우선순위**
FUR-01	스마트컨트랙트 생성	스마트 컨트랙트 생성한다.	중간
FUR-02	신원인증기관(CA) 등록	신원인증기관(CA)를 등록한다.	높음
FUR-03	인증서 발급정보 저장	인증서 발급정보 저장한다.	높음
TER-01	Solidity 코드 검증	Solidity 코드를 검증한다.	중간

3.1.2 기능 요구사항 (Functional Requirements)

요구사항 분류		블록체인 플렛폼 시스템
요구사항 번호		FUR-01
요구사항 명칭		스마트컨트랙트 생성
요구사항 상세설명	정의	신원인증기관 및 사용자 공개키 정보저장을 위한 스마트 컨트랙트 생성
	세부 내용	◦ 특정 함수는 특정 address 에서만 접근 가능하도록 생성자를 실행하는 address를 저장하도록 구현 ex:) 신원인증기관(CA) 등록은 모든 유저가 수행하지 않고 일부 유저만이 수행할 수 있어야 함 ◦ 스마트 컨트랙트 전체적으로 사용될 값 정의 및 생성자에서 초기화
산출정보		
관련 요구사항		FUR-01

요구사항 분류		블록체인 플렛폼 시스템
요구사항 번호		FUR-02
요구사항 명칭		신원인증기관(CA) 등록
요구사항 상세설명	정의	신원인증기관(CA) 등록에 요구되는 조건
	세부 내용	◦인증서 발급을 하는 신원인증기관(CA)의 공개키(public key) 또는 정보 등록을 위한 함수가 필요함 - 인증기관(CA)이 다수가 될 수도 있으므로 배열(array)을 사용할 필요가 있음 - 인증서가 신원인증기관(CA)의 개인키로 서명되었는지 확인하기 위한 공개키(public key) 정보를 저장할 필요가 있음
산출정보		
관련 요구사항		FUR-01

요구사항 분류		블록체인 플렛폼 시스템
요구사항 번호		FUR-03
요구사항 명칭		인증서 발급정보 저장
요구사항 상세설명	정의	인증서 발급정보 저장을 위해 요구되는 사항
	세부 내용	◦ 신원인증기관(CA)의 인증서 발급 정보를 블록체인에 저장하기 위한 함수 ◦ 신원인증기관(CA)가 발급한 인증서인지 검증하기 위한 정보들(서명값, 공개키 등)이 저장되어야 함 - 서명값 또는 검증을 위한 함수가 필요함
산출정보		
관련 요구사항		FUR-01

요구사항 분류		블록체인 플렛폼 시스템
요구사항 번호		FUR-01
요구사항 명칭		Solidity 코드 검증
요구사항 상세설명	정의	Solidity Code Test 를 위한 Populus 적용 및 CI 적용
	세부 내용	◦브라우니(brownie)를 통한 solidity code unit test 적용 ◦pytest를 통해 test 코드 실행

		◦github action을 통한 CI 적용
산출정보		
관련 요구사항		FUR-01, FUR-02, FUR-03

3.2 Issuer (System Feature 2)

3.2.1 설명 및 우선순위 (Description and Priority)

issuer 기능			
식별자	**기능**	**설명**	**우선순위**
FUR-04	주민증 발급 요청 수신	주민으로부터 주민증 발급을 요청받아 주민의 정보를 받음	높음
FUR-05	주민 검증	받은 주민의 정보로 검증을 함	중간
FUR-06	주민증 생성	검증된 주민을 대상으로 주민증을 발급해줌	높음
FUR-07	주민증 송신	생성한 주민증에 서명을 하여 사용자에게 주민증을 송신	중간
FUR-08	블록체인에 정보 등록	발급해준 정보에 대해 블록체인에 올림	높음

3.2.2 기능 요구사항 (Functional Requirements)

요구사항 분류		Issuer 기능
요구사항 번호		FUR-04
요구사항 명칭		주민증 발급 요청 수신
요구사항 상세설명	정의	사용자로부터 주민증 발급을 요청받음
	세부 내용	◦ 사용자로부터 주민증 발급을 요청 받음 - 사용자 정보 받음
산출정보		검증에 필요한 정보
관련 요구사항		주민 검증

요구사항 분류		Issuer 기능
요구사항 번호		FUR-05
요구사항 명칭		주민 검증
요구사항 상세설명	정의	검증에 필요한 정보를 사용하여 사용자가 주민임을 검증함
	세부 내용	◦ DID를 사용한 사용자 검증 과정 - 서명을 통해 사용자 검증
산출정보		검증에 대한 논리값 (True / Fasle)
관련 요구사항		주민증 발급 요청 수신, 주민증 생성

