
System Model (Sequence Diagram) Document

팀명 : BADID

조원 : 권재승, 조성락, 오하늘

지도교수: 류재철

Document Revision History

| REV# | DATE | AFFECTED SECTION | AUTHOR |
|------|------------|------------------|---------------------|
| 1 | 2020/05/12 | | 권재승, 조성락, 오하늘 |
| | | | |
| | | | |
| | | | |

Table of Contents

| | |
|---|----------|
| 1. INTRODUCTION | 5 |
| 1.1. OBJECTIVE | 5 |
| 2. USE CASE DIAGRAM | 6 |
| 3. SEQUENCE DIAGRAM | 7 |
| 3.1. AMSM_REQ_MONITORING_N001 (SUBSCRIBEESSTATUS) | 7 |

List of Figure

| | |
|---|---|
| FIGURE 1 – USE CASE DIAGRAM | 6 |
| FIGURE 2 – ESE STARTUP SEQUENCE DIAGRAM | 7 |

1. Introduction

1.1.

1.2. Objective

이 문서는 블록체인 기반 아파트 출입 시스템의 시스템 모델(시퀀스 다이어그램)에 대한 내용을 기술하고 있다. 요구사항 명세 단계에서 작성한 유스케이스 다이어그램을 기반으로 각 유스케이스의 상세한 내부 동작 흐름을 시퀀스 다이어그램으로 모델링한다.

