



# RENTAPP

## Secure System Design

Ambrosio Aniello - M63001343

Aramu Stefano - M63001348





# Panoramica

La finalità del progetto è rappresentata dall'apprendimento dell'attuazione di tecnologie che permettono di rendere una **web app** sicura.

L'applicazione selezionata per il caso di studio offre la possibilità di effettuare prenotazioni per il noleggio da parte di utenti "clienti" di autoveicoli messi a disposizione da utenti "gestori".

Le scelte progettuali sono state effettuate tenendo conto del documento **"Security and Privacy Controls for Information Systems and Organizations"** fornito dal NIST nella **"SP 800-53, Rev. 5"**, nella quale vengono specificati i vari **controlli** da implementare per garantire un certo security level.

In una fase preliminare sono state eseguite sull'applicazione di partenza tecniche di **threat modeling** al fine di identificare le debolezze del sistema in modo da poter applicare al Design dell'applicazione un'opportuna riconfigurazione in grado di eliminare le vulnerabilità evidenziate.

Al termine dell'applicazione delle tecnologie è stato rieffettuato sull'architettura ottenuta il threat modeling al fine di osservare i



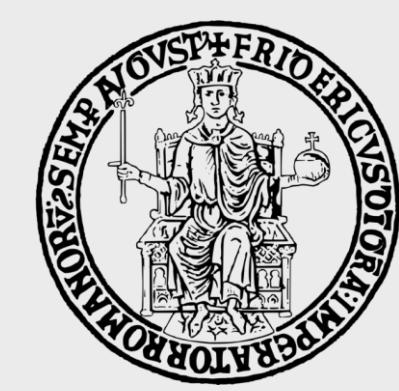
# Requisiti fondamentali di sicurezza

I tre requisiti fondamentali da garantire per 'proteggere il sistema informatico' sono:

- ✓ Confidenzialità
- ✓ Integrità
- ✓ Availability

Ai tre requisiti fondamentali poi si affiancano altri controlli specifici:

- ✓ Authenticity
- ✓ Accountability

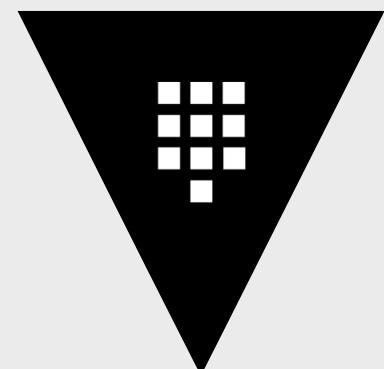


# Confidentiality

Questo termine copre due concetti:

- ✓ Data Confidentiality: le informazioni private non devono essere rese disponibili ad individui non autorizzati
- ✓ Privacy: rappresenta l'insieme di controlli da implementare per permette ad un utente di controllare in maniera precisa chi può accedere o no alle proprie informazioni

AZIONE INTRAPRESA:



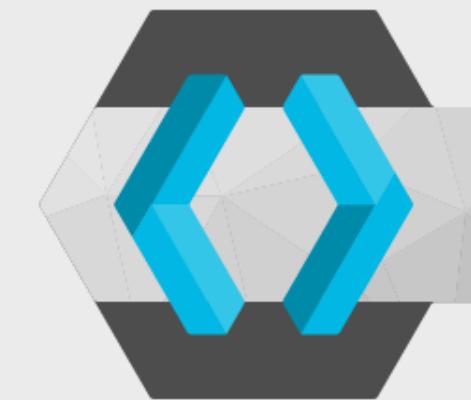
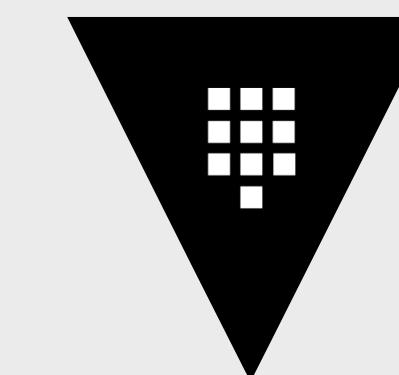


# Integrity

Questo termine copre due concetti:

- ✓ Data Integrity: ci assicura che le informazioni e i programmi possano essere cambiati solo da persone autorizzate e attraverso specifiche manipolazioni.
- ✓ System Integrity: garantisce che un sistema possa funzionare nel modo previsto anche se vi è una manipolazione deliberata o inavvertita del sistema.

AZIONE INTRAPRESA:



JPA  
HIBERNATE



# Availability

Richiede di garantire che il servizio funzioni sempre e per utenti autorizzati.



# Authenticity

È la proprietà di un messaggio, o di chi lo invia, di essere genuino e poterne verificare la fedeltà.

AZIONE INTRAPRESA:



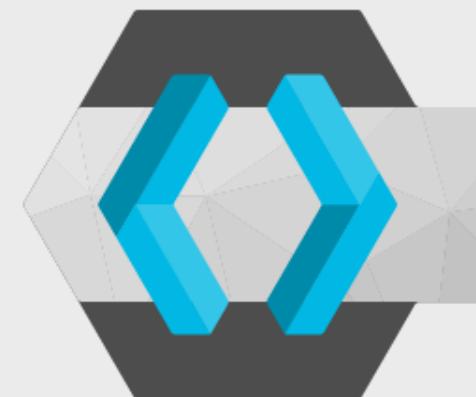


# Accountability

È la capacità di un sistema di identificare un singolo utente e di determinarne le azioni e il suo comportamento all'interno del sistema stesso.

Tale proprietà si basa sulla concezione che gli individui siano responsabili delle loro azioni all'interno del sistema.

AZIONE INTRAPRESA:





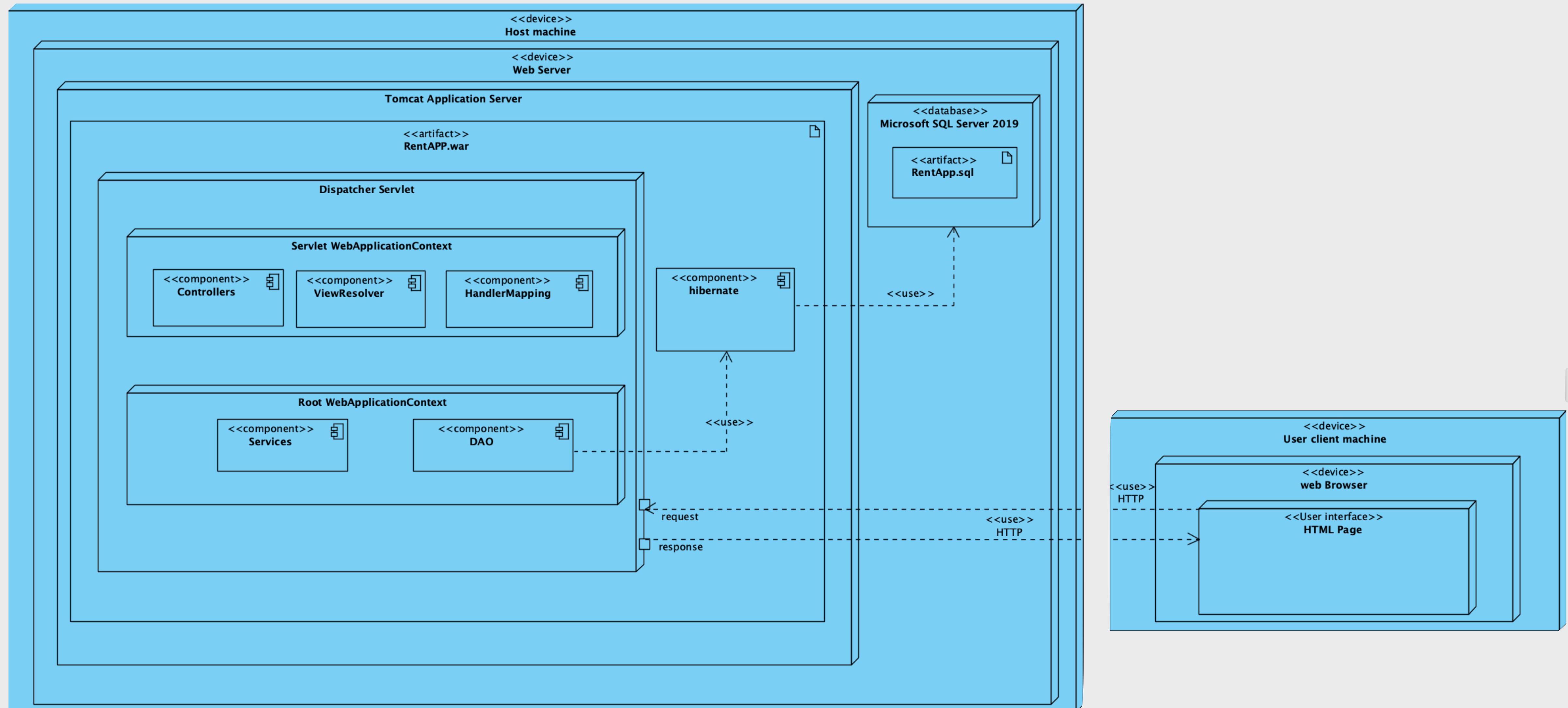
# Architettura

L'idea di base è realizzare l'applicazione come un' **architettura a microservizi**, inseriti in container e messi in esecuzione in un Docker Compose in modo da avere i vari microservizi connessi alla stessa subnet.

(Si potrebbe trasferire la rete di Docker su cloud in fase di produzione)



# Deployment Diagram

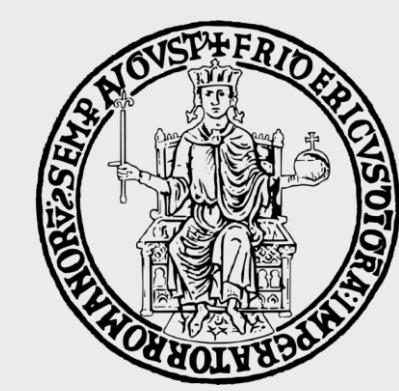




# Architettura

Più nello specifico l'applicazione monolitica è stata divisa in più microservizi:

- ▶ Tramite Spring MVC, eseguito su un web server Apache Tomcat 9.0.12, è stata realizzata la logica di Business separandola rispettivamente in tre controller che gestiscono:
  - ▶ **Area pubblica**
  - ▶ **Gestione degli Autonoleggi da parte dei gestori**
  - ▶ **Gestione delle Prenotazioni per il noleggio da parte di un cliente**
- ▶ Tramite Keycloak è stata realizzata la logica di Registrazione al servizio e di 'Identity and Access Management'.
- ▶ Un database MSSQL che è collocato in un container esterno all'applicazione ma connesso alla stessa subnet, garantisce la persistenza dei dati.

