요구사항명세서

(Software Requirements Specification)

과제명	**스마트 시티즌을 위한 모바일 신분증**

조	블록체인 떡상 조
지도교수	류재철 교수님
조원	201402315 곽현준 201302397 문준영 201203395 이우연

Table of Contents

1. Introduction

1.1. Purpose

블록체인을 활용한 자기주권형 신원증명시스템을 모바일 상으로 구현하여 편리하게 이용할 수 있는 모바일 신분증에 대해 설명 하고자한다.

시민으로서 신원을 증명해야할 필요가 생겼을 때 편리하게 이용가능한 모바일 신분증을 개발하고자하므로, 범용적으로 누구나 사용할 수 있는 제품이다.

1.2. Scope

모바일 상으로 구현된 신분증이기 때문에 지갑을 갖고다니지 않아도 언제나 간편하게 신분증을 제시하거나 조회할 수 있다. 또한, 블록체인의 특장점을 활용하여 개발되므로 보안성이 매우 강력하여 유출 위험성이 없는 자기 주권형 신분증으로 기능할 수있다. 중앙서버가 없는 분산형 시스템이기 때문에, 서버의 과부하 및 해킹위협 등으로부터 자유롭다.

현재 정부에서 진행중인 블록체인 사업의 경우 공무원증, 학생증, 운전면허증 등의 특수목적의 신원증명에 대해서 순차적으로 목표가 세워져있으나, 본 프로젝트의 목적은 대전시민에 한하여 자유롭게 신원증명이 가능한 범용적인 DID 개발에 목적을 둔다.

이에 따라 예상되는 사용자층은 일상생활에서 편리하게 신원증명을 이용할 대전시민 전체이다.

1.3. Definitions, acronyms, and abbreviations

블록체인: 데이터들이 P2P 방식으로 생성된 체인형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 임의로 수정될 수 없으면서 누구나 열람할 수 있는 분산 저장 시스템.

DID: Decentralized Identity 의 줄임말로 블록체인을 기반으로 한 탈 중앙화 신원 증명시스템을 말한다. 신원정보가 중앙서버에 저장되는 방식이 아닌, 분산저장되는 방식이므로 중앙화된 기관을 거치지 않고도 신뢰성 있는 검증이 가능하다.

