

Dipartimento di Ingegneria e Scienza dell’Informazione

**Progetto:**

**ACCESS light**

**Titolo del documento:**

**Specifica dei requisiti**

**Document Info**

|  |  |  |  |
| --- | --- | --- | --- |
| Doc. Name | *D2-ACCESS-LIGHT\_AnalisiRequisiti* | Doc. Number | SR2 |
| Description | Documento di specifica dei requisiti funzionali e non funzionali con diagrammi dei casi d’uso, tabelle, diagrammi di contesto e dei componenti | | |

**INDICE**

Sommario

[**1.** **Requisiti Funzionali** 3](#_Toc116390376)

[**2.** **Requisiti Non Funzionali** 6](#_Toc116390377)

[**3.** **Analisi del Contesto** 9](#_Toc116390378)

[**3.1.** **Utenti e sistemi esterni** 9](#_Toc116390379)

[**3.2.** **Diagramma di contesto** 10](#_Toc116390380)

[**4.** **Analisi dei Componenti** 11](#_Toc116390381)

[**4.1.** **Definizione dei componenti** 12](#_Toc116390382)

[**4.2.** **Diagramma dei componenti** 13](#_Toc116390383)

**Scopo del documento**

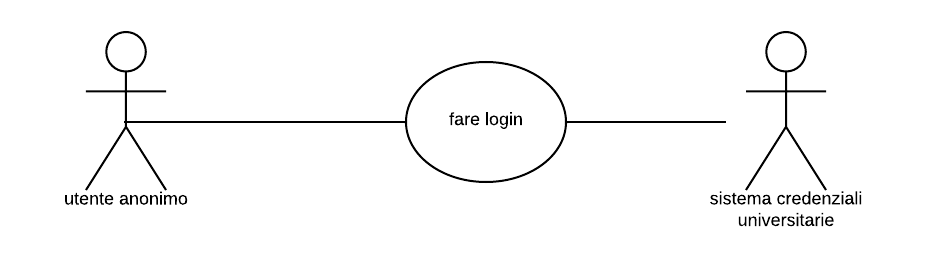
Il presente documento riporta la specifica dei requisiti di sistema del progetto ACCESS light usando diagrammi in Unified Modeling Language (UML) e tabelle strutturate. Nel precedente documento sono stati definiti gli obiettivi del progetto (PERCHE') e i requisiti (COSA) usando solo il linguaggio naturale. Ora i requisiti vengono specificati usando sia il linguaggio naturale sia linguaggi più formali e strutturati, UML per la descrizione dei requisiti funzionali e tabelle strutturate per la descrizione dei requisiti non funzionali. Inoltre, tenendo conto di tali requisiti, viene presentato il design del sistema con l’utilizzo di diagrammi di contesto e dei componenti.

1. **Requisiti Funzionali**

Nel presente capitolo vengono riportati i requisiti funzionali (RF) del sistema utilizzando il linguaggio naturale e Use Case Diagram (UCD) scritti in UML.