2. Use Case Diagram

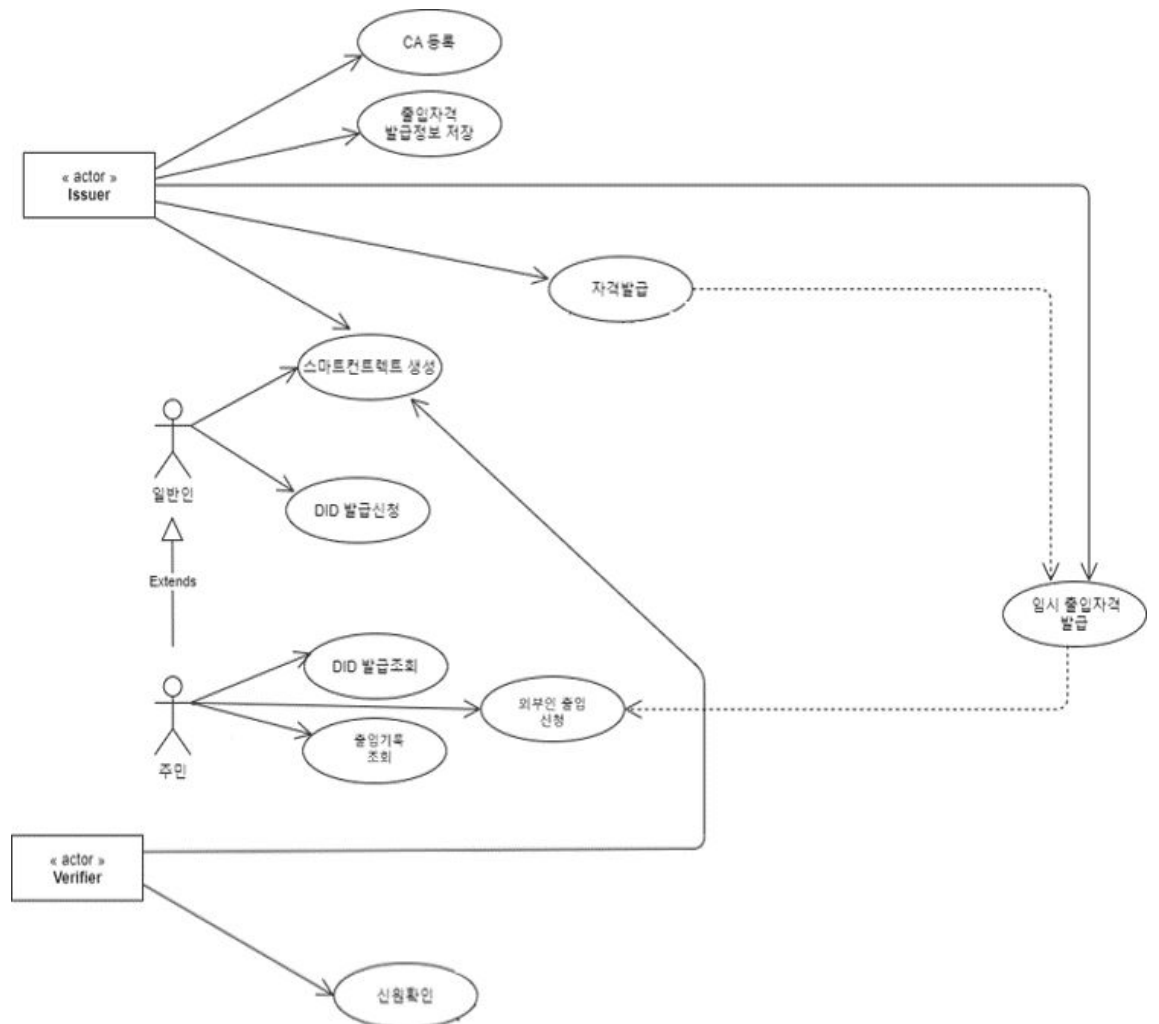
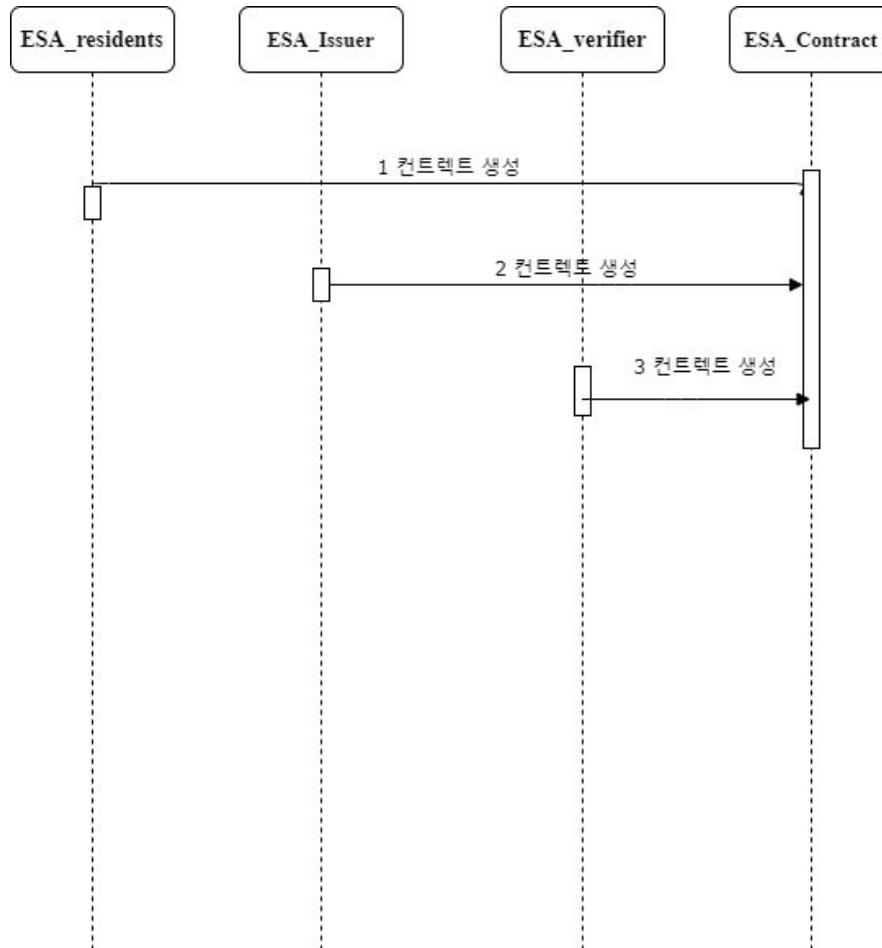