Host: 분산신원 발급 및 인증을 위해 어플리케이션을 사용하는 유저

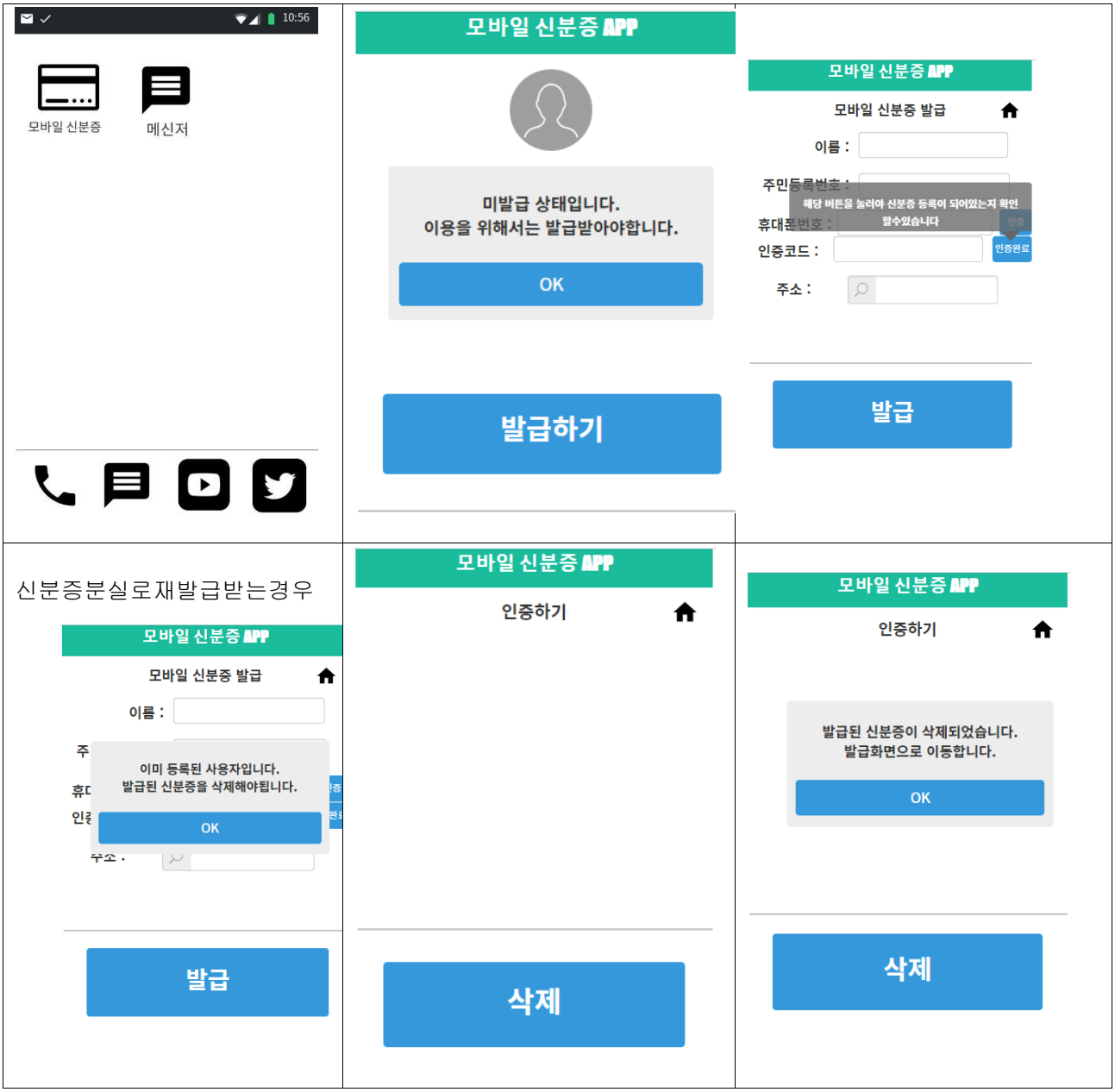
Verifier: Host 의 신원을 확인하고 서비스를 제공하는 자

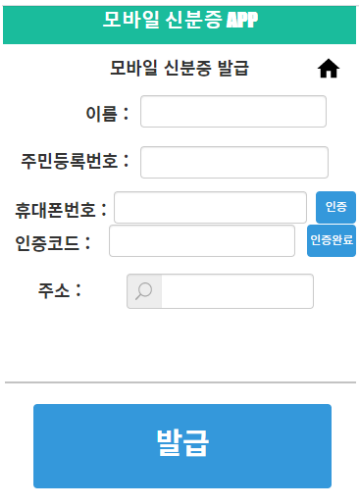
Issuer: 분산신원 발급에 관여하여 해당 신원정보가 실재하는지 검증하기 위한 공인기관

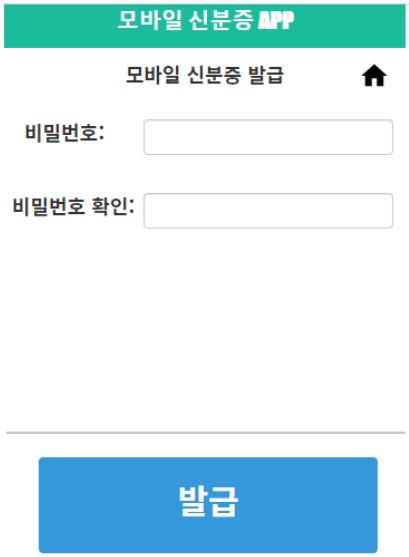
2. External Interface Requirements

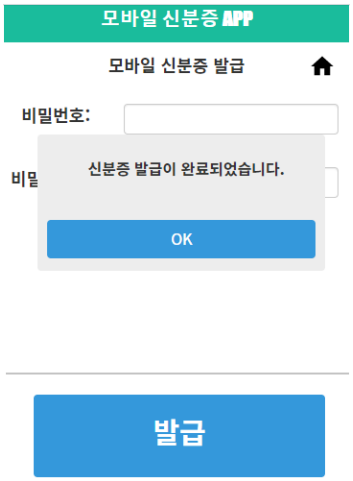
2.1. 사용자 인터페이스 (User Interface)