**Utente Anonimo**

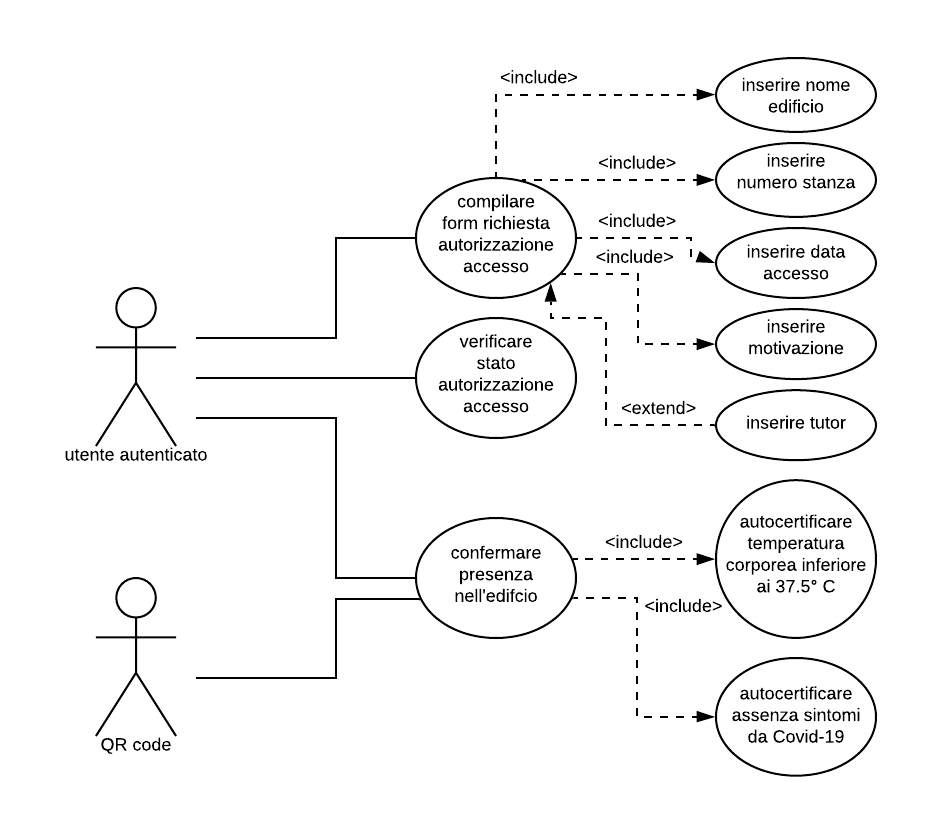
1. **Accesso protetto al sistema**



**Utente autenticato**

1. **Richiesta autorizzazione accesso**
2. **Verifica autorizzazione accesso**
3. **Conferma presenza nell’edificio**

**…**



**Descrizione Use Case “verificare stato autorizzazione accesso”**

Titolo: verificare stato autorizzazione accesso

Riassunto:

Questo use case descrive come avviene la verifica dello stato di autorizzazione di accesso

Descrizione:

1. L’utente autenticato seleziona il menù “Autorizzazioni” [exception 1]
2. Il sistema mostra la lista delle autorizzazioni valide sia passate sia future visualizzando solo data, nome edificio a cui si può accedere e nome autorizzatore
3. L’utente seleziona una specifica autorizzazione
4. Il Sistema mostra oltre alla data, nome edificio a cui si può accedere e nome autorizzatore anche il numero di stanza, la motivazione e l’eventuale tutor indicato in fase di richiesta [extension 1] [exception 2]

Exceptions

[exception 1] Se non ci sono autorizzazioni valide viene fornito un apposito messaggio

[exception 2] Se non è stato indicato un tutor in fase di richiesta il campo rimane vuoto

Extension

[extension 1] È possibile esportare queste informazioni in format XML

**Descrizione Use Case “autocertificare assenza sintomi da Covid-19”**

Titolo: autocertificare assenza sintomi da Covid-19

Riassunto:

Questo use case descrive come avviene l’autocertificazione di assenza sintomi da Covid-19

Descrizione:

1. L’utente autenticato seleziona il menù “Check-in”
2. Il sistema chiede di confermare di non avere tosse e difficoltà respiratorie [exception 1]
3. Il sistema chiede di confermare di non avere sintomi gastrointestinali (nausea/vomito, diarrea) [exception 1]
4. Il sistema chiede di confermare di non avere alterazione improvvisa del gusto e/o dell’olfatto (anosmia/iposmia) [exception 1]
5. Il sistema non procede nella schermata successiva fino a quando non vengono confermate tutte e tre le richieste [extension 1]