Figure 1 – Use Case Diagram

3. Sequence Diagram

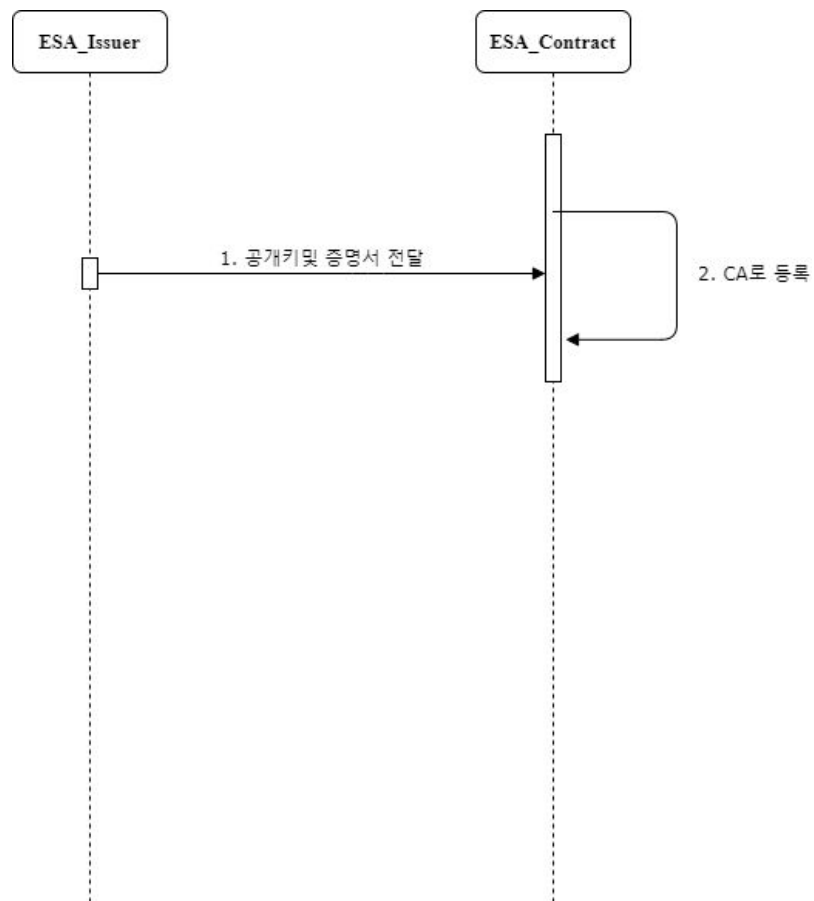
3.1. 스마트 컨트랙트 생성

EAS_resident, EAS_Issuer, EAS_verifier는 블록체인 시스템에 참여하기 위해 각자 스마트컨트랙트를 생성한다



1. 거주자의 스마트컨트랙트를 생성한다
2. Issuer의 스마트컨트랙트를 생성한다.
3. Verifier의 스마트 컨트랙트를 생성한다.