2.1.1. Host용 모바일 신분증 인터페이스 프로토타입

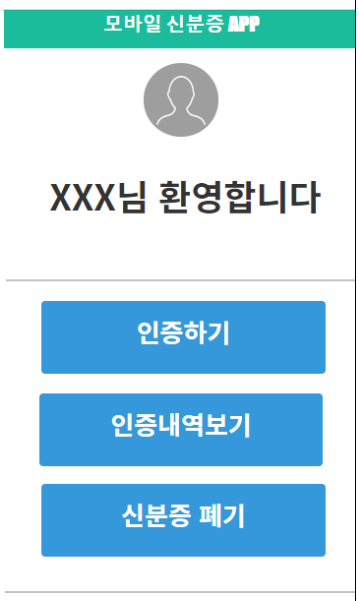




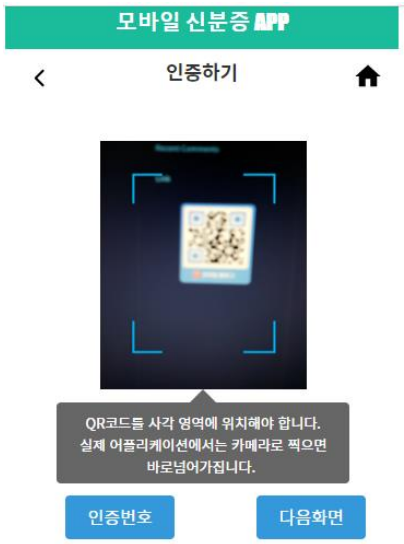




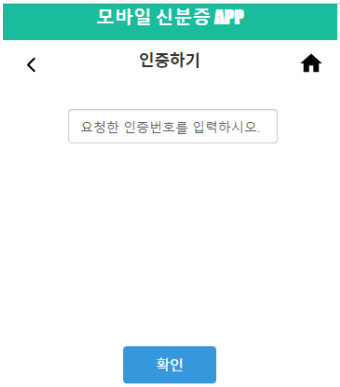
인증완료후메인화면



인증하기를선택한경우



인증번호를선택한경우

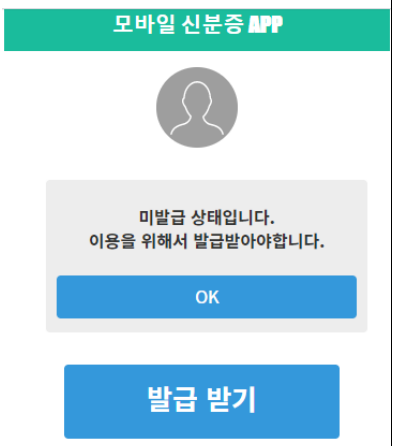


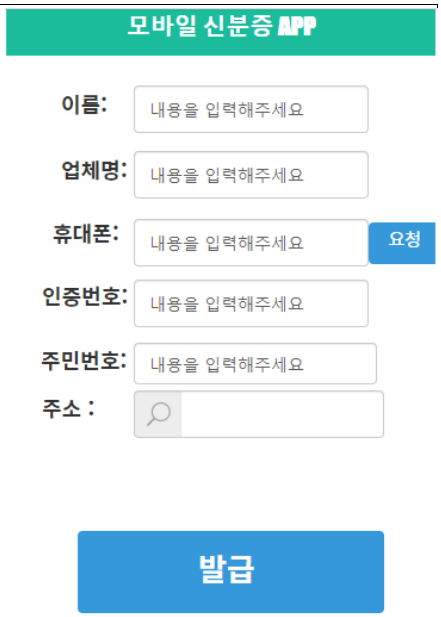
사용자는 Host 용 모바일 어플리케이션을 통해 신분증을 발급받고 인증할 수 있다.

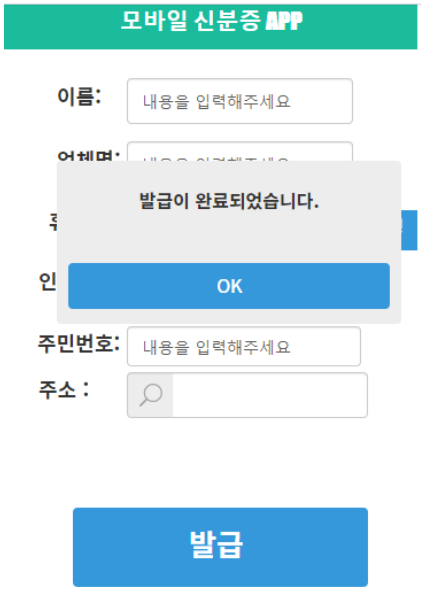
이 어플리케이션에는 신분증발급, 신원인증, 인증내역조회 등의 기능이 제공되며, 사용자는 신분증발급 이후 신원인증 및 인증내역조회 등의 기능을 사용할 수 있다.