Exceptions

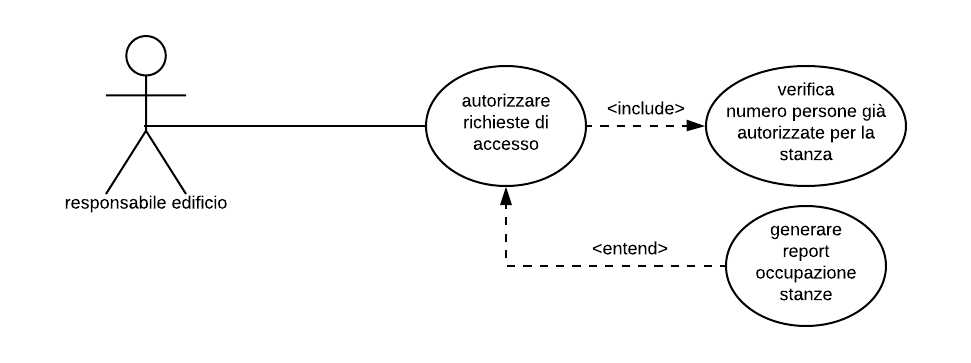
[exception 1] Se non viene data conferma viene fornito un apposito messaggio

Extension

[extension 1] È possibile inviare al proprio indirizzo mail copia di questa autocertificazione

**Responsabile Edificio**

1. **Autorizzazione accesso**



**[… dettagliare tutti i rimanenti RF]**

1. **Requisiti Non Funzionali**

Nel presente capitolo vengono riportati i requisiti non funzionali (RNF) del sistema utilizzando tabelle strutturate e specificando misure facilmente verificabili.

1. **Privacy**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Codice della privacy | Per codice dalla privacy intendiamo la norma della Repubblica Italiana, emanata con il Decreto legislativo 30 giugno 2003, n. 196, in vigore dal 1º gennaio 2004. | Conforme |
| Regolamento per la protezione dei dati (GDPR) | Il Regolamento Generale sulla Protezione dei Dati in sigla RGPD (o GDPR in inglese General Data Protection Regulation), ufficialmente regolamento (UE) n. 2016/679, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018. | Conforme |
| … | … | … |

1. **Sicurezza**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Trasmissione dati autenticazione | Modalità di trasmissione delle credenziali raccolte in fase di autenticazione | Utilizzo protocollo https |
| Raccolta dati tramite form | Modalità di trasmissione dei dati raccolti tramite i form proposti dall’applicazione | Utilizzo protocollo https |
| … |  | … |

1. **Scalabilità**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Elaborazione con un numero crescente di utenti | Capacità del sistema di gestire un numero crescente di utenti in simultanea | Garantita fino a 500 utenti in simultanea |
| Memorizzazione dei dati con un numero alto di utenti | Capacità del sistema di gestire i dati generati da un alto numero di utenti | Garantita fino a 500 utenti |
| … |  | … |

1. **Affidabilità**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Tempo medio di malfunzionamento | Per tempo medio di malfunzionamento si intende il numero massimo di giorni all’anno, ore al mese, minuti al giorno in cui il sistema non è raggiungibile. | 99% ("due nove") che corrisponde a 3,65 giorni all’anno, 7,31 ore al mese, 14,40 minuti al giorno |
| Disponibilità | Per disponibilità si intende la probabilità del software di non guastarsi entro le prime 10.000 ore di funzionamento | 97%, quindi il software ha il 97% di probabilità di non guastarsi entro le 10.000 ore di funzionamento |
| … |  | … |

1. **Logging & Monitoring**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Logging & Monitoring | Registrazione e monitoraggio di tutti gli accessi e di tutti gli eventi. | Meccanismo nativo per la registrazione e il monitoraggio su file di testo di tutti gli accessi e di tutti gli eventi con data ed ora. |
| … |  | … |

1. **Multilingua**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Multilingua | Lingue previste su tutte le schermate di cui è composto il software. | Schermate disponibili in lingua italiana ed in lingua inglese. |
| … |  | … |