요구사항 분류		Issuer 기능
요구사항 번호		FUR-06
요구사항 명칭		주민증 생성
요구사항 상세설명	정의	검증된 주민에 대한 정보를 가지고 주민증을 생성
	세부 내용	◦ 주민임이 검증된 대상에 대해 주민증을 생성 - 주민 검증에서 True 값이 나왔는지 확인 - 사용자에 대한 주민증 생성
산출정보		주민증 데이터
관련 요구사항		주민 검증, 주민증 송신

요구사항 분류		Issuer 기능
요구사항 번호		FUR-07
요구사항 명칭		주민증 송신
요구사항 상세설명	정의	생성한 주민증에 서명하여 사용자에게 전달
	세부 내용	◦ 서명한 주민증을 사용자에게 전달. - 주민증에 서명하기 - 사용자에게 전달
산출정보		송신 완료에 대한 논리값
관련 요구사항		주민증 생성, 블록체인에 정보 등록

요구사항 분류		Issuer 기능
요구사항 번호		FUR-08
요구사항 명칭		블록체인에 정보 등록
요구사항 상세설명	정의	주민증 발급을 완료한 사용자에해서 관련 정보를 블록체인에 등록
	세부 내용	◦ 블록체인에 주민증을 위한 정보를 등록
산출정보		정보를 등록에 대한 논리값
관련 요구사항		인증서 발급정보 저장, 주민증 생성

3.3 Verifier (System Feature 3)

3.3.1 설명 및 우선순위 (Description and Priority)

verifier 기능			
식별자	**기능**	**설명**	**우선순위**
FUR-09	출입 요청 수신	사용자로부터 출입 요청을 받음	높음
FUR-10	출입 요청 검증	요청받은 사용자에 대해 검증	중간
FUR-11	출입허가 여부	검증된 사용자에 대해서 문을 열어주는 것을 허락함	높음

3.3.2 기능 요구사항 (Functional Requirements)

요구사항 분류		verifier 기능
요구사항 번호		FUR-09
요구사항 명칭		출입 요청 수신
요구사항 상세설명	정의	사용자로부터 출입을 요청받음
	세부 내용	◦ 사용자로부터 출입을 요청 받음 - 사용자로부터 출입에 대한 DID를 받음
산출정보		검증에 필요한 정보
관련 요구사항		FUR-10

요구사항 분류		verifier 기능
요구사항 번호		FUR-10
요구사항 명칭		출입 요청 검증
요구사항 상세설명	정의	검증에 필요한 정보를 사용하여 출입에 허가된 사용자인지 검증함

	세부 내용	◦ DID를 사용한 사용자 검증 과정 - 서명을 통해 주민증에 대한 사용자 검증 - 서명을 통해 주민증 발급 인증기관 검증
산출정보		검증에 대한 논리값 (True / Fasle)
관련 요구사항		FUR-09, FUR-11

요구사항 분류		verifier 기능
요구사항 번호		FUR-11
요구사항 명칭		출입허가 여부
요구사항 상세설명	정의	검증된 사용자에 대한 출입허가 여부를 판단
	세부 내용	◦ 검증된 사용자에 대해 출입 허가를 여부 판단 - 출입 요청 검증에서 True 값이 나왔는지 확인
산출정보		출입허가에 대한 논리값
관련 요구사항		FUR-10

3.4 사용자 어플리케이션 (System Feature 4)

3.4.1 설명 및 우선순위 (Description and Priority)

DID 어플리케이션			
식별자	기능	설명	우선순위
FUR-12	DID 발급신청	DID를 발급신청한다.	높음
FUR-13	DID 발급조회	DID발급 내역을 조회한다.	높음
FUR-14	인증ON/OFF	인증모드를 켜고 닫는다.	높음
FUR-15	외부인 출입관리	외부인에 대한 출입권한을 관리한다	중간
FUR-16	인증내역조회	출입인증에 관한 내역을 조회한다.	중간
FUR017	출입기록조회	출입기록을 조회한다.	낮음

3.4.2 기능 요구사항 (Functional Requirements)

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-12
요구사항 명칭		DID 발급신청
요구사항 상세설명	정의	사용자의 정보를 이용하여 DID 발급 신청
	세부 내용	◦사용자 정보를 입력받아, 신용기관과 연동하여 DID를 발급 및 암호화, 서명을 한다. - 사용자 정보 입력 기능 - 신용기관과 연동되어 DID발급 및 서명 기능
산출정보		
관련 요구사항		

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-13
요구사항 명칭		DID 발급조회
요구사항 상세설명	정의	DID발급 및 신청 내역 조회
	세부 내용	- DID 발급 신청 날짜 및 시간, 인증기관 정보를 목록에 출력
산출정보		
관련 요구사항		FUR-12