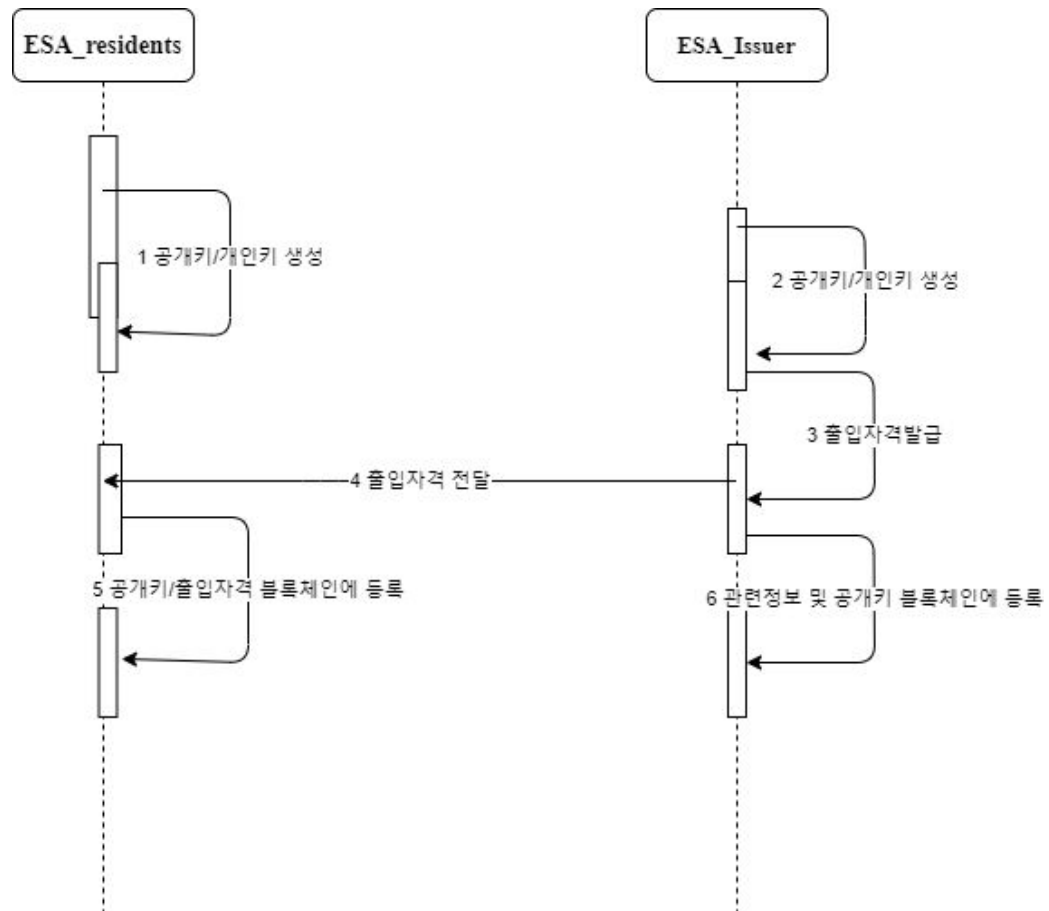
3.2. CA 등록



1. Issuer는 자신의 공개키와 인증서를 블록체인 관리자에게 넘겨준다
2. Issuer의 공개키와 증명서를 보고 판단하여 CA로 지정이 된다.

3.3. 출입자격 발급 정보 저장

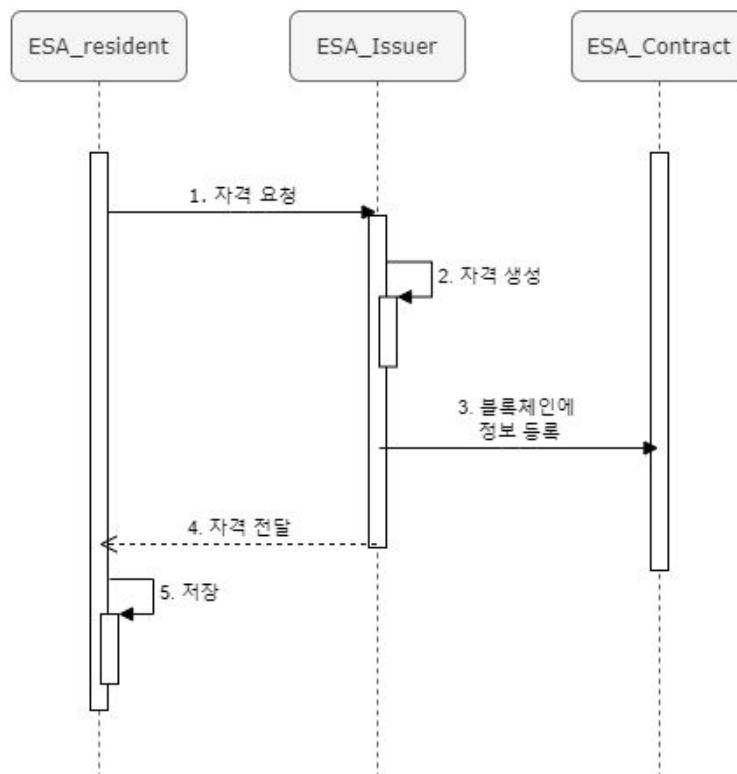
ESA_resident와 ESA_Issuer는 자신만의 공개키/개인키를 생성하고, ESA_Issuer는 resident에게 출입자격을 발급 및 전달한다. 그 후 각자 관련된 정보를 블록체인에 등록한다.