1. **Prestazioni**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Avvio applicazione | Tempo massivo di avvio dell’applicazione da parte dell’utente sul proprio SmartPhone. | Quando l’utente avvia l’applicazione, l’applicazione deve essere disponibile entro 3 secondi |
| Transizione tra una schermata e l’altra | Tempo massivo di transizione tra una schermata e la successiva da parte dell’utente sul proprio SmartPhone. | La transizione tra una schermata e l’altra all’interno dell’applicazione dovrà avvenire entro 2 secondi |
| … |  | … |

1. **Compatibilità**

|  |  |  |
| --- | --- | --- |
| **Proprietà** | **Descrizione** | **Misura** |
| Compatibilità con Android | Sistema operativo e versione a partire dalla quale l’applicazione può essere installata | L’applicazione deve essere compatibile con Android 5.0 o superiori |
| Compatibilità con iOS | Sistema operativo e versione a partire dalla quale l’applicazione può essere installata | L’applicazione deve essere compatibile con iOS 12 o superiori |
| … |  | … |

**[… dettagliare tutti i rimanenti RNF]**

1. **Analisi del Contesto**

Nel presente capitolo viene discusso il contesto di funzionamento del sistema, fornendo una descrizione testuale e una rappresentazione grafica basata su Context Diagram.

Nella seguente parte della sezione vengono presentati gli attori e i sistemi esterni con cui l’applicazione ACCESS light si interfaccerà.

* 1. **Utenti e sistemi esterni**
     1. **User**

Colui che utilizza l’applicazione per accedere agli edifici universitari.

Il **RF1** identifica l’utente anonimo e l’utente autenticato, specificando poi per questi attori i **RF 2, 3, 4, 5**.

* + 1. **Responsabile di edificio**

Identificato nel **RF1**, il responsabile edificio è colui che monitora ed autorizza gli accessi, come specificato da **RF6**.

* + 1. **QR code**

Il sistema usato per confermare la presenza nell’edificio, come specificato nel **RF5**.

* + 1. **Sistema di credenziali universitarie**

Usato per autenticare l’utente utilizzatore dell’applicazione, come nel **RF2**.