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-14
요구사항 명칭		인증 ON/OFF
요구사항 상세설명	정의	인증모드를 켜고 끔
	세부 내용	- DID 발급 신청 날짜 및 시간, 인증기관 정보를 목록에 출력
산출정보		
관련 요구사항		

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-15
요구사항 명칭		외부인출입관리
요구사항 상세설명	정의	외부인에 대한 출입권한을 관리한다
	세부 내용	- 배달원,우체국,AS기사등, 자신의 집에 신원이 인증된 사람이 출입을 할 예정일 경우, 보다 편리한 출입을 위해, 미리 인증권한을 부여함. - 외부출입자는 따로, 출입원한을 신청 할 필요가 없음.
산출정보		
관련 요구사항		

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-16
요구사항 명칭		인증내역조회
요구사항 상세설명	정의	자신의 DID가 인증된 내역을 조회
	세부 내용	-자신의 DID가 사용된 장소,날짜,시간을 출력 -목록 삭제 및 자신이 인증 한적 없는 경우를 대비해 신고 기능
산출정보		
관련 요구사항		

요구사항 분류		DID 어플리케이션
요구사항 번호		FUR-17
요구사항 명칭		출입기록조회
요구사항 상세설명	정의	출입한 기록을 조회한다.
	세부 내용	- 출입한 기록을 출력한다. - 출입기록 날짜,시간별로 출력, 삭제 기능
산출정보		
관련 요구사항		

4. Other Nonfunctional Requirements

4.1 성능 요구 (Performance Requirements)

본 연구인 블록체인 기반 자기주권형 분산 신원 증명에서 성능은 크게 요구되지 않는다. 프로젝트의 가장 큰 목적은 아파트 입출입에 사용하는 것이며, 플랫폼은 이더리움 프라이빗 네트워크에서 동작한다. 블록체인 기반이기 때문에 데이터를 업데이트하고 추가하는 것에서 작업증명(PoW)가 필요하고 이 때문에 마이닝을 수행하게 된다. 하지만 마이닝 난이도(difficulty) 및 가스량 등은 모두 우리가 설정할 수 있기 때문에 큰 문제가 없다.

요구사항 분류		성능
요구사항 번호		PER-001
요구사항 명칭		아파트 입출입 응답 시간
요구사항 상세설명	정의	아파트 입출입 응답 시간 목표 정의
	세부 내용	◦ 사용자가 아파트 입출입을 위해 사용자가 자격증명을 제출하면 최소한 2초 이내에는 출입문이 열릴 수 있도록 해야함 ◦ 정상적인 자격증명이 아닌 경우(해커에 의한 공격, 변조된 자격증명), 즉시 경보가 울리고 아파트관리사무소에 알림이 조치가 되어야 함
산출정보		
관련 요구사항		

요구사항 분류		성능
요구사항 번호		PER-002
요구사항 명칭		채굴 난이도
요구사항 상세설명	정의	채굴 난이도 목표 정의
	세부 내용	◦ 인증된 사용자만이 참여한 이더리움 프라이빗 네트워크에서 채굴 난이도는 매우 낮게 설정되어 있어야 함. ◦ 채굴을 수행하여 다음 블록체인을 연결하는데 걸리는 시간이 10초 이상 걸리면 안됨
산출정보		
관련 요구사항		

4.2 보안 요구 (Security Requirements)

아파트 출입을 위해서는 아파트 주민임을 증명할 수 있는 정보들을 제출할 필요가 있다. 아파트 출입에 있어 아파트 주민임을 증명하는 자격 증명을 제출할 수 있고, 이 자격증명이 탈취되거나 중간에서 변조되더라도 문제없도록 시스템이 구성되어야 한다. 또한 정보가 탈취된다고 하여도 안에 있는 사용자의 개인정보는 암호화되어 식별하지 못하여야 한다.