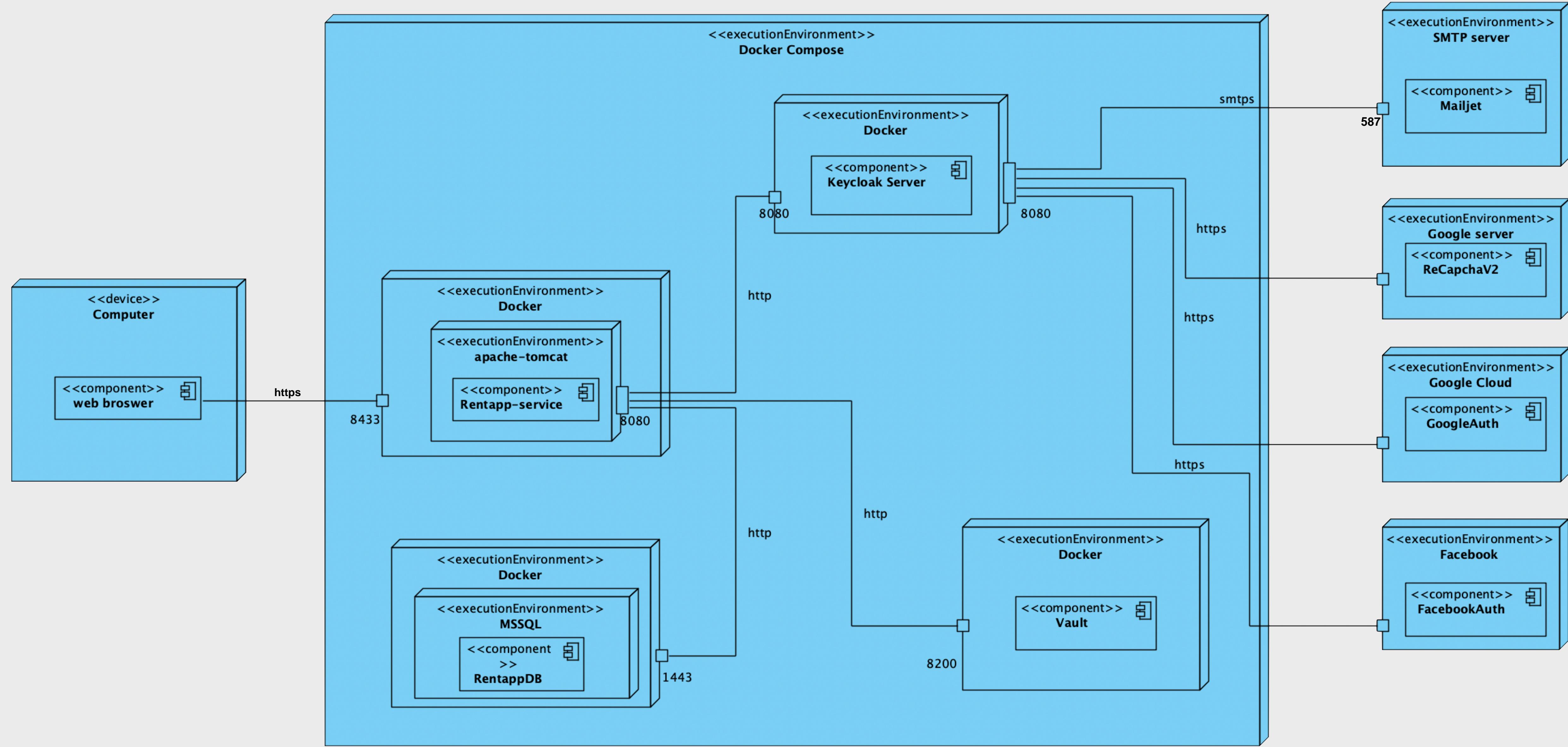


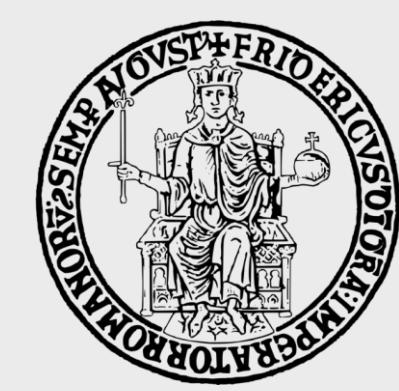
# Architettura

- ▶ Tramite Hashicorp Vault le informazioni che non devono essere inserite all'interno della logica di controllo vengono conservate in modo sicuro e rese accessibili solo a seguito di un processo di autenticazione.  
In particolare, vi sono state conservative le credenziali per accedere al Database SQL. Tale scelta è stata presa al fine di evitare l'hard Coding delle credenziali nel codice della logica di business.
- ▶ Un server SMTP 'MailJet' gestisce il corretto invio delle comunicazioni tramite mail agli utenti da parte di Keycloak che vi comunica tramite protocollo StartTLS.



# Deployment Diagram

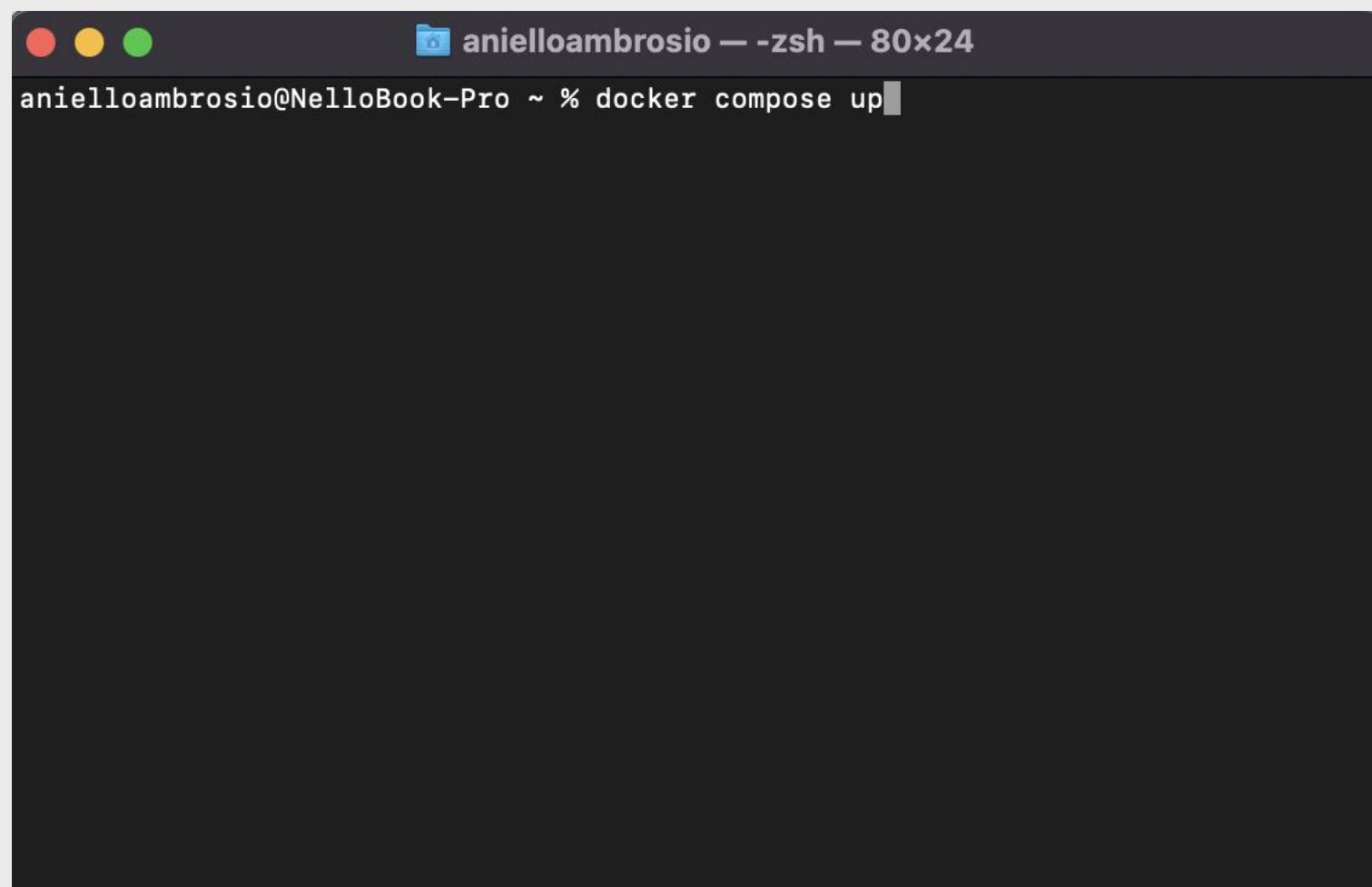




# Considerazioni

- ▶ L'utilizzo di docker consente la messa in esecuzione dei microservizi all'interno dei container, garantendo un livello di isolamento elevato per quest'ultimi.  
I container, generati dalle immagini dei vari microservizi, sono messi in esecuzione tramite docker compose che ne garantisce il funzionamento.

```
1 version: '3.8'
2
3 networks:
4   rentweb:
5     driver: bridge
6     ipam:
7       config:
8         - subnet: 172.21.0.0/16
9           gateway: 172.21.0.1
10
11 services:
12   db:
13     container_name: db
14     image: sqllimage
15     restart: unless-stopped
16     ports:
17       - 1433:1433
18     networks:
19       rentweb:
20         ipv4_address: 172.21.0.4
21     environment:
22       - ACCEPT_EULA=1
23       - MSSQL_PID=Developer
24       - MSSQL_USER=SA
25       - MSSQL_SA_PASSWORD=Root12345_
26       - MSSQL_DATA_DIR=/var/opt/mssql/data
27       - MSSQL_LOG_DIR=/var/opt/mssql/log
28       - MSSQL_BACKUP_DIR=/var/opt/mssql/backup
29       - MSSQL_RPC_PORT=135
30
31   vault:
32     container_name: vault
33     image: vaultfinal
34     restart: unless-stopped
35     ports:
36       - 8200:8200
37     networks:
38       rentweb:
39         ipv4_address: 172.21.0.5
40     environment:
41       - VAULT_ADDR=http://0.0.0.0:8200
42       - VAULT_DEV_ROOT_TOKEN_ID="hvs.Klr7WSS9QJFx5StuD5fmd0Qf"
43     cap_add:
44       - IPC_LOCK
45
46
47   keycloakcp:
48     container_name: keycloak
49     image: keycloakfinalv3
50     ports:
51       - 8080:8080
52     environment:
53       - KEYCLOAK_ADMIN: admin
54       - KEYCLOAK_ADMIN_PASSWORD: admin
55       - PROXY_ADDRESS_FORWARDING: true
56     networks:
57       rentweb:
58         ipv4_address: 172.21.0.3
59     volumes:
60       - ./realm.json:/tmp/realm.json
61     restart: unless-stopped
62
63   rentapp:
64     container_name: rentapp
65     image: rentapp.war
66     ports:
67       - 9001:8080
68       - 8443:8443
69     expose:
70       - 8443:8443
71     networks:
72       rentweb:
73         ipv4_address: 172.21.0.2
74     restart: unless-stopped
75
76 |
```





# Considerazioni

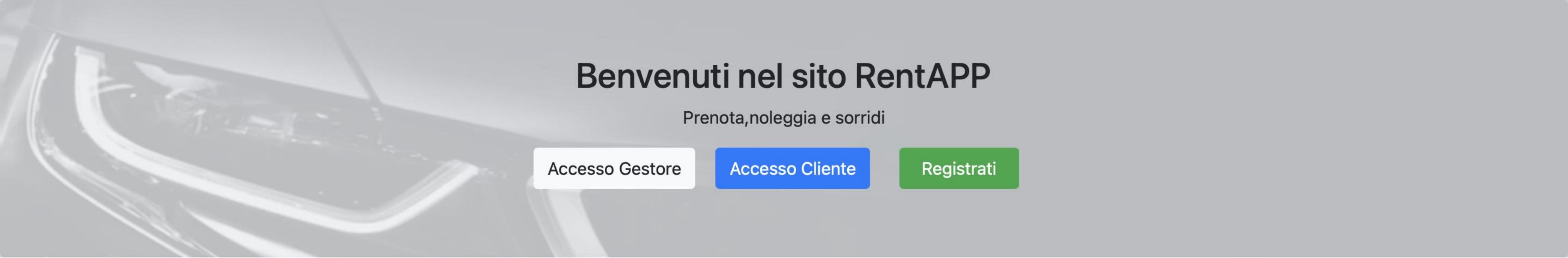
- ▶ L'utilizzo di docker compose consente di mantenere tutti i microservizi all'interno della stessa sottorete privata non accessibile esternamente.  
L'unico punto di accesso alla rete è il Server Tomcat esposto sulla porta 8443 la cui connessione è protetta da crittografia con HTTPS.
- ▶ Le connessioni interne alla sottorete saranno effettuate con protocollo HTTP rendendole computazionalmente meno onerose dei collegamenti con gli ambienti esterni.
- ▶ I metodi invocati dall'applicazione sul database prevengono l'SQL injection:
  - ▶ I metodi sono invocabili solo una volta che l'utente è autenticato.
  - ▶ L'utilizzo di Hibernate ha permesso la creazione dei metodi invocabili sul database tramite i CriteriaBuilder messi a disposizione da JPQL che effettua in automatico la sanificazione degli input.
  - ▶ L'utilizzo delle Stored Procedures per la creazione delle query.



# Rentapp Samples



## RentAPP



**Benvenuti nel sito RentAPP**

Prenota, noleggia e sorridi

[Accesso Gestore](#) [Accesso Cliente](#) [Registrati](#)



**La politica sul carburante migliore in Europa**

I nostri gestori adottano una politica sul carburante molto vantaggiosa per il cliente, che riceve le macchine con un pieno e può restituirla con almeno una tassa di livello sopra quello della riserva. Inoltre scopri il noleggio di veicoli elettrici.