사용자는 신원인증 시 취사 선택사항으로 QR 코드 스캔 및 인증코드입력 기능 또한 활용할 수 있다. 인증이 완료된 건에 대해서는 인증내역에 저장이 되어 언제든지 사용자가 언제, 어디서, 어떤 목적으로 인증하였는지 확인할 수 있다. 사용자가 휴대전화를 분실하거나 신분증을 폐기하고자 하는 경우에는 신분증을 비가역적으로 폐기할 수 있다.

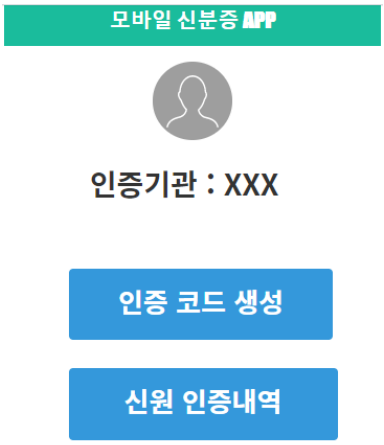
2.1.2. Verifier 용 모바일 신분증 인터페이스 프로토타입



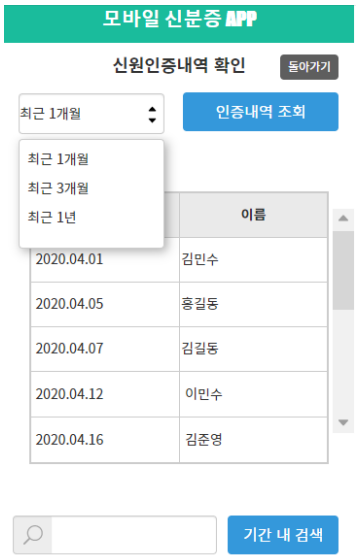




등록후메인화면



인증코드생성을선택한경우

신원인증을선택한경우  	

Verifier 용 모바일 신분증의 경우 신원 요청을 원하는 기관이 사용하게 된다.

기관은 최초에 기관 인증을 받게되면 QR 코드와 인증코드를 발급받을 수 있으며, 해당 인증코드를 인쇄하는 등의 방법으로 Host 에게 내용을 전달하고 인증을 요청할 수 있다.

2.2. 하드웨어 인터페이스 (Hardware Interface)

안드로이드 시스템을 사용하는 스마트폰에서 해당앱을 설치 및 실행할 수 있다. DID 와 연동하기 위해 WIFI 혹은 모바일 데이터를 통해 통신할 수 있어야한다. 생체기능 인식을 활용하고자 한다면 이를 지원하는 센서가 제공되는 스마트폰을 사용해야 한다.

2.3. 소프트웨어 인터페이스 (Software Interface)

안드로이드를 통해 개발된 사용자에게 제공될 어플리케이션과 DID가 연동되기 위한 인터페이스가 필요하다. 이 인터페이스상에서는 사용자가 요구한 기능이 DID상에서 수행될 수 있도록 제공되어야 하며, 신원정보 저장 및 신원정보 조회, 인증내역 저장 및 조회 등의 기능이 연동될 수 있도록 한다.

2.4. 통신 인터페이스 (Communication Interface)

DID와 모바일 어플리케이션의 통신과 서비스 제공자와의 통신간에 노출되어서는 안 될 신원정보들은 공개키암호화 방식을 통해 적절히 암호화 되어야한다. 또한, 블록체인상에 저장될 신원정보들은 해쉬화하여 저장되어 신원인증을 위한 통신간에 노출이 되거나 DID 자체에 대한 참조를 통해 노출이 되어도 신원정보가 유출되지 않도록 해야한다..

3. System Features

3.1. 시스템 기능 1 (System Feature 1)

3.1.1. 설명 및 우선순위 (Description and Priority)

모바일 신분증 어플리케이션을 이용할 수있는 사용자 기능 제공 (우선순위 높음).