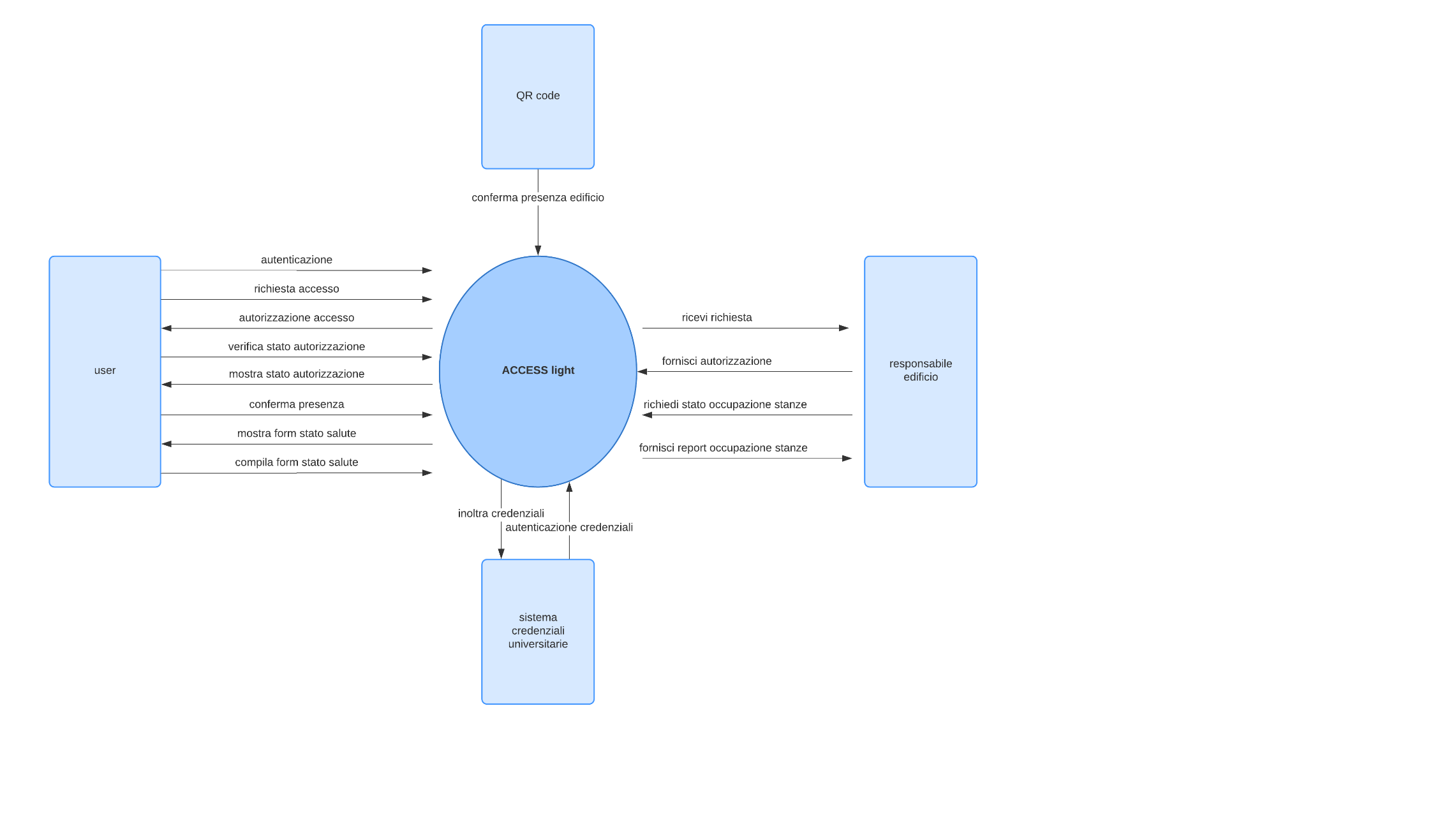
* 1. **Diagramma di contesto**

L’utente esegue l’autenticazione con l’applicazione, come da **RF2**. Richiede l’autorizzazione per poter accedere ad un edificio **RF3**. Viene notificato/riceve la conferma di autorizzazione per l’accesso ad un edificio **RF4**. Può inoltre richiedere di controllare lo stato della richiesta di autorizzazione che gli viene mostrato quindi dall’applicazione **RF4**. Tramite l’applicazione, l’utente, conferma l’ingresso in un edificio **RF5**. L’utente dichiara il suo stato di salute tramite la compilazione di una form che gli viene mostrata dal sistema **RF5**.

Il responsabile riceve le richieste di accesso degli utenti, può quindi approvarle o respingerle, anche sulla base dell’occupazione delle stanze specificate nelle richieste di accesso **RF6**. Infine, può richiedere dei report sull’effettiva presenza negli edifici e occupazione delle stanze.

Per soddisfare il **RF2**, le credenziali degli utenti vengono inviate al sistema Sistema di Credenziali Universitarie per validarle e quindi autenticarne l’accesso all’applicazione.

Il sistema di QR code permette di convalidare la presenza all’interno dell’edificio degli utenti, come da **RF5**.



**Figura 1. Diagramma di contesto per l’applicazione ACCESS light**

La Figura 1 mostra le principali interazioni tra attori o sistemi esterni e l’applicazione ACCESS light. Segue una descrizione delle interazioni evidenziate dal diagramma.

1. **Analisi dei Componenti**

Nel presente capitolo viene presentata l’architettura in termini di componenti interni al sistema definiti sulla base dei requisiti analizzati nei precedenti documenti, minimizzando il livello di *coesione*. Viene poi adottato l’uso di Component Diagram per rappresentare l’interconnessione tra i vari componenti, identificando quindi le interfacce tra questi e verso sistemi esterni. Viene infine valutato il livello di *accoppiamento* tra i componenti.

* 1. **Definizione dei componenti**

In questa sezione vengono definiti i componenti.