Last updated 3 mins ago



**Viaggi per lavoro ?**

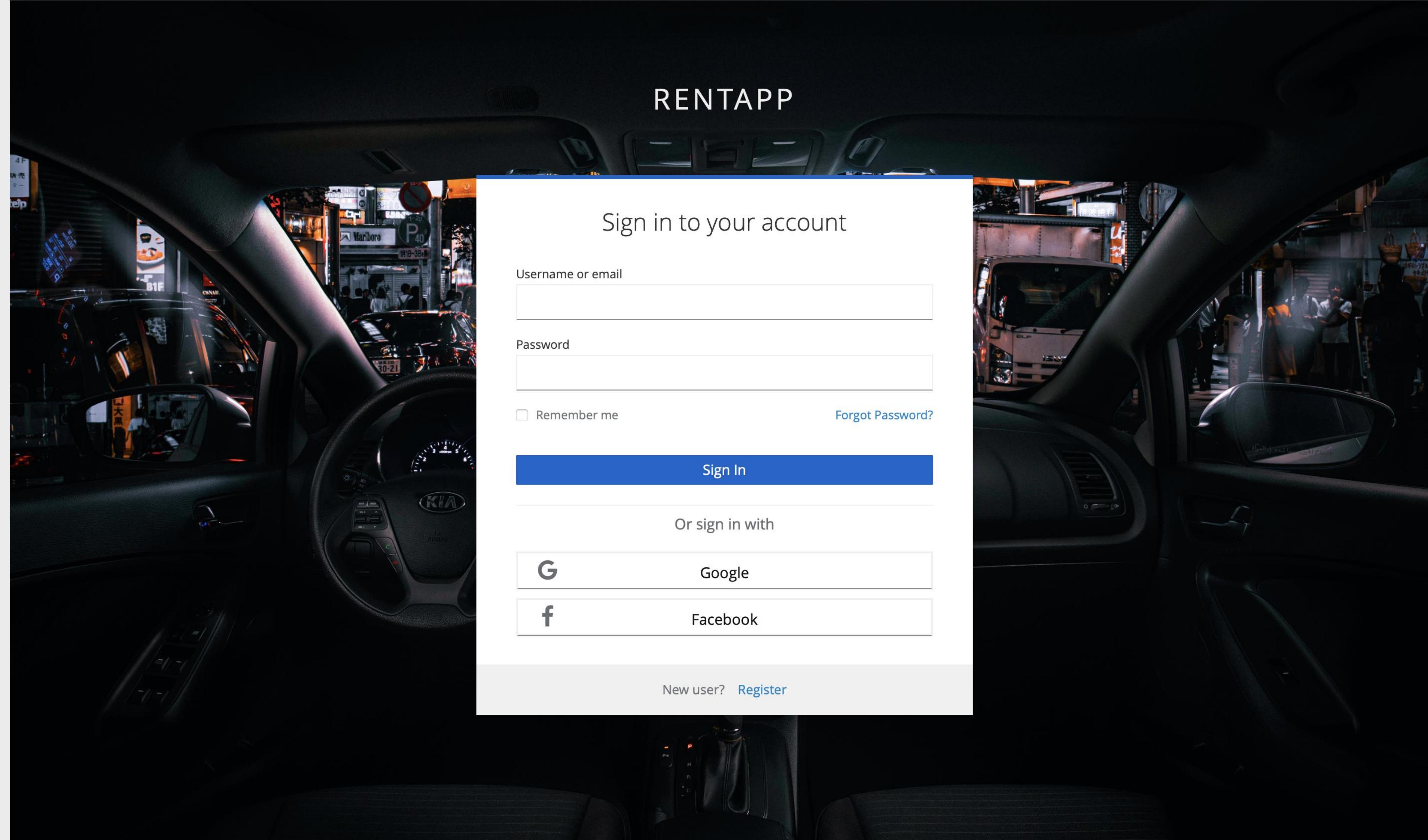
A breve saranno disponibili sconti e promozioni per chi effettua una prenotazione per necessità lavorative sia aziendali, sia di liberi professionisti

Last updated 3 mins ago





# Rentapp Samples





# Rentapp Samples

 RentAPP

Benvenuto Gestore :  
nello97

Questa è la tua dashboard, da qui potrai accedere alle svariate funzionalità che il sistema ti offre. Se hai già un parco auto puoi usufruire del servizio di inserimento veicolo per arricchirlo, altrimenti creane uno da zero



**Visualizza prenotazioni**  
Visualizza le prenotazioni attive e relative ai tuoi parchi auto.

[Visualizza Prenotazioni](#)



**Crea nuovo Parco Auto**  
Se recentemente hai aperto un tuo nuovo autonoleggio qui potrai virtualizzare la tua flotta auto.

[Crea Parco Auto](#)



**Aggiungi veicolo**  
Hai un nuovo veicolo che vuoi mettere a disposizione per il noleggio? Aggiungili tramite questa funzione a un parco auto già esistente.

[Inserisci veicolo](#)



# Rentapp Samples



## RentAPP



Risultati Visualizza Prenotazioni : 1 Prenotazioni

Pagine: 10 ▾

| <b>Id Prenotazione</b> | <b>Data Inizio</b> | <b>Data Fine</b> | <b>Utente</b> | <b>Parco Auto</b> | <b>Targa Veicolo</b> |
|------------------------|--------------------|------------------|---------------|-------------------|----------------------|
| 47                     | 01/01/2023         | 01/01/2024       | stefaramu     | NelloP            | AB123AB              |

[DashBoard](#)

© 2021 by aVerySadProject. [Termini & Condizioni](#) [Chi Siamo](#)



# Rentapp Samples



**RentAPP**

**CREA NUOVO PARCO AUTO**

Nome Parco Auto

Nome

Indirizzo

Indirizzo

Dislocazione

Dislocazione

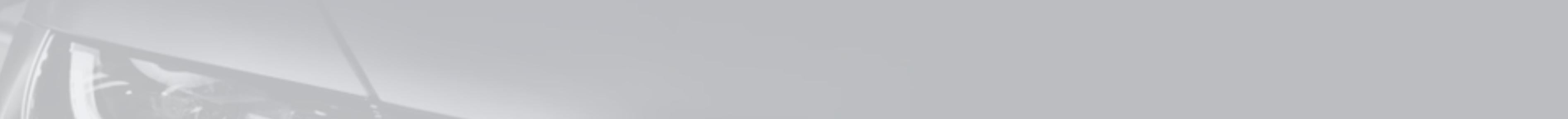
**Crea** **Dashboard**

© 2021 by aVerySadProject. [Termini & Condizioni](#) [Chi Siamo](#)



# Rentapp Samples

 RentAPP



**DATI VEICOLO**

|                           |                        |
|---------------------------|------------------------|
| Targa:                    | Modello:               |
| <input type="text"/>      | <input type="text"/>   |
| Marca:                    | Alimentazione:         |
| <input type="text"/>      | Benzina                |
| Segmento:                 |                        |
| <input type="text"/>      |                        |
| Tipos:                    |                        |
| <input type="text"/> tipo |                        |
| Cilindrata:               |                        |
| <input type="text"/> 0    |                        |
| Colore:                   | km:                    |
| <input type="text"/>      | <input type="text"/> 0 |
| prezzo:                   | Id ParcoAuto:          |
| <input type="text"/> 0.0  | NelloP                 |

[Aggiungi](#) [Dashboard](#)

© 2021 by aVerySadProject. [Termini & Condizioni](#) [Chi Siamo](#)



# Rentapp Samples

 RentAPP ≡

**Benvenuto Cliente :**  
nello97

Questa è la tua dashboard, da qui potrai accedere alle svariate funzionalità che il sistema ti offre. Effettua una prenotazione cercando un veicolo tra quelli disponibili in tutti i parchi auto o visualizza le prenotazioni effettuate



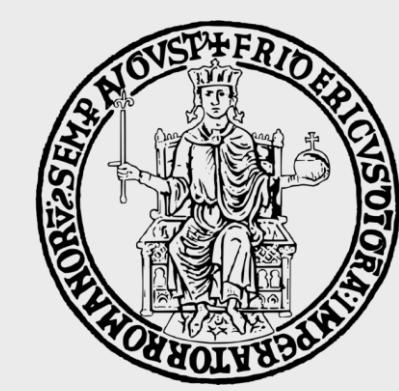
**Visualizza prenotazioni**  
Visualizza le prenotazioni da te effettuate e gestiscile tramite le funzionalità della nostra webapp.  
[Visualizza Prenotazioni](#)



**Effettua prenotazione**  
Effettua una prenotazione in base alle date in cui necessiti di un veicolo e al luogo di ritiro.  
[Prenota veicolo](#)



**Segnala guasti o incidenti**  
Invia la tua posizione specificando il motivo dell'impossibilità di locomozione del veicolo e ricevi la nostra assistenza gratuitamente  
[Effettua Segnalazione](#)



# Rentapp Samples



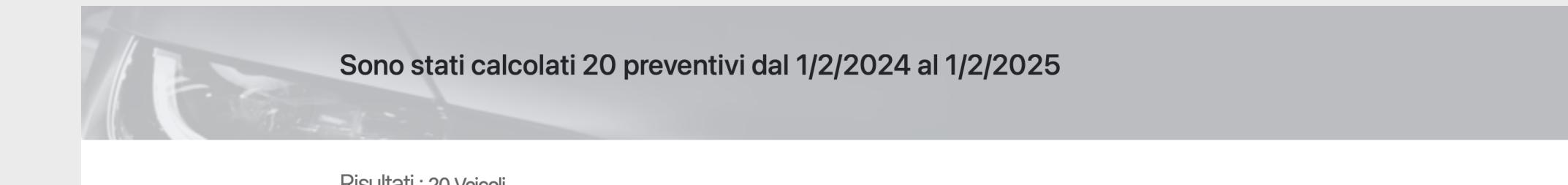
## EFFETTUA PRENOTAZIONE

Data Inizio Prenotazione      Data Fine Prenotazione      Dislocazione

|            |            |        |
|------------|------------|--------|
| 01/01/2000 | 01/01/2000 | Napoli |
|------------|------------|--------|

[Cerca](#) [Dashboard](#)

© 2021 by aVerySadProject. [Termini & Condizioni](#) [Chi Siamo](#)

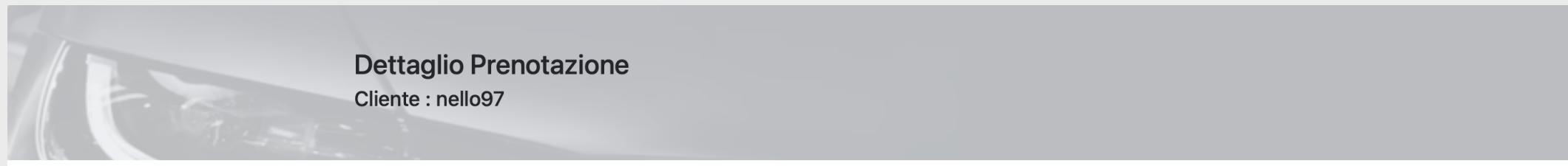


Sono stati calcolati 20 preventivi dal 1/2/2024 al 1/2/2025

Risultati : 20 Veicoli

Durata Periodo Selezionato : 366 Giorni

| Targa   | Modello  | Marca      | Alimentazione | Segmento         | Cilindrata | Colore | Km     | €      | Preventivo | Autonoleggio |                         |
|---------|----------|------------|---------------|------------------|------------|--------|--------|--------|------------|--------------|-------------------------|
| AP345ML | Classe E | Mercedes   | Hybrid        | Ammiraglia       | 3954       | rosso  | 123564 | 4290.0 | 1570140.0  | Neloparco    | <a href="#">Prenota</a> |
| BA234FD | Twingo   | Renault    | DHDI          | citycar          | 1210       | bianco | 300    | 57.0   | 20862.0    | Neloparco    | <a href="#">Prenota</a> |
| BA345NB | Es       | Lexus      | Hybrid        | Ammiraglia       | 2674       | Nero   | 12014  | 450.0  | 164700.0   | Neloparco    | <a href="#">Prenota</a> |
| BA934FD | up       | Volkswagen | GPL           | citycar          | 1160       | bianco | 20     | 51.0   | 18666.0    | Neloparco    | <a href="#">Prenota</a> |
| BC254TA | Ypsilon  | Lancia     | Benzina       | utilitaria       | 1510       | Nero   | 34000  | 97.0   | 35502.0    | Neloparco    | <a href="#">Prenota</a> |
| BN256TR | Fiesta   | Ford       | diesi         | utilitaria       | 1600       | rossa  | 180    | 129.0  | 47214.0    | Neloparco    | <a href="#">Prenota</a> |
| BR546WE | Clio     | Renault    | benzina       | utilitaria       | 1490       | verde  | 40     | 98.0   | 35868.0    | Neloparco    | <a href="#">Prenota</a> |
| BV556PO | corsa    | Opel       | elettrica     | utilitaria       | 1510       | Bianco | 14     | 119.0  | 43554.0    | Neloparco    | <a href="#">Prenota</a> |
| C256NB  | classe A | Mercedes   | Benzina       | compatta premium | 1980       | verde  | 170    | 240.0  | 87840.0    | Neloparco    | <a href="#">Prenota</a> |



## Dettaglio Prenotazione

Cliente : nello97

### Renault Twingo

Targa: BA234FD  
Modello: Automobile  
Alimentazione: DHDI  
Cilindrata: 1210  
Colore: bianco  
KM: 300  
Prezzo: 57.0  
Autonoleggio: Neloparco  
Indirizzo: Via Domenico Cimarosa 2  
Dislocazione: Napoli  
Data Inizio : 1/2/2024  
Data Fine : 1/2/2025

[Conferma](#) [Annulla](#)



## Dati Pagamento

Metodi di Pagamento accettati:



Titolare Carta:  
Mario Rossi

Numero carta:  
5246 1000 2000 3000

CVV:  Data di scadenza:

**Totale : 20862.0**

[Conferma](#) [Annulla](#)

© 2021 by aVerySadProject. [Termini & Condizioni](#) [Chi Siamo](#)



# Rentapp Samples

The screenshot shows a mobile application interface for 'RentAPP'. At the top left is a logo consisting of a car icon and the text 'RentAPP'. The main content area displays a large, semi-transparent gray box containing the text 'Pagamento effettuato con successo' (Payment successful). Below this box is a green button labeled 'Dashboard'. At the bottom of the screen, there is a footer bar with the text '© 2021 by aVerySadProject. Termini & Condizioni Chi Siamo'.