1. 거주자의 공개키/개인키를 생성한다.
2. Issuer의 공개키/개인키를 생성한다.
3. Issuer가 거주민의 출입자격을 발급한다.
4. Issuer가 거주민에게 출입자격을 전달한다.
5. 거주민은 자신의 공개키와 출입자격을 블록체인에 등록한다.
6. Issuer는 출입자격과 관련된 정보를 블록체인에 등록한다.

3.4. 자격발급

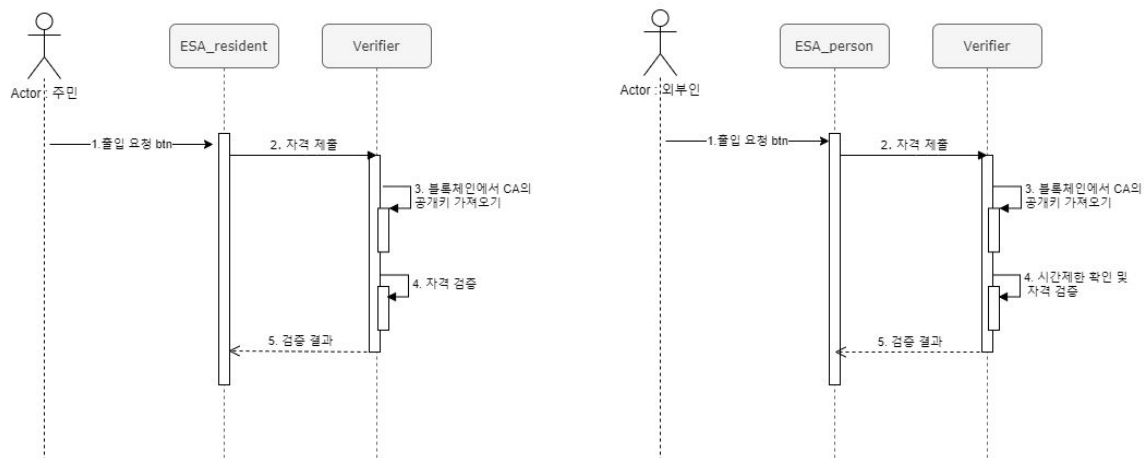
Issuer는 주민에 대한 출입자격을 발급해준다.



1. 주민은 Issuer에게 발급을 요청한다. 이때 자신의 DID와 공개키를 함께 전달한다.
2. Issuer는 전달받은 정보가 유효한지 확인 한 후 자격을 생성해준다.
3. 생성한 자격에 대해서 관련 정보를 블록체인에 등록한다.
4. 생성한 자격을 주민 또는 외부인에게 전달한다.
5. 발급된 자격을 저장한다.