3.1.2. 기능 요구사항 (Functional Requirements)

요구사항 분류		기능
요구사항 번호		SFR-001
요구사항 명칭		Host 용 모바일 신분증 어플리케이션 사용자 요구사항
요구사항 상세설명	정의	모바일 신분증 어플리케이션을 이용할 수 있는 사용자 기능 제공
	세부내용	1. 발급 : - 사용자가 모바일 신분증을 사용할 수 있도록 자신의 신원에 대한 정보를 발급받는기능 사용자는 주어진 폼에 맞추어 신원정보를 입력하고, 인증 기관에서 해당 신원정보를 검증하여 모바일 신분증에 신분증을 발급받게 된다. 2. 인증 : - 사용자가 신원을 요청하는 기관에 인증 받을수있게 하는 기능 기관에서 제공하는 QR 코드 및 인증번호를 입력하여 신원인증을 진행할 수 있다. 3. 인증내역보기 -사용자가 인증을 받은 내역들을 스크롤 형태의 GUI 를 통해 쉽게 볼수있다. 인증받은내역들은 어떤기관에서 인증을받았는지, 인증 목적이 무엇이였는지에 대한 정보들이 담겨 있다. 또한 최근 몇개월간의 인증내역 또한 GUI 를 통해 따로 쉽게 조회가 가능하다. 4. 삭제:

		- 사용자가 스마트폰을 분실하는 등의 이유 혹은 기타 이유로 기존에 등록한 신원정보를 통해서 모바일 신분증을 더 이상 사용하지 않기를 원할 시, 블록체 네트워크에서 기존 신원정보를 삭제하기 위한 기능 사용자는 신원정보를 삭제하여 더 이상 해당 신원정보를 이용한 인증절차를 진행할 수 없으며, 도용 및 악용 등의 피해를 방지할 수 있다. 삭제는 비가역적으로 복구가 불가능하며 재이용을 위해서는 재발급 해야 한다.
산출정보		
관련 요구사항		

3.2. 시스템 기능 2 (System Feature 2)

3.2.1. 설명 및 우선순위 (Description and Priority)

모바일 신분증 어플레이이션을 위한 블록체인 네트워크 (우선순위 높음)

3.2.2. 기능 요구사항 (Functional Requirements)

요구사항 분류		기능
요구사항 번호		SFR-002
요구사항 명칭		Verifier 용 모바일 신분증 어플리케이션 사용자 요구사항
요구사항 상세설명	정의	Verifier 용 모바일 신분증 어플리케이션을 이용할 수 있는 사용자 기능 제공
	세부내용	1. 인증 코드 생성: - Verifier 는 어플리케이션을 통해 인증 코드를 생성한다.. Verifier 는 QR 코드를 생성한다. Host 는 Verifier 가 생성한 QR 코드를 스캔하여 신원 인증을 할수있다. Verifier 는 인증번호를 생성한다. Host 는 Verifier 가 생성한 인증코드를 입력하여 신원 인증을 할수있다. 2. 신원 인증 내역 : - Host 가 인증을 받은 내역들을 스크롤 형태의 GUI 를 통해 쉽게 볼수있다. 인증내역에는 신원인증을 받은 Host 의 이름 인증한 날짜와 같은 간략한 정보가 저장이되어있다. 또한 최근 몇개월간의 인증내역 또한 GUI 를 통해 따로 쉽게 조회가 가능하다.
산출정보		
관련 요구사항		

3.3. 시스템 기능 3 (System Feature 3)

3.3.1. 설명 및 우선순위 (Description and Priority)

모바일 신분증 어플레이이션을 위한 블록체인 네트워크 (우선순위 높음)

3.3.2. 기능 요구사항 (Functional Requirements)

요구사항 분류		기능
요구사항 번호		SFR-003
요구사항 명칭		모바일 신분증 어플리케이션을 위한 블록체인네트워크
요구사항 상세설명	정의	모바일 신분증 어플리케이션을 위한 블록체인네트워크
	세부내용	1. 모바일 신분증 사용자의 신분증 발급 요청 어플리케이션에서 신분증 발급을 요청하는 경우 휴대폰 본인인증 API 를 통해 본인인증을 진행한다. 신원이 확인된 사용자는 블록 내에 있는 체인 코드를 통해 WorldState(블록체인 DB)에 입력한 신원정보를 해쉬화 하여 저장한다. 2. 모바일 신분증 사용자 신원인증 요청 어플리케이션에서 신원인증을 요청하는 경우 블록 내부에 있는 신원 인증 요청 체인 코드를 통해 WorldState(블록체인 DB) 에 있는 정보를 확인한다. 올바른 신원 정보인 경우 모바일 신분증에 신원 인증이 완료되었다는 메시지를 전송한다. 3. 모바일 신분증 사용자의 신분증 삭제 요청 어플리케이션에서 신분증 삭제를 요청하는 경우 WorldState(블록체인 DB)에 있는 정보를 통해 요청한 사용자를 검색한다. 블록 내부에 있는 신원 삭제 요청 체인 코드를 통해 수행한다.
산출정보		
관련 요구사항		Private 블록체인인 하이퍼레저 패브릿을 사용