RentAPP

Pagamento effettuato con successo

Dashboard

© 2021 by aVerySadProject. Termini & Condizioni Chi Siamo



# Rentapp Samples



RentAPP



Risultati Visualizza Prenotazioni : 4 Prenotazioni

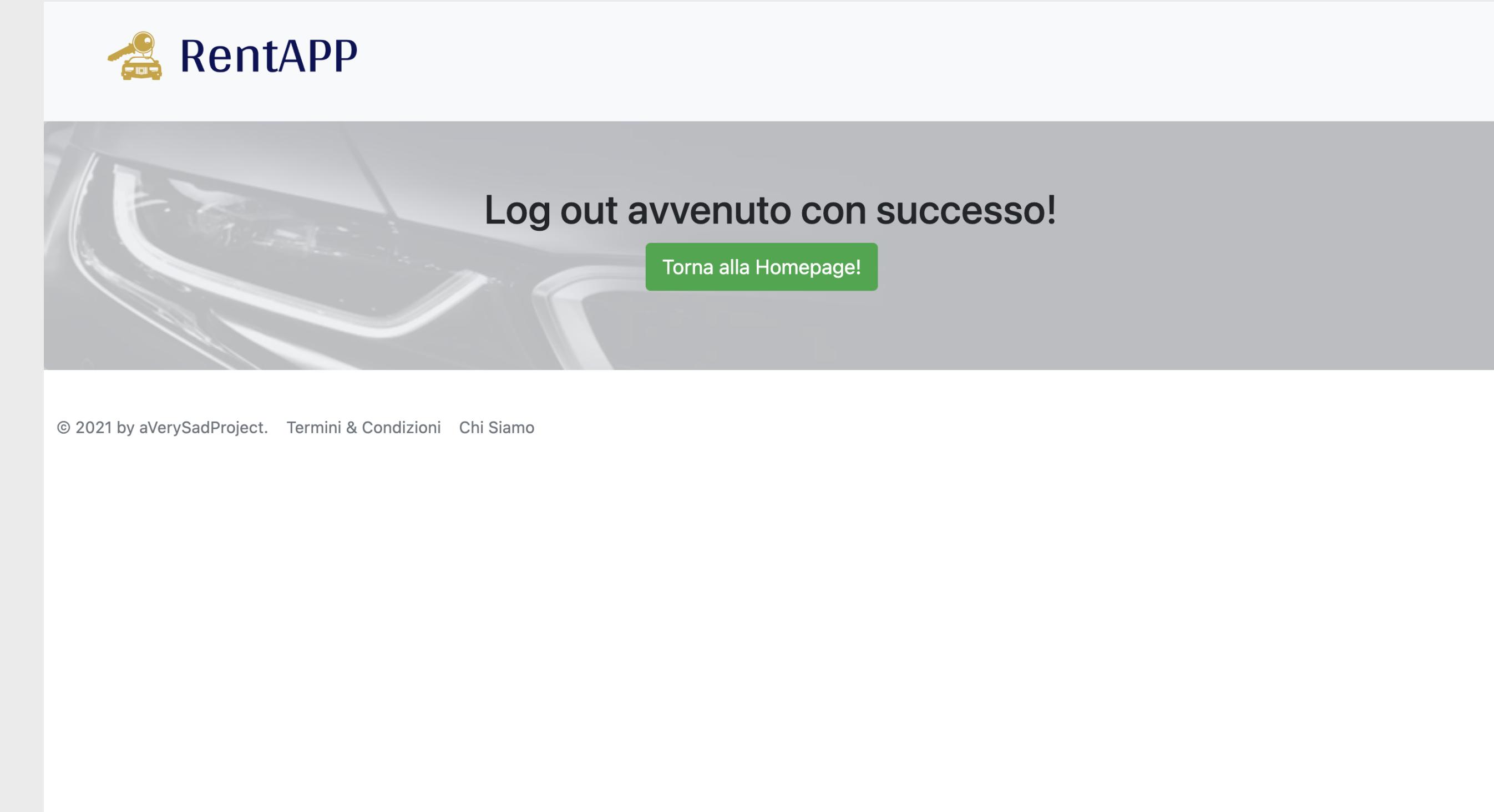
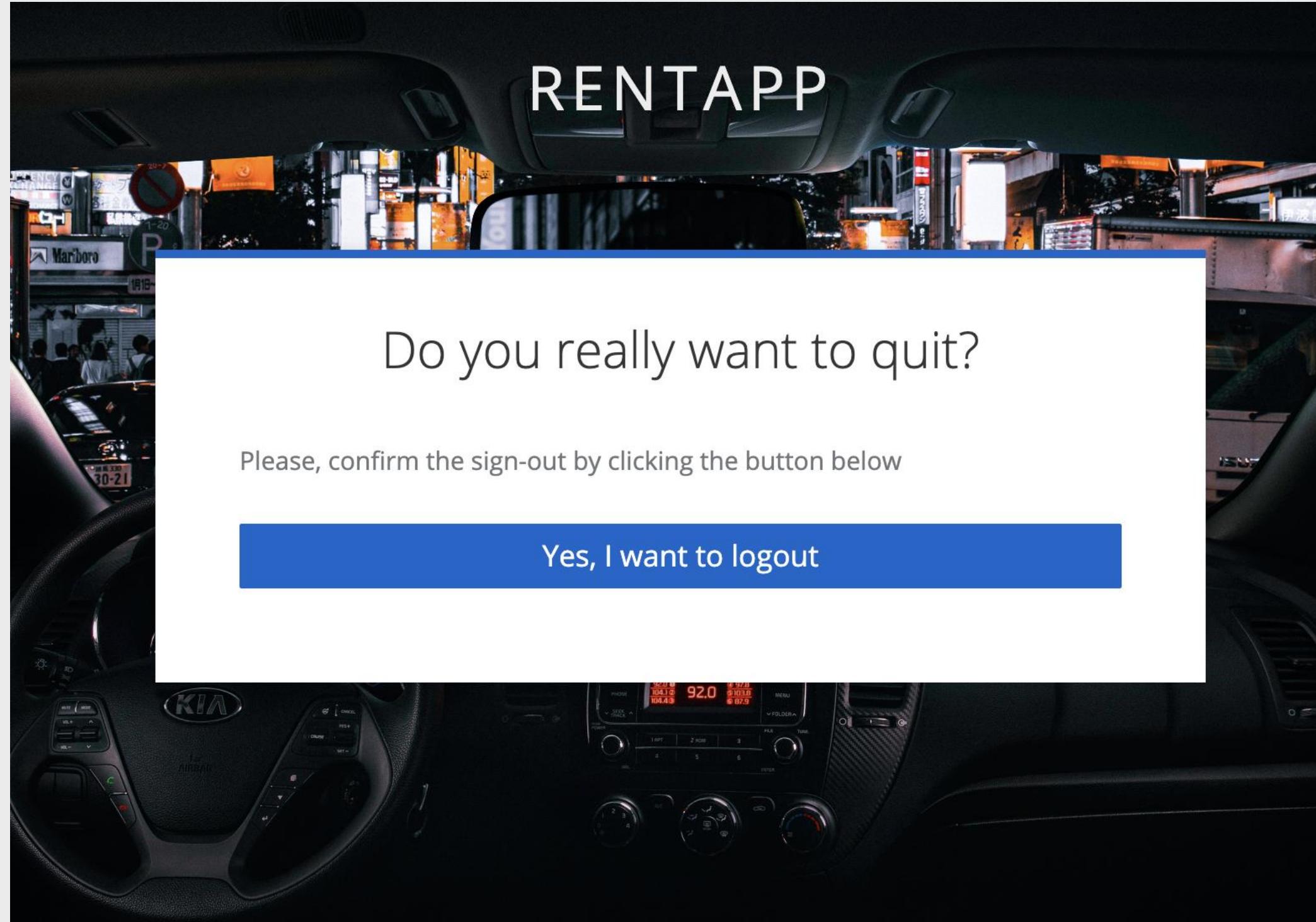
Pagine: 10

| Id Prenotazione | Data Inizio | Data Fine  | Utente  | Parco Auto | Targa Veicolo |
|-----------------|-------------|------------|---------|------------|---------------|
| 37              | 01-08-2021  | 10-08-2021 | Nello97 | Nelloparco | AP345ML       |
| 43              | 01-08-2021  | 08-08-2021 | Nello97 | Nelloparco | BA234FD       |
| 48              | 01-02-2023  | 01-03-2023 | nello97 | Nelloparco | BV556PO       |
| 1048            | 01-02-2024  | 01-02-2025 | nello97 | Nelloparco | BA234FD       |

[DashBoard](#)



# Rentapp Samples





# Rentapp Samples

## Register

First name  
Stefano

Last name  
Aramu

Email  
blackaramudev@gmail.com

Username  
aramdj

Password  
\*\*\*\*\*

Confirm password  
\*\*\*\*\*

I'm not a robot

reCAPTCHA

[Privacy - Terms](#)

[« Back to Login](#)

**Register**

## RentAPP

### Benvenuto Cliente :

Prima di cominciare abbiamo bisogno di alcune informazioni

**DATI UTENTE**

Username:  
aramdj

Nome: Stefano Cognome: Aramu

Indirizzo:  
Indirizzo

Patente:  
Numero Patente

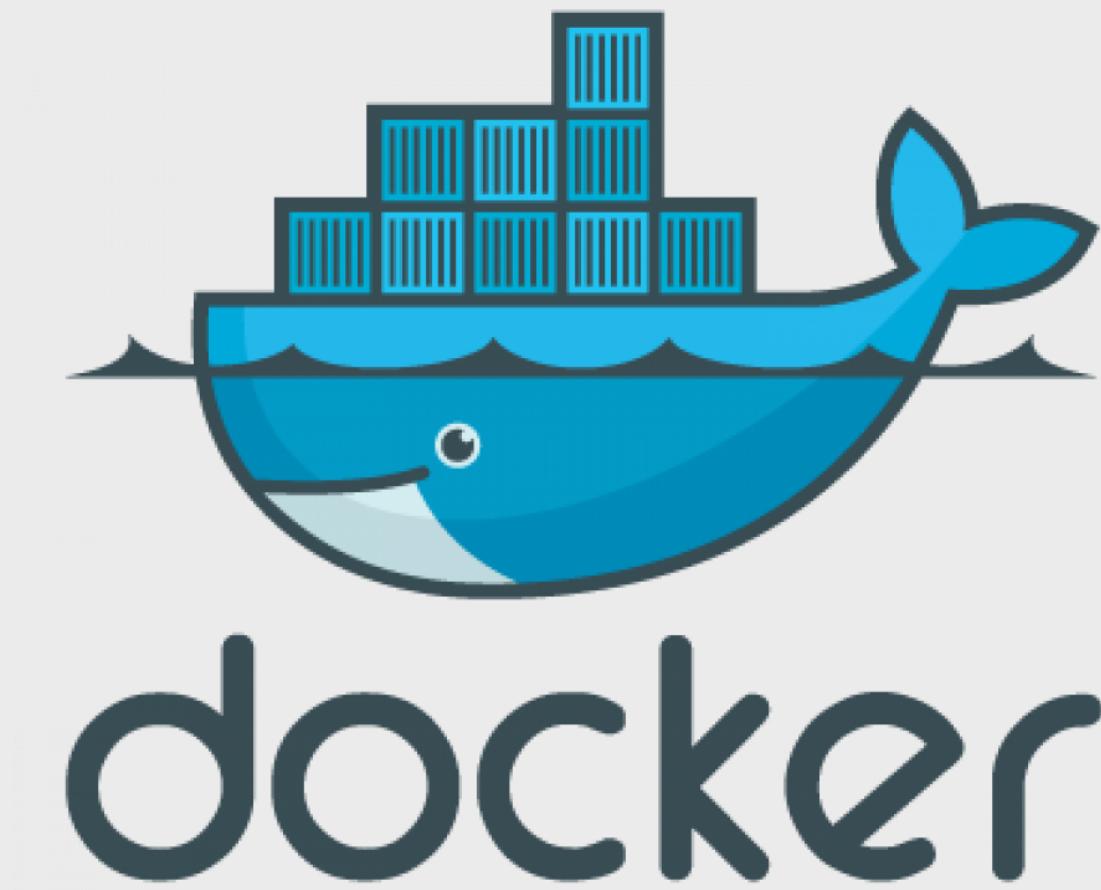
Partita IVA: Codice Fiscale:

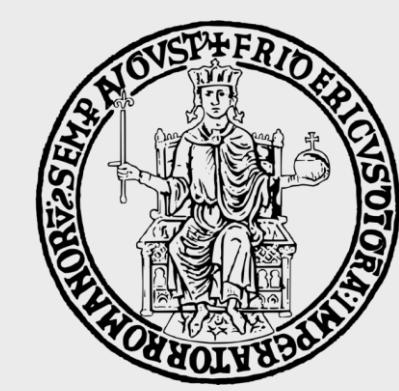
Luogo di nascita: Data di nascita:  
01/01/2000

**Conferma** **Annulla**



# Tecnologie Utilizzate



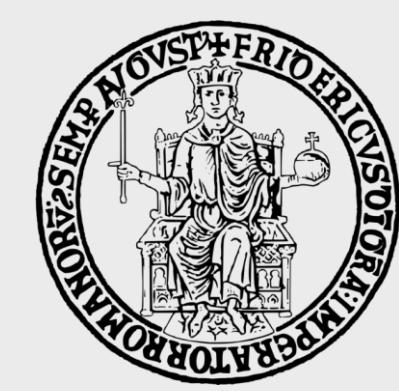


# Tecnologie Utilizzate - Keycloak

**Keycloak** è un software di tipo Identity and Access Management (IAM) distribuito con licenza open-source.

Lanciando una distribuzione del server di keycloak è possibile realizzare un meccanismo di autenticazione di Single Sign-On (SSO) con Identity Provider.