* + 1. **Gestione autenticazione**

*Motivazione.* Dato il **RF2**, l’autenticazione degli utenti si appoggia al sistema di credenziali universitario. È stato quindi identificato un componente **Gestione autenticazione**, che si interfaccerà con il sistema di gestione delle credenziali di ateneo, gestendo la creazione delle richieste d’accesso dell’utente e il check-in negli edifici.

In particolare, il componente gestisce il login dell’utente autenticandolo tramite il sistema di credenziali di ateneo, mantenendo poi attiva la sessione utente all’interno dell’applicazione.

**Coesione**: livello **7** – funzionale.

*Spiegazione:* Il componente gestisce la funzionalità di autenticazione dell’utente all’interno dell’app, tramite il sistema di ateneo.

* + 1. **Pagina Check-In Edificio**

*Motivazione.* È stato considerato il **RF5** ed il mock-up della schermata check-in in Figura 4.2 Documento AR01 Sezione Front-End).

È stato quindi definito il componente **Pagina Check-In Edificio** allo scopo di gestire la parte di front-end della funzionalità di check-in in un edificio dell’ateneo.

Il componente implementa la sotto-pagina dell’app utilizzata dagli utenti per gestisce la procedura che l’utente segue per confermare l’ingresso, inquadrando il codice QR in portineria e compilando quindi il form sullo stato di salute.

**Coesione**: livello **4** – procedurale.

*Spiegazione:* Il componente gestisce l’intera procedura che l’utente segue per eseguire il check-in e confermare l’ingresso in un edificio. Prima viene chiesto di inquadrato il codice QR in portineria che identifica l’edificio, poi viene fatto compilare il form sullo stato di salute.

* + 1. **Pagina gestione autorizzazioni utente**

*Motivazione.* Dato il **RF3**, il sistema deve permette agli utenti di richiedere l’autorizzazione per l’accesso agli edifici. Inoltre, secondo il **RF4**, l’utente può verificare lo stato delle autorizzazioni per le proprie richieste.

Definiamo quindi il componente **Pagina gestione autorizzazioni utente** allo scopo di permettere all’utente la creazione di nuove richieste di accesso.