3.5. 신원확인

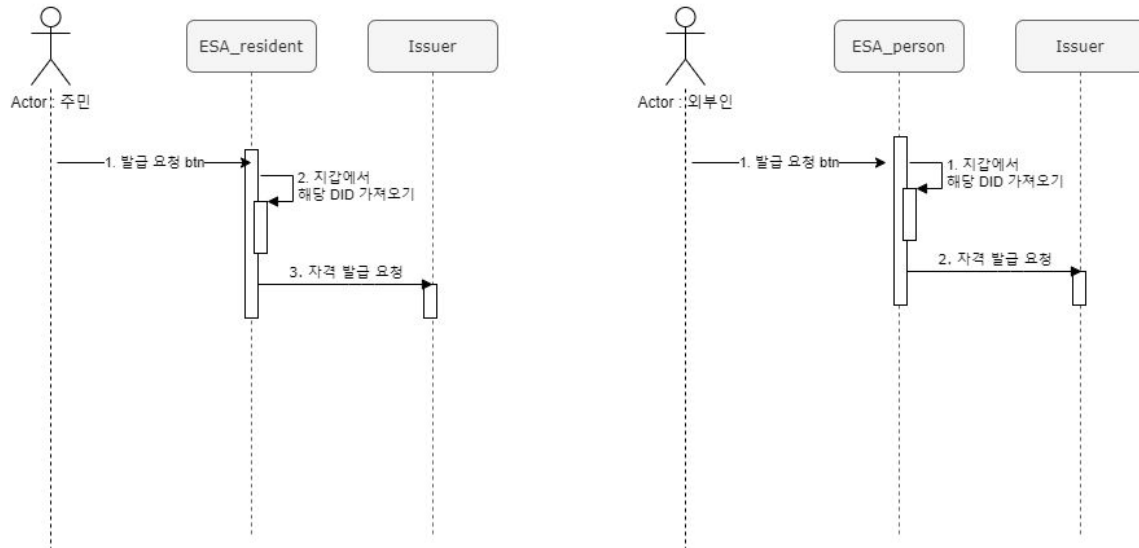
주민 또는 외부인이 verifier에게 자격을 제출하여 출입을 시도한다. verifier는 받은 자격에 대해 검증하여 검증 결과를 전달해준다.



1. 주민 또는 일반인은 어플에서 자격요청하는 버튼을 누른다.
2. 버튼을 누름으로써 verifier에게 자격을 제출한다.
3. verifier는 블록체인에서 CA의 공개키를 가져온다.
4. 가져온 공개키로 받은 자격에 대해서 검증한다.
 - a. 외부인의 경우 제한시간에 대해서도 확인해준다.
5. 검증한 결과에 대해서 주민 또는 일반인에게 전달해준다. 검증 결과가 유효하면 문이 열리고 유효하지 않으면 문이 열리지 않는 것이다.

3.6. 출입자격 발급 신청

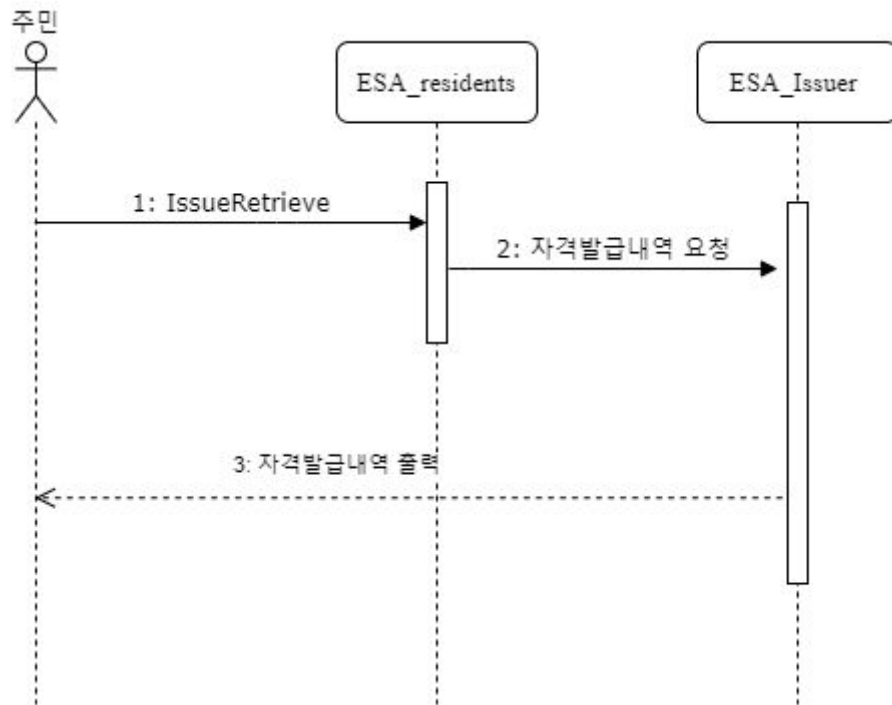
주민 또는 외부인은 출입자격을 Issuer에게 발급을 요청한다. 요청할 때 자신의 DID 정보와 공개키를 보낸다.