4. Other Nonfunctional Requirements

4.1. 성능 요구 (Performance Requirements)

요구사항 분류		성능
요구사항 번호		PER-001
요구사항 명칭		인증 응답 시간
요구사항 상세설명	정의	사용자 인증 시 응답시간 목표
	세부 내용	◦ 사용자가 주어진 폼에 맞추어 인증 등록을 진행하는 경우 빠른 시간 내에 response 를 주도록 한다.
산출정보		
관련 요구사항		

4.2. 안전 요구 (Safety Requirements)

스마트폰 어플로 이루어진 어플이므로 안전상의 요구는 불필요하다.

4.3. 보안 요구 (Security Requirements)

요구사항 분류	보안 요구사항
요구사항 번호	SER-001
요구사항 명칭	기술적 보안

요구사항 상세설명	정의	기술적 보안 요건
	세부내용	◦ 공통사항 - 암호화키 기반의 데이터 암호화 및 보안대책 강구 - 블록체인의 특성상 사용자 모두가 블록의 내용(개인정보)를 확인할 수 있으므로, 해시를 통해 암호화하여 저장 - 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 - 사용자의 개인정보를 저장하고, 블록체인의 특성상 다른 사용자들이 모두 해당 정보를 확인할 수 있으므로 이에 대한 보안이 반드시 필요하다. - 또한 사용자가 휴대전화를 분실하는 등의 신분증을 잃어버리고, 이를 타인이 확인할 수 있는 경우에 개인정보 유출의 위험이 있으므로 이에 대한 해경 방법 또한 필요하다. - 사용자는 지정된 폼에 맞추어 자신의 정보를 입력하고, 해당 정보는 해시를 통해 암호화 되어 블록에 저장된다.
산출정보		
관련 요구사항		

4.4. 소프트웨어 품질 속성 (Software Quality Attributes)

요구사항 분류	품질
요구사항 번호	QUR-001
요구사항 명칭	신뢰성(reliability)

요구사항 상세설명	정의	신뢰성 개념 정의
	세부내용	◦ 시스템은 통상적인 업무시간 동안 가용성을 보장하여야 하며, 시스템 조건이 무엇이든지 간에 모든 채널에 동일한 자료 및 결과를 생성하고 인도해야 함 ◦ 시스템은 정상상태에서 매일 24 시간 동안 무중단으로 운영되어야함 ◦ 복구할 수 없는 자료의 손실로 이어질 수 있는 거래 오류를 방지하고, 오류가 발생하는 즉시 사용자에게 관련 메시지를 공지할 것 ◦ 사용자의 입력 오류나 시스템의 오류 발생 시 오류메시지를 3 초 이내에 사용자에게 제시하여야 함 ◦ 에러복구, 장애대책 확보 등 신뢰성 있는 서비스환경을 제공
산출정보		
관련 요구사항		

요구사항 분류		품질
요구사항 번호		QUR-002
요구사항 명칭		적응력(adaptability)
요구사항 상세설명	정의	적응력 개념 정의
	세부내용	◦ 스마트폰 어플리케이션으로 이루어진 시스템이므로 대표적으로 사용되는 OS 인 안드로이드 및 IOS 에서 모두 원활히 운영될 수 있어야 함.

산출정보	
관련 요구사항	

요구사항 분류		품질
요구사항 번호		QUR-003
요구사항 명칭		이용가능성(availability)
요구사항 상세설명	정의	이용가능성 개념 정의
	세부내용	◦ 사용자는 시스템 내에서 신원등록 및 인증이 가능해야함
산출정보		
관련 요구사항		

5. Other Requirements

5.1. H/W 제약 조건

해당 시스템이 스마트폰 어플리케이션이므로 보통의 스마트폰에서 사용 가능하도록 한다.

대중적으로 사용하고 있는 안드로이드와 IOS기반의 스마트폰에서 사용할 수 있도록 구성한다.

무선연결이 가능한 경우에 사용 가능하도록 하되, 오프라인에서 사용하는 방법을 찾는다면 오프라인도 지원할 수 있도록 할 것.

5.2. 자원, 인력에 대한 제약 조건

해당 시스템을 구동할 수 있는 스마트폰