Sfruttando i protocolli OpenID Connect, OAuth o SAML 2.0 keycloak consente l'autenticazione di utenti per l'accesso a risorse protette.



# Tecnologie Utilizzate - Keycloak

L'immagine ufficiale di Keycloak è stata scaricata da docker hub (v. 20.0.1).

Tale immagine lanciata in un container è stata opportunamente modificata e adattata al contesto dell'applicazione sia tramite la User Interface messa a disposizione dall'applicazione che tramite l'opportuna alterazione dei file di estensione .ftl che permettono di modificare la struttura del CSS e HTML delle varie interfacce fornite dal IAM.

L'immagine modificata è stata successivamente clonata e resa disponibile per l'utilizzo.



# Tecnologie Utilizzate - Keycloak

La creazione del docker avviene tramite l'esecuzione di un file .yaml che provvede all'inserimento di quest'ultimo in un docker

|   | NAME ↓         | IMAGE                                  | STATUS        | PORT(S)                | STARTED        | ACTIONS |
|---|----------------|--|---------------|------------------------|----------------|---------|
| □ | composedsystem | -                                      | Running (4/4) |                        |                |         |
| □ | vault          | vaultfinal:latest<br>7fb174a6ff22      | Running       | 8200:8200              | 47 minutes ago |         |
| □ | rentapp        | rentapp.war:latest<br>f6b51cff4903     | Running       | 9001:8080<br>8443:8443 | 47 minutes ago |         |
| □ | keycloak       | keycloakfinalv3:latest<br>d1717dc2b81e | Running       | 8080:8080              | 47 minutes ago |         |
| □ | db             | sqlimage:latest<br>2e6ed9a46e00        | Running       | 1433:1433              | 47 minutes ago |         |

```
47 keycloakcp:  
48   container_name: keycloak  
49   image: keycloakfinalv3  
50   ports:  
51     - 8080:8080  
52   environment:  
53     -KEYCLOAK_ADMIN: admin  
54     -KEYCLOAK_ADMIN_PASSWORD: admin  
55     -PROXY_ADDRESS_FORWARDING: true  
56   networks:  
57     rentweb:  
58       ipv4_address: 172.21.0.3  
59   volumes:  
60     - ./realm.json:/tmp/realm.json  
61   restart: unless-stopped  
62
```

La variabile di ambiente PROXY\_ADDRESS\_FORWARDING è stata settata con valore true per permettere l'interazione con Tomcat.

Il valore del campo 'restart' è stato dettato a 'unless-stopped' in modo tale da riavviare il docker ogni qualvolta possa verificarsi un errore.

Inoltre, così come per gli altri docker, gli è stato aggiunto un



# Tecnologie Utilizzate - Keycloak

## Realms e Client

Una volta messo su il server di keycloak è possibile accedere all'admin console.

Un **realm** corrisponde al contesto dell'applicazione nel quale i diversi ruoli, utenti e client coesistono.

Il passo successivo quindi è stato quello di creare un realm dedicato all'app, abbiamo scelto come nome RentApp.

Successivamente è stato creato il client "rentapp\_client" con la funzionalità di fare richieste a keycloak per autenticare gli utenti.

Ad ogni client viene associata un applicazione che richiede a keycloak di utilizzare la funzione di Single Sign-On

| Clients list                           |                | Initial access token   |
|--|----------------|------------------------|
| <input type="text"/> Search for client |                | <input type="button"/> |
| Client ID                              | Type           |                        |
| account                                | OpenID Connect |                        |
| account-console                        | OpenID Connect |                        |
| admin-cli                              | OpenID Connect |                        |
| broker                                 | OpenID Connect |                        |
| realm-management                       | OpenID Connect |                        |
| rentapp_client                         | OpenID Connect |                        |
| security-admin-console                 | OpenID Connect |                        |



# Tecnologie Utilizzate - Keycloak

## Ruoli e Utenti

Il tipo di controllo degli accessi implementato è di tipo Role-based, per cui sono stati definiti i ruoli **cliente** e **gestore**. All'atto della registrazione al nuovo utente viene assegnato un ruolo di default corrispondente a quello di cliente. Per diventare gestore sarà necessario fare un'opportuna richiesta tramite email all'admin del sito "rentappssd@gmail.com".

| User list                                       | Permissions             |
|---|-------------------------|
| <input type="text"/> Search user                | →                       |
| <input type="button"/> Add user                 | ⋮                       |
| <input type="checkbox"/> Username               | Email                   |
| <input type="checkbox"/> accounts manager       | —                       |
| <input type="checkbox"/> admin                  | —                       |
| <input type="checkbox"/> aramdj                 | blackaramudev@gmail.com |
| <input type="checkbox"/> cliente                | —                       |
| <input type="checkbox"/> gestore                | —                       |
| <input type="checkbox"/> ne_ne.12.06@hotmail.it | ne_ne.12.06@hotmail.it  |
| <input type="checkbox"/> nello97                | ne.ambrosio.6@gmail.com |

| Realm roles  |           |
|--|-----------|
| Realm roles are the roles that you define for use in the current realm. <a href="#">Learn more</a> |           |
| <input type="text"/> Search role by name   | →         |
| <input type="button"/> Create role   |           |
| Role name  | Composite |
| CLIENTE  | False     |
| GESTORE  | False     |
| default-roles-rentapp  | True      |
| offline_access   | False     |
| uma_authorization  | False     |



# Tecnologie Utilizzate - Keycloak

## Ruoli e Utenti

Tramite la User Interface di Keycloak è possibile tenere traccia degli eventi sia degli utenti che dell'admin di sistema e delle sessioni attive di tutti gli utenti.

**Sessions**

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)

Search session → 1 - 3

|             |                        |   |
|-------------|------------------------|---|
| User        | nello97                | ⋮ |
| Started     | 12/29/2022, 6:33:50 PM |   |
| Last access | 12/29/2022, 6:33:50 PM |   |
| IP address  | 172.21.0.1             |   |
| Clients     | rentapp_client         |   |

|             |                        |   |
|-------------|------------------------|---|
| User        | aramdj                 | ⋮ |
| Started     | 12/29/2022, 6:34:09 PM |   |
| Last access | 12/29/2022, 6:34:09 PM |   |
| IP address  | 172.21.0.1             |   |
| Clients     | rentapp_client         |   |

|             |                        |   |
|-------------|------------------------|---|
| User        | rentapp                | ⋮ |
| Started     | 12/29/2022, 6:34:40 PM |   |
| Last access | 12/29/2022, 6:34:40 PM |   |

**Events**

Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events Admin events

Search user event Refresh 1 - 10

|            |                                     |
|------------|-------------------------------------|
| Time       | December 29, 2022 at 6:34 PM        |
| User       | 4fb633c-9456-4977-8794-d2bd8bea4e0e |
| Event type | CODE_TO_TOKEN                       |
| IP address | 172.21.0.2                          |
| Client     | rentapp_client                      |

|            |                                     |
|------------|-------------------------------------|
| Time       | December 29, 2022 at 6:34 PM        |
| User       | 4fb633c-9456-4977-8794-d2bd8bea4e0e |
| Event type | LOGIN                               |
| IP address | 172.21.0.1                          |
| Client     | rentapp_client                      |

|      |                              |
|------|------------------------------|
| Time | December 29, 2022 at 6:34 PM |
|------|------------------------------|



# Tecnologie Utilizzate - Keycloak

## Integrazione con Tomcat

Per l'integrazione con Tomcat è stato definito un file web.xml che può essere considerato come una sorta di indice.

Il **module-name** corrisponde al nome del realm.

Successivamente tramite il tag **“security-constraint”** vengono definiti i path da proteggere.

Il tag **web-resource-name** corrisponde alla risorsa protetta definita tramite interfaccia utente di keycloak, il tag **url-pattern** a quello del percorso relativo della risorsa e il **“role-name”** al ruolo necessario per accedere alla risorsa.

```
7   <module-name>RentApp</module-name>
8   <welcome-file-list>
9     <welcome-file>index.jsp</welcome-file>
10  </welcome-file-list>
11
```

```
25  <!-- Cliente -->
26  <security-constraint>
27    <web-resource-collection>
28      <web-resource-name>cliente</web-resource-name>
29      <url-pattern>/dashcliente/*</url-pattern>
30      <http-method>GET</http-method>
31      <http-method>POST</http-method>
32    </web-resource-collection>
33    <auth-constraint>
34      <role-name>CLIENTE</role-name>
35    </auth-constraint>
36  </security-constraint>
37
```



# Tecnologie Utilizzate - Keycloak

## Integrazione con Tomcat

Nel caso di Rentapp sono stati creati due security-constraints:

- ▶ Il primo serve a proteggere la risorsa denominata gestore, giacente nel path /dashgestore/\* e accessibile solo dagli utenti con ruolo GESTORE
- ▶ Il secondo serve a proteggere la risorsa denominata cliente, giacente nel path /dashcliente/\* e accessibile solo dagli utenti con ruolo CLIENTE.

Infine con “**error-page**” viene specificato l’indirizzo della pagina d’errore 403 da restituire all’utente che prova ad accedere ad una risorsa protetta senza il

```
12      <!-- Gestore -->
13  <security-constraint>
14    <web-resource-collection>
15      <web-resource-name>gestore</web-resource-name>
16      <url-pattern>/dashgestore/*</url-pattern>
17      <http-method>GET</http-method>
18      <http-method>POST</http-method>
19    </web-resource-collection>
20  <auth-constraint>
21    <role-name>GESTORE</role-name>
22  </auth-constraint>
23 </security-constraint>
24
25      <!-- Cliente -->
26  <security-constraint>
27    <web-resource-collection>
28      <web-resource-name>cliente</web-resource-name>
29      <url-pattern>/dashcliente/*</url-pattern>
30      <http-method>GET</http-method>
31      <http-method>POST</http-method>
32    </web-resource-collection>
33  <auth-constraint>
34    <role-name>CLIENTE</role-name>
35  </auth-constraint>
36 </security-constraint>
37
```

```
48
49  <error-page>
50    <error-code>403</error-code>
51    <location>/errore</location>
52  </error-page>
53 </web-app>
```



# Tecnologie Utilizzate - Keycloak

## Integrazione con Tomcat

Successivamente è necessario scaricare gli adapter di keycloak corrispondenti all'apposita versione di tomcat. Questi ultimi devono essere copiati e incollati nella directory **/lib** del server.

Infine è necessario creare un ulteriore file **context.xml** dove viene specificato il percorso del server a partire da cui Keycloak deve essere invocato.

```
1 <Context path="/rentapp">
2   <Valve className="org.keycloak.adapters.tomcat.KeycloakAuthenticatorValve"/>
3 </Context>
```

```
/usr/local/tomcat/lib # ls
annotations-api.jar
bcpkix-jdk15on-1.68.jar
bcpkix-jdk15on-1.70.jar
bcprov-jdk15on-1.68.jar
bcprov-jdk15on-1.70.jar
bcutil-jdk15on-1.70.jar
catalina-ant.jar
catalina-ha.jar
catalina-storeconfig.jar
catalina-tribes.jar
catalina.jar
commons-codec-1.11.jar
commons-collections4-4.1.jar
commons-logging-1.2.jar
ecj-4.6.3.jar
ecj-4.7.3a.jar
el-api.jar
httpclient-4.5.13.jar
httpcore-4.4.14.jar
jackson-annotations-2.12.1.jar
jackson-annotations-2.13.4.jar
jackson-core-2.12.1.jar
jackson-core-2.13.4.jar
jackson-databind-2.12.1.jar
jackson-databind-2.13.4.2.jar
jakarta.activation-1.2.2.jar
jasper-el.jar
jasper.jar
jaspic-api.jar
jboss-logging-3.4.1.Final.jar
jsp-api.jar
keycloak-adapter-core-15.0.2.jar
keycloak-adapter-core-20.0.1.jar
keycloak-adapter-spi-15.0.2.jar
keycloak-adapter-spi-20.0.1.jar
keycloak-authz-client-15.0.2.jar
keycloak-authz-client-20.0.1.jar
keycloak-common-15.0.2.jar
keycloak-common-20.0.1.jar
keycloak-core-15.0.2.jar
keycloak-core-20.0.1.jar
keycloak-crypto-default-20.0.1.jar
keycloak-server-spi-20.0.1.jar
keycloak-server-spi-private-20.0.1.jar
keycloak-tomcat-adapter-15.0.2.jar
keycloak-tomcat-adapter-20.0.1.jar
keycloak-tomcat-adapter-spi-15.0.2.jar
keycloak-tomcat-adapter-spi-20.0.1.jar
keycloak-tomcat-core-adapter-15.0.2.jar
keycloak-tomcat-core-adapter-20.0.1.jar
servlet-api.jar
snakeyaml-1.26.jar
tomcat-api.jar
tomcat-coyote.jar
tomcat-dbcp.jar
tomcat-i18n-es.jar
tomcat-i18n-fr.jar
tomcat-i18n-ja.jar
tomcat-i18n-ru.jar
tomcat-jdbc.jar
tomcat-jni.jar
tomcat-util-scan.jar
tomcat-util.jar
tomcat-websocket.jar
uap-java-1.5.2.jar
websocket-api.jar
```



# Tecnologie Utilizzate - Keycloak

## Integrazione con Tomcat

L'ultimo file necessario per la configurazione è **keycloak.json**. Questo è importabile da keycloak dopo aver configurato il client.