1. 주민 또는 외부인은 어플리케이션의 발급 요청 버튼을 누른다.
2. 주민 또는 외부인은 자신의 DID 정보를 Issuer에게 제출하기 위해 지갑에서 가져온다.
3. 자신의 DID 정보와 공개키를 Issuer에게 전달하여 자격 발급을 요청한다.

3.7. 발급 조회

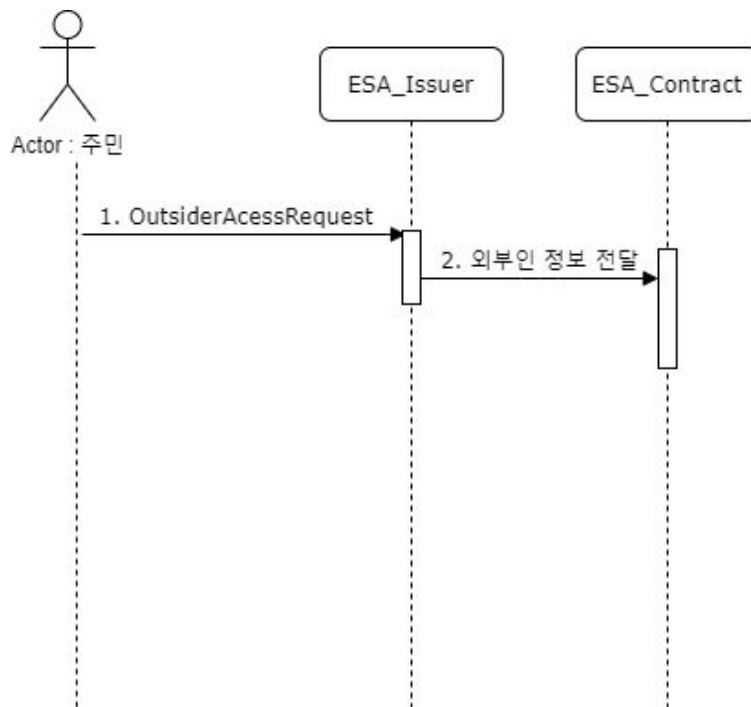
발급 조회는 사용자가 ESA_residents로 ESA_Issuer에게 발급내역을 요청함으로써 ESA_Issuer에게 발급내역을 전달받아 사용자에게 출력해준다.



1. 사용자(주민)는 발급내역 조회 버튼을 누른다.
2. ESA_residents가 ESA_Issuer에게 발급내역정보를 요청한다.
3. ESA_Issuer는 사용자(주민)에게 발급내역정보를 출력해준다.