요구사항 분류		보안 요구사항
요구사항 번호		SER-001
요구사항 명칭		전자서명을 위한 암호키 생성
요구사항 상세설명	정의	전자서명을 위한 암호키 생성의 보안 요건
	세부 내용	◦ 적용 대상 : 아파트관리사무소(Issuer), 사용자 - 공개키 암호(RSA, ECC) 기반의 서명 알고리즘을 통한 데이터 무결성 보장 - 공개키 암호에 대한 공격을 방지하기 위한 충분한 키 길이 사용 - 생성한 개인키는 외부에 공개되어서는 안되며, 개인이 철저히 관리해야함. - 임시로 발급한 키에 대해서는 만료기간을 두어 기간내에만 사용되어야함 키 길이의 사용접근 및 정보 탈취를 차단하기 위한정보 시스템의 불법적인 접근을 차단하기 위해 사용자별 또는 그룹별로 접근권한을 부여 - 정보시스템 관리자가 업무별, 데이터별 중요도에 따라 접근 권한을 차등 부여할 수 있도록 하여 운영 - 데이터 및 장비의 무결성과 가용성을 유지하기 위해 백업 계획을 수립·이행하며, 사고 발생시 적시에 복구할 수 있도록 관리체계 마련 - 각급기관 도입을 위한 상용 정보보호시스템 보안성 검토 지침(국정원) 준수 - 시스템의 안정적인 운영을 위하여 보안취약점 발견 시 분석 및 조치를 수행하여야 함
산출정보		보안관리계획서, 점검내역
관련 요구사항		

요구사항 분류		보안 요구사항
요구사항 번호		SER-002
요구사항 명칭		자격 요청/제출 시 안전한 암호화 채널 이용
요구사항 상세설명	정의	자격 요청/제출 시 안전한 암호화 채널 이용의 조건

	세부 내용	◦ 적용 대상 : 아파트관리사무소(Issuer), 사용자, 아파트출입통제시스템(Verifier) - 네트워크 참여자간의 정보교환에 있어 안전한 암호화 통신 채널을 이용하도록 운영하여 평문 그대로 전송되지않게함 - 암호화 통신이 사용되는 구간은 아파트관리사무소(Issuer)와 사용자간의 정보요청 및 자격발급에서 사용하며, 사용자와 아파트출입통제시스템(Verifier)간의 아파트출입 증명제출 간에도 사용함
산출정보		보안관리계획서, 점검내역
관련 요구사항		

요구사항 분류		보안 요구사항
요구사항 번호		SER-003
요구사항 명칭		블록체인 기반 분산 신원 증명(DID) 플랫폼
요구사항 상세설명	정의	자격 요청/제출 시 안전한 암호화 채널 이용의 조건
	세부 내용	◦ 적용 대상 : 아파트관리사무소(Issuer), 사용자, 아파트출입통제시스템(Verifier) - 정보시스템 관리자가 서비스 이용자 정보, 발급 내역, 요청 내역 등을 조회하고 자격 박탈 등을 관리할 수 있도록 하여 운영 - 시스템의 안정적인 운영을 위하여 보안취약점 발견 시 분석 및 조치를 수행하여야 함
산출정보		보안관리계획서, 점검내역
관련 요구사항		

4.3 소프트웨어 품질 속성 (Software Quality Attributes)

블록체인 기반 자기주권형 분산 신원 증명에서 사용자 어플리케이션은 사용자가 자신의 자격과 개인정보를 자신이 관리하고 자신이 제출함으로서 자기주권형 신원 증명을 실현할 수 있다. 이로 인해 자격증명을 자신만이 가지고 있고, 자격증명이 중간에 탈취되어도 자신만이 서명하여 사용할 수 있다는 신뢰성이 필요하다.

요구사항 분류	품질
요구사항 번호	QUR-001

요구사항 명칭		신뢰성(reliability)
요구사항 상세설명	정의	신뢰성 개념 정의
	세부 내용	◦ 블록체인 기반 자기주권형 분산 신원 증명 시스템은 통상적인 업무시간 동안 가용성을 보장하여야 하며, 사용자가 요청한 자격 증명을 사용자에게만 발급하되 저장하여서는 안된다. ◦ 사용자에게 발급된 자격 증명안에는 사용자의 공개키가 포함된 상태로 신원인증기관의 서명이 되어있어야 하며, 타인이 이를 탈취하여 임의로 서명할 수 없게 하여야 한다.
산출정보		사업수행계획서
관련 요구사항		

5. Other Requirements

5.1. H/W 제약 조건

아파트 출입 통제 시스템에 사용하는 출입문은 한번에 한사람만 통과할 수 있게 하여야한다. 이를 위해 지하철 개찰표에서 사용하는 적외선 센서 등을 이용할 수 있으나 본 프로젝트에서 요구하는 중요한 사항은 아니기 때문에 옵션으로서 사용 가능하다. 또한 다른 사람이 출입하는 틈을 타 출입하거나 힘으로 문을 강제로 열게 될 경우, 경보가 울리는 등의 동작이 필요하다.

5.2. 자원, 인력에 대한 제약 조건

일단 블록체인 기반 자기주권형 분산 신원 증명 플랫폼을 운영할 관리자가 있어야 하고, 블록체인 사설 네트워크는 24시간동안 계속해서 운영되어야하기 때문에 별도의 서버가 필요하다.

6. 부록