All'interno vengono mappati rispettivamente il **nome del realm**, **l'indirizzo del server keycloak**, in che caso keycloak deve provvedere a stabilire connessioni SSL, il client e il segreto necessario per l'autenticazione dell'app al server.

Come specificato nel file, il campo **ssl-required** è impostato su **external**, per cui Keycloak richiederà una connessione SSL a chiunque cercherà di connettersi al di fuori della rete su cui è ospitato il server e quindi la rete creata con docker compose

```
{
  "realm": "RentApp",
  "auth-server-url": "http://keycloak:8080/",
  "ssl-required": "external",
  "resource": "rentapp_client",
  "verify-token-audience": true,
  "credentials": {
    "secret": "x700st2fvFeECegzHhLxHe7Nqm30asl7"
  },
  "confidential-port": 0
}
```



# Tecnologie Utilizzate - Keycloak

## Integrazione con SpringMVC

Per utilizzare le librerie di keycloak all'interno dell'ambiente Spring è stato necessario importare le dipendenze corrispondenti alla versione 20.0.1 dell' IAM.

A tal fine all'interno del file pom.xml del progetto maven, si è importata la seguente dipendenza.

In tal modo verranno scaricate nel progetto tutte le librerie java che ci permetteranno di interagire in backend con Keycloak.

```
145<dependency>
146    <groupId>org.keycloak</groupId>
147    <artifactId>keycloak-installed-adapter</artifactId>
148    <version>20.0.1</version>
149</dependency>
150
```



# Tecnologie Utilizzate - Keycloak

## Integrazione con SpringMVC

Dopo aver importato le dipendenze di potrà procedere all'utilizzo delle librerie.

```
54  
55 import org.keycloak.AuthorizationContext;  
56 import org.keycloak.KeycloakPrincipal;  
57 import org.keycloak.KeycloakSecurityContext;  
58 import org.keycloak.authorization.client.util.Http;  
59 import org.keycloak.representations.AccessToken;  
60 import org.keycloak.representations.IDToken;  
61 import org.keycloak.representations.idm.authorization.Permission;  
62
```

Nell'applicazione tale utilizzo è stato effettuato principalmente al fine di :

- ▶ Effettuare il **Log-Out**
- ▶ Otttenere alcune **informazioni** sulla sessione e sull'utente che



# Tecnologie Utilizzate - Keycloak

## Integrazione con SpringMVC

Il recupero delle informazioni relative all'utente è stato effettuato sfruttando l'Auth Token fornito da Keycloak.

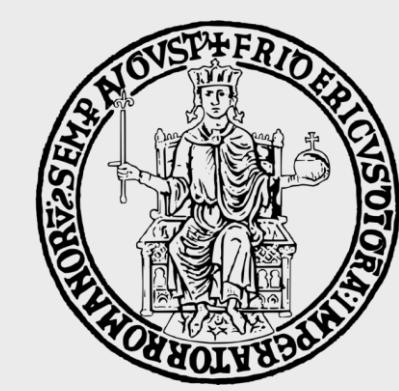
```
112  
113 KeycloakSecurityContext keycloakSecurityContext = (KeycloakSecurityContext) request.getAttribute(KeycloakSecurityContext.class.getName());  
114     AuthorizationContext authzContext = keycloakSecurityContext.getAuthorizationContext();  
115     userdetails.setUsername(keycloakSecurityContext.getToken().getPreferredUsername());  
116
```

In particolare, viene estratto dalla `request` http l'attributo rappresentante il `KeycloakSecurityContext`.

In seguito dal `KeycloakSecurityContext` viene estratto l'`AuthorizationContext`.

L'`AuthorizationContext` conterrà informazione riguardanti i permessi posseduti dall'utente e può essere utile in caso di condivisione di funzioni tra utenti con ruoli differenti.

In fine dal `KeycloakSecurityContext` viene estratto l'`AuthToken` da cui si estrarranno le informazioni relative all'utente come



# Tecnologie Utilizzate - Keycloak

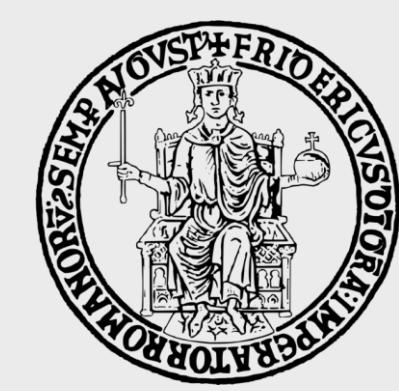
## Integrazione con SpringMVC

Dall'AuthToken estratto dal KeycloakSecurityContext è possibile ottenere anche altri attributi che l'utente fornisce a keycloak.

```
128     Map<String, Object> customClaims=keycloakSecurityContext.getToken().getOtherClaims();
129     String[] splits = keycloakSecurityContext.getToken().getName().split(" ");
130     userdetails.setNome(splits[0]);
131     userdetails.setCognome(splits[1]);
```

Tramite la funzione 'getOtherClaims()' è possibile estrarre, utilizzando l'AuthToken, tutti gli attributi di un utente per il quale all'interno del client è definito un Mappers come ad esempio il genere, l'indirizzo email o qualsiasi attributo custom chiesto durante la registrazione. È possibile definire questi attributi nel Mapper.

| Name        | Category     | Type           | Priority |   |
|-------------|--------------|----------------|----------|---|
| gender      | Token mapper | User Attribute | 0        | ⋮ |
| middle name | Token mapper | User Attribute | 0        | ⋮ |
| locale      | Token mapper | User Attribute | 0        | ⋮ |
| username    | Token mapper | User Property  | 0        | ⋮ |
| profile     | Token mapper | User Attribute | 0        | ⋮ |
| nickname    | Token mapper | User Attribute | 0        | ⋮ |



# Tecnologie Utilizzate - Keycloak

## Integrazione con SpringMVC

Per quanto riguarda l'operazione di logout è stato utilizzata una Servlet Request messa a disposizione da Keycloak e opportunamente modificata indicando il client id di keycloak e il post redirect logout, quest'ultimo poi deve essere specificato nella console di amministrazione del client sfruttato dall'applicazione. Inoltre si è proceduto anche ad invalidare la sessione per eliminare da quest'ultima i dati relativi all'utente.

```
@RequestMapping(value="logout",method=RequestMethod.POST)
public String logout(HttpServletRequest request) throws ServletException
{
    request.logout();
    return "redirect:" + "http://localhost:8080/realm/RentApp/"
        + "protocol/openid-connect/logout"
        + "?client_id=rentapp_client"
        + "&post_logout_redirect_uri=http%3A%2F%2Flocalhost%3A9001%2Frentapp%2Fpostlogout";

}
@RequestMapping(value="postlogout",method=RequestMethod.GET)
public String postlogout(HttpServletRequest request) throws ServletException
{
    request.logout();
    return "logout";
}
```



# Tecnologie Utilizzate - Keycloak

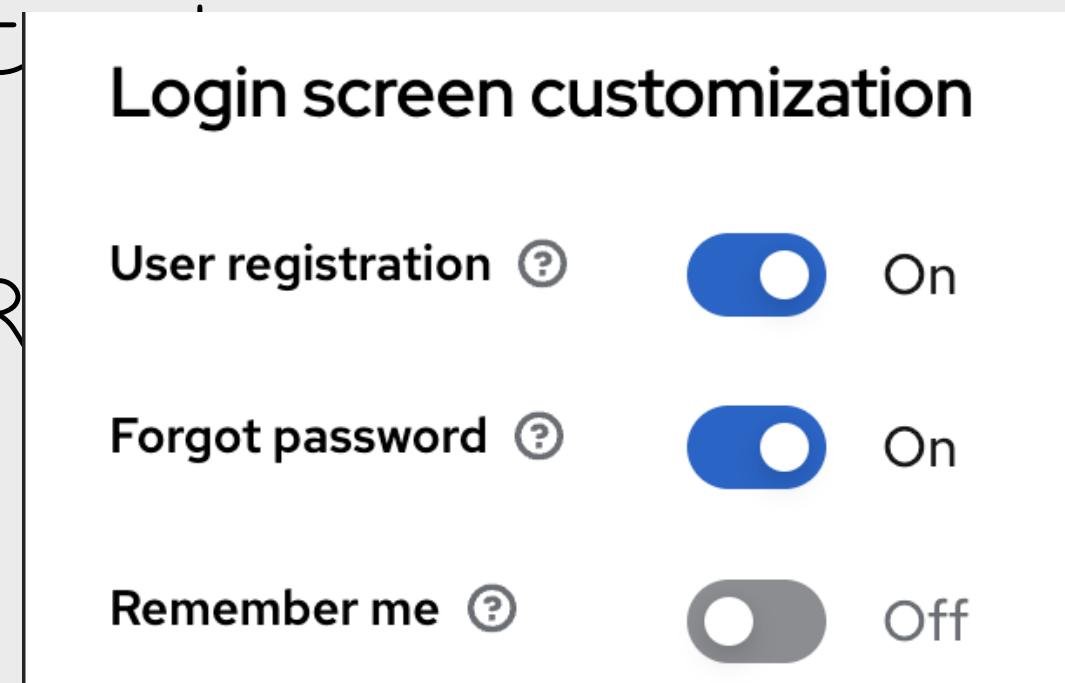
## Registrazione

Per accedere al servizio l'utente dovrà essere registrato sull'IAM.

A tale scopo è stata abilitata la registrazione nei Relying Party Settings.

Si è optato poi per suddividere la registrazione in due fasi:

- ▶ Registrazione su Keycloak
- ▶ Inserimento delle informazioni necessarie al funzionamento della WebApp





# Tecnologie Utilizzate - Keycloak

## Registrazione Keycloak Side

Su Keycloak si è scelto di mantenere solo le informazioni sensibili dell'utente come Username e Password, email, Nome e Cognome.

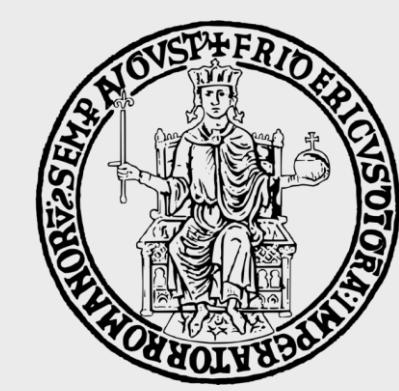
È stato inserito anche il servizio di reCaptcha offerto da Google al fine di evitare la registrazione al servizio da parte di tool automatizzati.

I dati collezionati da Keycloak verranno conservati dall' IAM stesso in un proprio

The central image shows a registration form titled "Register". The form fields are as follows:

- First name: Stefano
- Last name: Aramu
- Email: blackaramudev@gmail.com
- Username: aramdj
- Password: (redacted)
- Confirm password: (redacted)
- reCAPTCHA: A checkbox labeled "I'm not a robot" with a green checkmark, followed by the reCAPTCHA logo and links to "Privacy - Terms".

At the bottom of the form are two buttons: "« Back to Login" and a large blue "Register" button.



# Tecnologie Utilizzate - Keycloak

## Registrazione RentApp Side

Su RentApp invece è stato scelto di mantenere solo le informazioni dell'utente utili al funzionamento dell'applicazione.

L'applicazione non chiederà mai l'inserimento di informazioni sensibili come la Password al fine di salvarle nel proprio database.

Tale pagina verrà mostrata all'utente dopo la registrazione su keycloak e le funzionalità fornite dalla WebApp non saranno disponibili finché non

**DATI UTENTE**

|                   |                                |          |       |
|-------------------|--------------------------------|----------|-------|
| Username:         | aramdj                         |          |       |
| Nome:             | Stefano                        | Cognome: | Aramu |
| Indirizzo:        | Indirizzo                      |          |       |
| Patente:          | Numero Patente                 |          |       |
| Partita IVA:      | Codice Fiscale:                |          |       |
| Luogo di nascita: | Data di nascita:<br>01/01/2000 |          |       |

**Conferma** **Annulla**



# Tecnologie Utilizzate - Keycloak

## Registrazione

Abbiamo deciso di effettuare questa separazione per tre principali motivi:

- ▶ Separare i dati di accesso dal resto dei dati al fine di separare il contesto di accesso all'applicazione dal contesto di funzionamento dell'applicazione stessa.
- ▶ Conservare i dati necessari al funzionamento nel database dell'applicazione garantisce comunque un discreto livello di sicurezza grazie all'utilizzo delle Stored Procedures e di Hibernate.
- ▶ L'applicazione funziona utilizzando una parte di dati 'non sensibili' condivisi fra gli utenti. Keycloak non permette di accedere ad attributi personali di altri utenti che usufruiscono



# Tecnologie Utilizzate - Keycloak

## Registrazione

La registrazione per essere effettiva deve essere confermata accedendo al link inviato tramite mail dal server SMTP all'indirizzo fornito dall'utente.

Inoltre c'è bisogno di confermare i termini e condizioni d'uso e configurare un OTP per la sicurezza.