3.8. 외부인 출입 신청

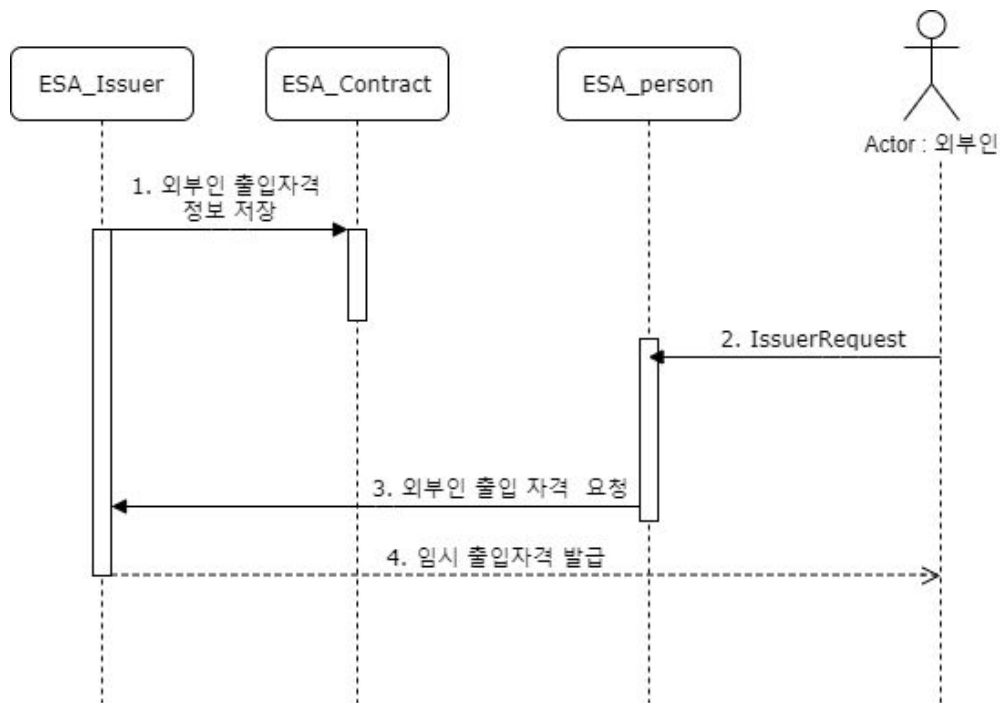
외부인 출입 신청은 ESA_residents가 OutsiderAccessRequest 기능을 호출하여 Issuer에게 외부인에 관한 정보를 전달한다.



1. 사용자는 ESA_residents로서 외부인 출입관리 버튼을 눌러 OutsiderAccessRequest을 기능을 호출한다.
2. ESA_residents에서 외부인의 정보를 ESA_Issuer에게 외부인에 관한 정보를 전달한다.

3.9. 임시 출입자격 발급

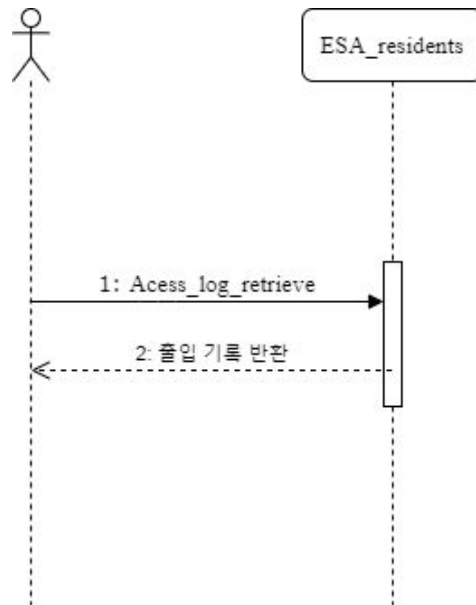
Issuer는 외부인에 관한 정보를 블록체인에 등록하여 임시로 출입자격을 부여해준다.



1. ESA_Issuer는 외부인 출입자격 정보를 ESA_Contract를 통해서 블록체인 올린다.
2. 외부인은 ESA_person로서 IssuerRequest를 호출한다.
3. EAS_person은 ESA_Issuer에게 출입자격을 요청한다.
4. ESA_Issuer는 외부인에게 임시 출입 자격을 발급한다.

3.10.출입기록 조회

출입기록 조회는 ESA_residents가 Acess_log_retrieve 기능이 호출될 때 마다 이 기능을 출입기록을 사용자에게 알려준다.



1. 사용자는 어플리케이션을 통해 출입 기록 조회 버튼 조작을 통해 출입정보를 요청한다.
2. 어플리케이션의 데이터베이스에서 출입기록 정보를 가져와 사용자에게 반환한다.