**[...descrizione componente da completare]**

* + 1. **Gestione responsabili edificio**

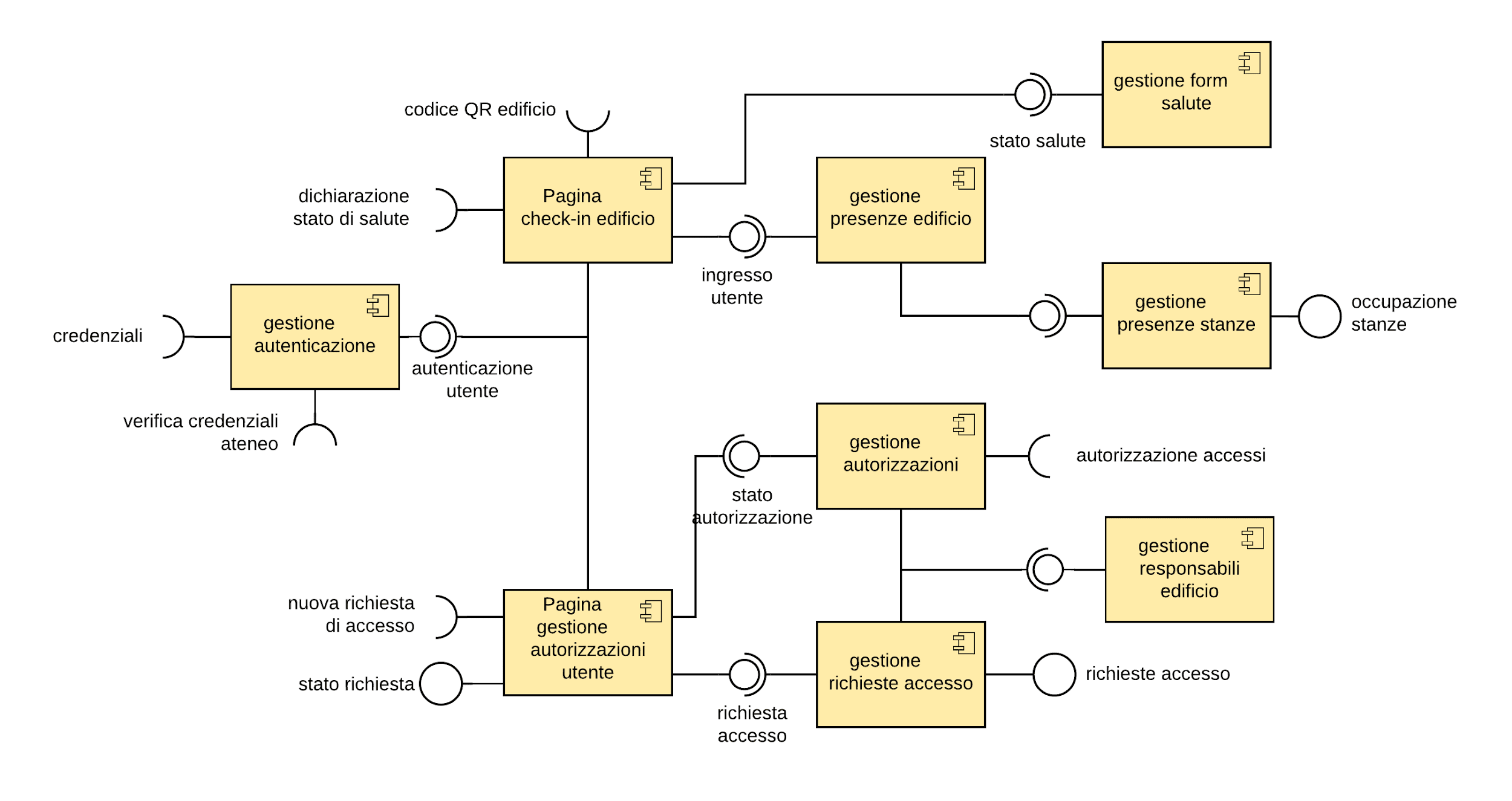
*Motivazione.* Per il **RF6**, il responsabile di edificio può autorizzare gli accessi degli utenti, confermando o meno la richiesta di accesso degli utenti.

Definiamo quindi un componente **Gestione responsabili di edificio**, che permette la gestione dei responsabili di edificio, dando loro la possibilità di autorizzare o meno le richieste di accesso.

**[...descrizione componente da completare]**

**[… dettagliare tutti i rimanenti componenti]**

* 1. **Diagramma dei componenti**



**Figura 2. Diagramma dei componenti per l’applicazione ACCESS light**

La Figura 2 mostra i componenti di sistema e la loro interconnessione. A seguire una descrizione dei componenti e delle interfacce presenti nel diagramma.

* + 1. **Gestione autenticazione**

*Descrizione*: il componente si occupa della funzionalità di autenticazione tramite il sistema di credenziali di ateneo. Include una pagina per il login per il logout dell’utente. L’interfacciamento con il server remoto di ateneo. E la gestione della sessione utente all’interno dell’app.

*Interfaccia richiesta – credenziali*. Le credenziali includono mail e password. Sono richieste all’utente per la convalida sul sistema di ateneo.

*Interfaccia richiesta – verifica credenziali di ateneo.* La convalida delle credenziali include la conferma o il rifiuto delle credenziali, inclusi eventuali errori dovuti ad utenti inesistenti o account bloccati. La conferma di convalida delle credenziali viene richiesta al sistema di ateneo. Il sistema di ateneo può convalidare o meno le credenziali dell’utente, permettendo o negando l’accesso all’app.

*Interfaccia fornita – Autenticazione utente.* La sessione di autenticazione dell’utente è condivisa all’interno dell’applicazione. Questa include dati relativi al nome dell’utente, metodo di autenticazione, e data ultimo log-in.

**[… dettagliare tutti i rimanenti componenti e interfacce]**