The screenshot illustrates the multi-step registration process:

- OTP Check:** A step where users are prompted to set up a mobile authenticator. It lists several apps: Google Authenticator, One Login Protect, FreeOTP(Only Android System), and 2FA Authenticator (2FAS). A QR code is provided for scanning.
- Email Verification:** An email from "Rentapp" is shown in the inbox, containing a link for email address verification. The message body states: "Someone has created an account with this email address. If this was you, click the link below to verify your email address". Below the message is a link: "Link to e-mail address verification".
- Terms and Conditions:** A separate page titled "Terms and Conditions" is displayed. It welcomes users to Rentapp and outlines the rules and regulations for the website. It includes a detailed legal notice and a statement: "By accessing this website we assume you accept these terms and conditions. Do not continue to use Rentapp if you do not agree to take all of the terms and conditions stated on this page."



# Tecnologie Utilizzate - Keycloak

## Login

Al fine di effettuare il login si può procedere seguendo due alternative:

- ▶ Inserimento di username e password
- ▶ Se si effettua l'accesso mediante Facebook o Google ci si può trovare in due scenari differenti:

- ▶ L'email è già associata ad un account. In questo caso verrà chiesto all'utente di associare il metodo di autenticazione federata all'account trovato tramite l'inserimento della password.
- ▶ L'email non è associata ad un account. In questo caso si procederà con la registrazione del nuovo utente.

Sign in to your account

Username or email

Password

Remember me [Forgot Password?](#)

[Sign In](#)

Or sign in with

 [Google](#)

 [Facebook](#)

New user? [Register](#)



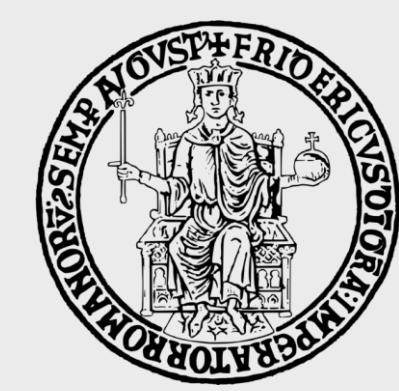
# Tecnologie Utilizzate - Vault

Hashicorp **Vault** è un software di **“Identity-based secret and encryption management”** che permette di conservare in modo sicuro dei segreti utilizzati dalla WebApp.

Il funzionamento prevede l'esecuzione di un server con il quale l'applicazione interagisce opportunamente.

Nonostante Hashicorp si riferisca al servizio come architettura a Plug-in, l'utilizzo sfrutta in realtà un architettura Client-Server:

Il client, e in questo caso la nostra WebApp, tramite l'utilizzo di opportuni metodi, richiede al Server un servizio.



# Tecnologie Utilizzate - Vault

L'immagine ufficiale di Vault è stata scaricata da docker hub (v. 1.12.2).

Tale immagine lanciata in un container in server mode è stata opportunamente configurata e al suo interno sono stati inseriti i segreti da contenere che all'occorrenza verranno richiesti dalla WebApp.

L'immagine modificata è stata successivamente clonata e resa disponibile per l'utilizzo.



# Tecnologie Utilizzate - Vault

La creazione del docker avviene tramite l'esecuzione di un file .yaml che provvede all'inserimento di quest'ultimo in un docker

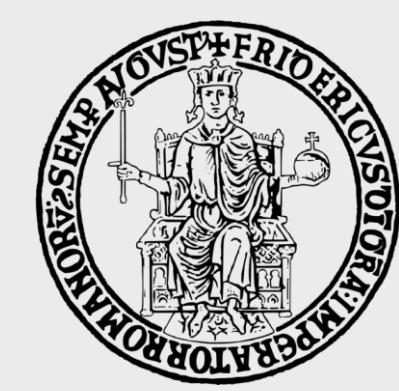
|   | NAME ↓         | IMAGE                                  | STATUS        | PORT(S)                | STARTED        | ACTIONS |
|---|----------------|--|---------------|------------------------|----------------|---------|
| □ | composedsystem | -                                      | Running (4/4) |                        |                | ■ :     |
| □ | vault          | vaultfinal:latest<br>7fb174a6ff22      | Running       | 8200:8200              | 47 minutes ago | ■ :     |
| □ | rentapp        | rentapp.war:latest<br>f6b51cff4903     | Running       | 9001:8080<br>8443:8443 | 47 minutes ago | ■ :     |
| □ | keycloak       | keycloakfinalv3:latest<br>d1717dc2b81e | Running       | 8080:8080              | 47 minutes ago | ■ :     |
| □ | db             | sqlimage:latest<br>2e6ed9a46e00        | Running       | 1433:1433              | 47 minutes ago | ■ :     |

```
32   vault:  
33     container_name: vault  
34     image: vaultfinal  
35     restart: unless-stopped  
36     ports:  
37       - 8200:8200  
38     networks:  
39       rentweb:  
40         ipv4_address: 172.21.0.5  
41     environment:  
42       - VAULT_ADDR=http://0.0.0.0:8200  
43       - VAULT_DEV_ROOT_TOKEN_ID="hvs.Klr7WSS9QJFx5StuD5fmd0Qf"  
44     cap_add:  
45       - IPC_LOCK
```

Vault è stato esposto sulla porta 8200. Il Restart è sestato a 'unless-stopped'

Nelle variabili d'ambiente sono state settate l'indirizzo di Vault e il root token di accesso.

In fine è la variabile configurata corrispondente all'IPC LOCK indica che tutte le pagine di memoria che afferiscono all'applicazione verranno conservate all'interno della RAM senza la



# Tecnologie Utilizzate - Vault

L'accesso a Vault avviene tramite un token statico, generato al primo avvio del microservizio.

A partire dal token radice è possibile creare ulteriori token per fornire l'accesso a terzi. Si verrà così a creare una struttura gerarchica di questi Token:

Nel caso in cui venga rimosso un token, verranno revocati anche tutti i token creati a partire dal token eliminato.



# Tecnologie Utilizzate - Vault

All'avvio del servizio al fine di poter accedere ai dati presenti all'interno di vault è necessario effettuare una procedura detta 'unsealing' che utilizzerà la 'Unseal Key Portion' per effettuare l' 'apertura' del servizio tramite algoritmo SHA.

Per l'unsealing possono essere selezionate un numero minimo di chiavi disponibili e un valore di threshold che corrisponde alla soglia minima intesa come numero di chiavi che dovranno essere inserite per sbloccare il vault.

Questi valori sono stati fissati entrambi ad 1 in fase di configurazione ma si potrebbe effettuare anche la scelta di distribuire più chiavi a diversi individui/entità in maniera tale da spargere e distribuire separatamente le chiavi per lo sblocco aumentando la sicurezza.

## Unseal Key Portion

.....| ↴

Unseal



# Tecnologie Utilizzate - Vault

Vault mette a disposizione differenti tipologie di 'Secret engine'.

Tra le disponibili è stato scelto di utilizzare l'engine kv ovvero <key>:<value> che ad ogni chiave associa un valore univoco.

L'inserimento del segreto può avvenire sia dalla User Interface  
La nostra Web App utilizza Vault messa a disposizione sufficien-  
porta 8200 che da linea di comando dopo per conservare in modo sicuro le aver effettuato la procedura di credenziali di accesso al

database che non vengono conservate nel codice (evitare l'Hard Coding) ma vengono richieste al servizio una sola volta in fase di avvio dell'applicazione ovvero quando la WebApp instaura la connessione al database tramite Hibernate.

| Secret                        | Metadata |
|-------------------------------|----------|
| <input type="checkbox"/> JSON |          |
| Key                           | Value    |
| password                      | .....    |
| username                      | SA       |



# Tecnologie Utilizzate - Vault

## Integrazione Con SpringMVC

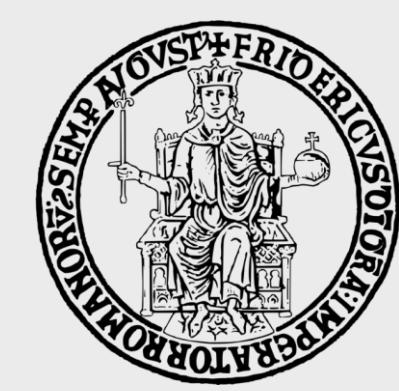
Per utilizzare le librerie di Vault all'interno dell'ambiente Spring è stato necessario importare le dipendenze corrispondenti alla versione 1.12.2 del tool.

A tal fine all'interno del file pom.xml del progetto maven, si è importata la seguente dipendenza.

In tal modo verranno scaricate nel progetto tutte le librerie java che ci permetteranno di interagire in backend con Vault.

```
<!-- Vault -->
<dependencyManagement>
    <dependencies>
        <dependency>
            <groupId>org.springframework.cloud</groupId>
            <artifactId>spring-cloud-dependencies</artifactId>
            <version>2021.0.3</version>
            <type>pom</type>
            <scope>import</scope>
        </dependency>
    </dependencies>
</dependencyManagement>
```

```
<!-- Vault -->
<dependency>
    <groupId>org.springframework.cloud</groupId>
    <artifactId>spring-cloud-starter-config</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.cloud</groupId>
    <artifactId>spring-cloud-starter-netflix-eureka-client</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.vault</groupId>
    <artifactId>spring-vault-core</artifactId>
</dependency>
```



# Tecnologie Utilizzate - Vault

## Integrazione Con SpringMVC

Dopo aver importato le dipendenze si potrà procedere all'utilizzo delle librerie.

Nella nostra applicazione è stato utilizzato Vault per conservare le credenziali di accesso al database.

Nel file di configurazione di Jdbc è stata definita una funzione getVaultCredentials nella quale viene creato un endpoint di accesso a vault e vengono settati tutti i parametri necessari alla corretta comunicazione con il software. I dati

```
private void getVaultCredentials(){
    VaultEndpoint endpoint= new VaultEndpoint();
    endpoint.setScheme(environment.getRequiredProperty("spring.cloud.vault.scheme"));
    endpoint.setHost(environment.getRequiredProperty("spring.cloud.vault.host"));
    endpoint.setPort(8200);
    endpoint.setPath(environment.getRequiredProperty("spring.cloud.vault.path"));
    TokenAuthentication token = new TokenAuthentication(environment.getRequiredProperty("spring.cloud.vault.token"));
    VaultTemplate vaultTemplate = new VaultTemplate(endpoint,token);
    VaultResponse response = vaultTemplate.read(environment.getRequiredProperty("spring.cloud.vault.datapath"));

    ObjectMapper objectMapper = new ObjectMapper();
    assert response != null;
    credentials = objectMapper.convertValue(response.getData().get("data"), Credentials.class);
}
```

```
public class Credentials {
    @Id
    private String username;
    private String password;

    public Credentials() {}

    public Credentials (String username, String password) {}

    public String getUsername() {}

    public String getPassword() {}

    public void setUsername(String username) {}

    public void setPassword (String password) {}

    public String toString() {}
}
```



# Tecnologie Utilizzate - Vault

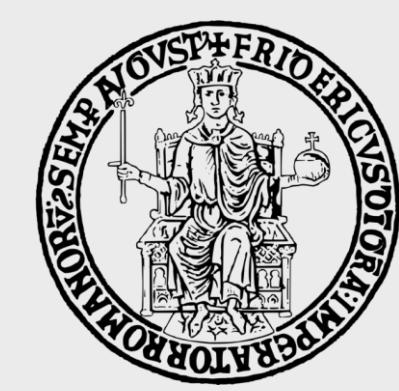
## Integrazione Con SpringMVC

Nella fase di inizializzazione della connessione Jdbc verrà poi richiamata la funzione appena definita e gli attributi dell'oggetto credential verranno utilizzati per istanziare la connessione.

L'oggetto dataSource restituito verrà utilizzato dal modulo

```
Hi
@Bean(name = "dataSource")
public DataSource dataSource()
{
    DriverManagerDataSource dataSource = new DriverManagerDataSource();
    getVaultCredentials();
    dataSource.setDriverClassName(environment.getRequiredProperty("jdbc.driverClassName"));
    dataSource.setUrl(environment.getRequiredProperty("jdbc.url"));
    dataSource.setUsername(credentials.getUsername());
    dataSource.setPassword(credentials.getPassword());

    return dataSource;
}
```



# Tecnologie Utilizzate - Vault

## Integrazione Con SpringMVC

Le informazioni utili a creare l'endpoint e quindi utili ad ottenere le informazioni da Vault sono salvate nell'application Properties.

```
#Vault
spring.cloud.vault.host=172.21.0.5
spring.cloud.vault.port=8200
spring.cloud.vault.path=v1
spring.cloud.vault.datapath=secret/data/MSSQL_access_credentials
spring.cloud.vault.token=hvs.NbLaoLyXuTrL7BY8Xt9awWcc
spring.cloud.vault.authentication=token
spring.cloud.vault.scheme=http
```

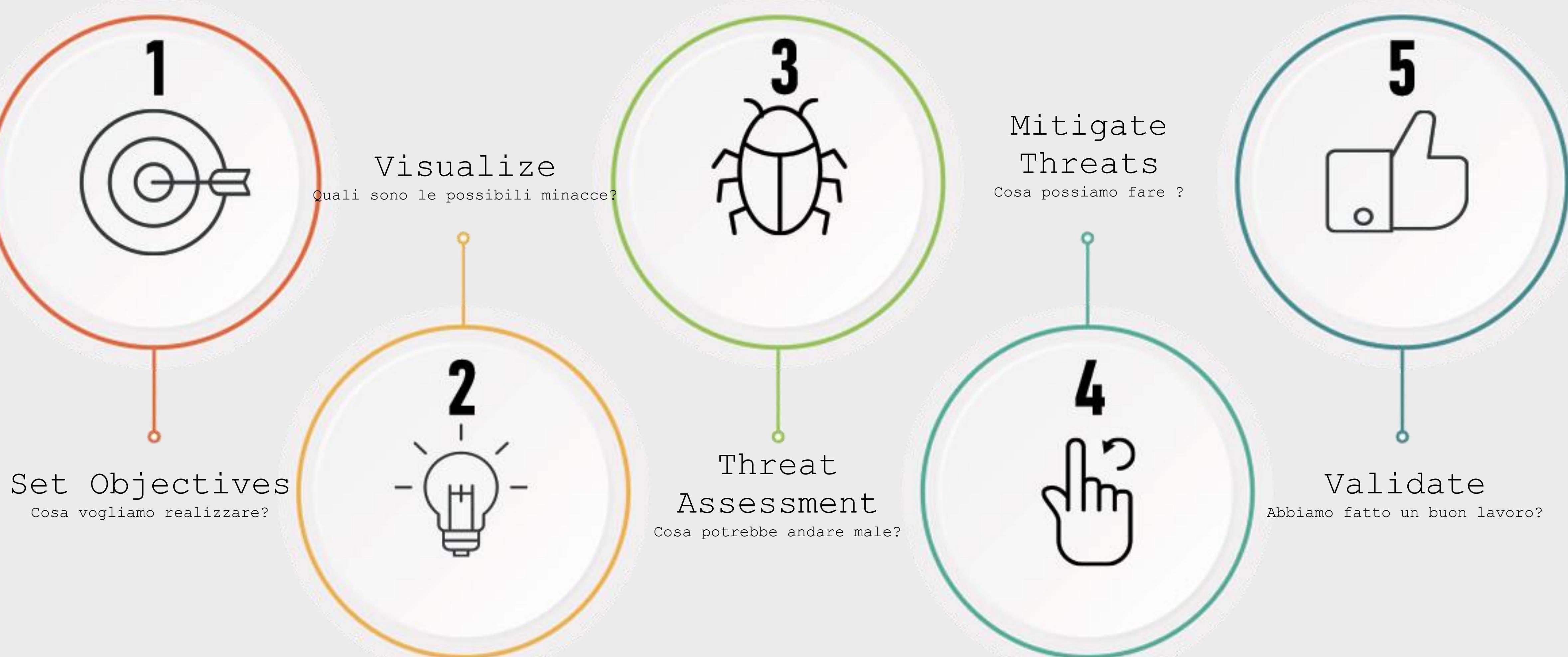
In particolare sono stati indicati:

- ▶ L'indirizzo IP del server Vault
- ▶ La porta aperta alla connessione con l'esterno
- ▶ Il root path e il datapath dove sono conservati la coppia chiave:valore
- ▶ Il token di accesso
- ▶ La tipologia di accesso da effettuare
- ▶ Il protocollo di comunicazione

Anche se il token in questo caso è esposto nel caso in cui venisse



# Threat Modeling Process





# Threat Analysis

La **threat analysis** è un processo utilizzato per determinare quali componenti del sistema devono essere protetti e quali sono i tipi di minacce ai quali sono sottoposti, determinando il rischio ad esse associato.

I **threat** includono interferenze ambientali, errori umani o meccanici nonché attacchi mirati e possono compromettere la **confidentiality**, l'**integrity** o la **availability** delle informazioni elaborate, archiviate o trasmesse.



# Threat Modeling

Il primo passo dell'analisi consiste nell'elaborare un **Threat Modeling**:

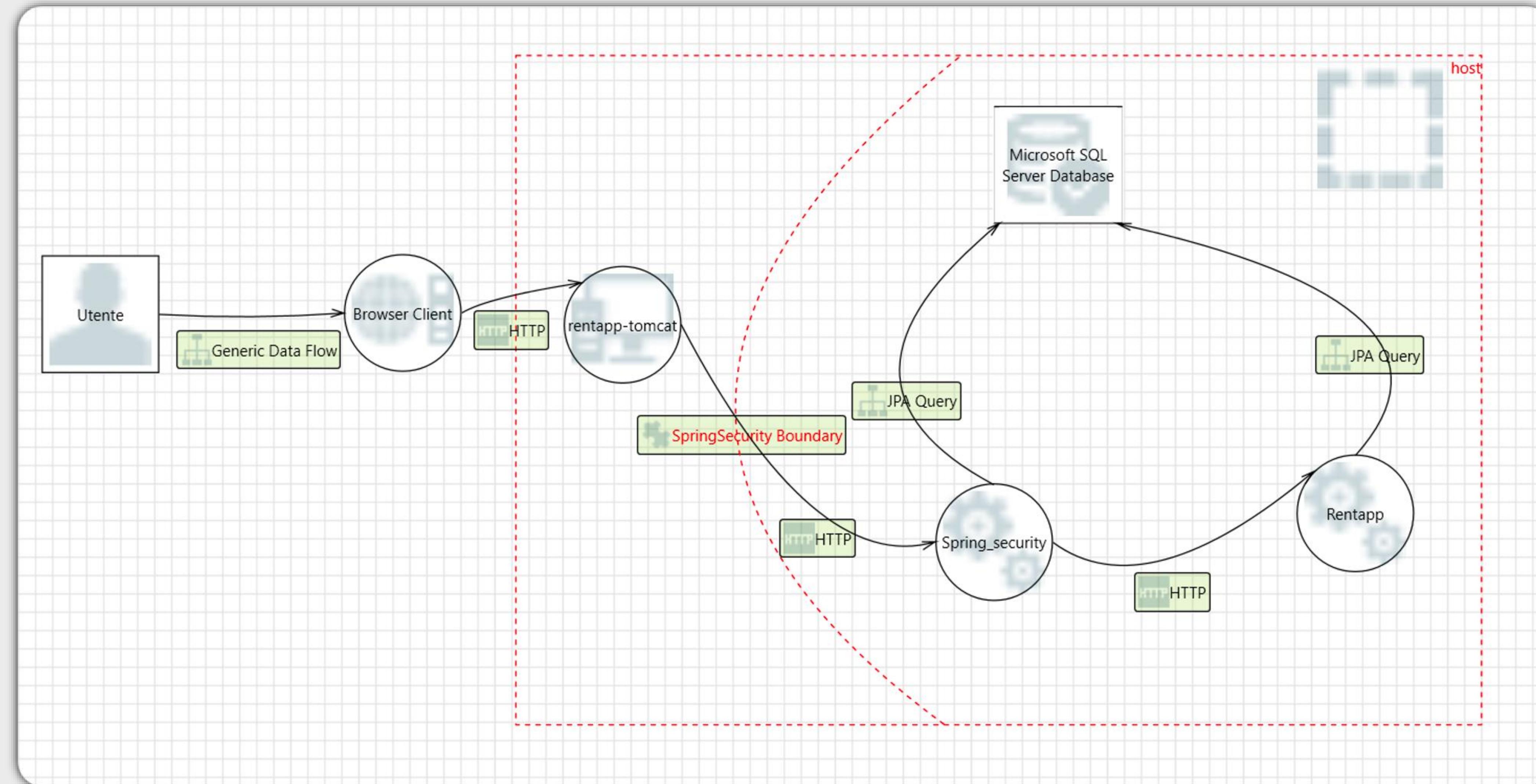
Tale processo consente di identificare, enumerare e comprendere le minacce che possono interessare l'applicazione, oltre ad essere la base di partenza da cui derivare le contromisure necessarie per mitigarle.

Per effettuare quest'operazione è stato utilizzato il tool

| Micros<br>STRIDE | Tipologia di Threat    | Proprietà Violate | Come viene effettuata la violazione?                   |
|------------------|------------------------|-------------------|--|
| S                | Spoofing               | Autenticità       | Impersonare qualcos'altro o qualcun'altro              |
| T                | Tampering              | Integrità         | Modificare dati sulla memoria, rete, etc..             |
| R                | Repudiation            | Non Repudiation   | Affermare di non aver compiuto una determinata azione  |
| I                | Information Disclosure | Confidenzialità   | Fornire informazioni a persone non autorizzate         |
| D                | Denial of Service      | Availability      | Impedire l'accesso alle risorse e/o i servizi          |
| E                | Elevation of Privilege | Authorization     | Eseguire un'azione che richiederebbe maggiori permessi |



# Threat Modeling





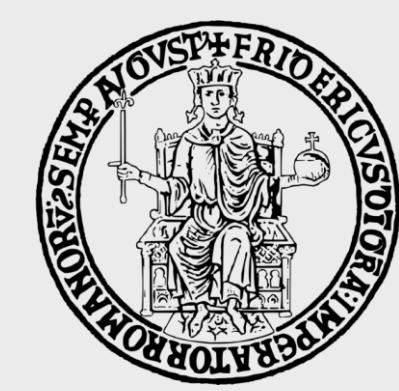
# Threat Modeling

Come si può notare è presente un enorme boundary che rappresenta il computer su cui è ospitata l'applicazione, nella versione precedente infatti tutti i servizi erano ospitati su un'unica macchina senza essere distribuiti in container.

L'applicazione .war veniva lanciata in locale sfruttando il server tomcat.

L'autenticazione avveniva tramite SpringSecurity.

I dati degli utenti erano interamente memorizzati su un Database ospitato sul servizio Microsoft SQL Server che girava sulla stessa macchina dell'applicazione.



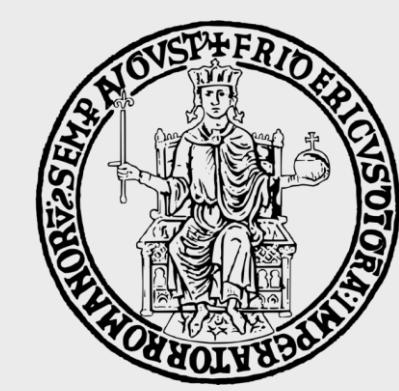
# Threat Analysis

Dopo aver effettuato la modellazione è possibile muoversi verso l'Analysis view dove viene caricata la lista delle possibili minacce.

Quest'ultima è organizzata in base a un titolo della minaccia , la categoria STRIDE a cui la minaccia appartiene , un suggerimento su come gli asset

| ID  | Diagram   | Changed By | Last Modified | State   | Title                  | Category   | Description | Justification | Interaction | Priority |
|-----|-----------|------------|---------------|---|------------------------|--|-------------|---------------|-------------|----------|
| 128 | Diagram 1 | Generated  | Not Started   | Spoofing the Browser Client Process                   | Spoofing               | Browser Client may be spoofed by an attacker and   | HTTP        | High          |             |          |
| 129 | Diagram 1 | Generated  | Not Started   | Spoofing the rentapp-tomcat Process                   | Spoofing               | rentapp-tomcat may be spoofed by an attacker an    | HTTP        | High          |             |          |
| 130 | Diagram 1 | Generated  | Not Started   | Potential Lack of Input Validation for rentapp-tomcat | Tampering              | Data flowing across HTTP may be tampered with b    | HTTP        | High          |             |          |
| 131 | Diagram 1 | Generated  | Not Started   | Potential Data Repudiation by rentapp-tomcat          | Repudiation            | rentapp-tomcat claims that it did not receive data | HTTP        | High          |             |          |
| 132 | Diagram 1 | Generated  | Not Started   | Data Flow Sniffing                                    | Information Disclosure | Data flowing across HTTP may be sniffed by an att  | HTTP        | High          |             |          |
| 133 | Diagram 1 | Generated  | Not Started   | Potential Process Crash or Stop for rentapp-tomcat    | Denial Of Service      | rentapp-tomcat crashes, halts, stops or runs slowl | HTTP        | High          |             |          |
| 134 | Diagram 1 | Generated  | Not Started   | Data Flow HTTP Is Potentially Interrupted             | Denial Of Service      | An external agent interrupts data flowing across a | HTTP        | High          |             |          |
| 135 | Diagram 1 | Generated  | Not Started   | Elevation Using Impersonation                         | Elevation Of Privilege | rentapp-tomcat may be able to impersonate the co   | HTTP        | High          |             |          |
| 136 | Diagram 1 | Generated  | Not Started   | rentapp-tomcat May be Subject to Elevation of Priv    | Elevation Of Privilege | Browser Client may be able to remotely execute cc  | HTTP        | High          |             |          |
| 137 | Diagram 1 | Generated  | Not Started   | Elevation by Changing the Execution Flow in rentap    | Elevation Of Privilege | An attacker may pass data into rentapp-tomcat in   | HTTP        | High          |             |          |
| 138 | Diagram 1 | Generated  | Not Started   | Weak Authentication Scheme                            | Information Disclosure | Custom authentication schemes are susceptible to   | HTTP        | High          |             |          |
| 139 | Diagram 1 | Generated  | Not Started   | Elevation Using Impersonation                         | Elevation Of Privilege | Rentapp may be able to impersonate the context c   | HTTP        | High          |             |          |

Il report delle possibili minacce è stato accuratamente letto e nel momento in cui una minaccia è stata mitigata questo è stato scritto nel campo "Changed by".



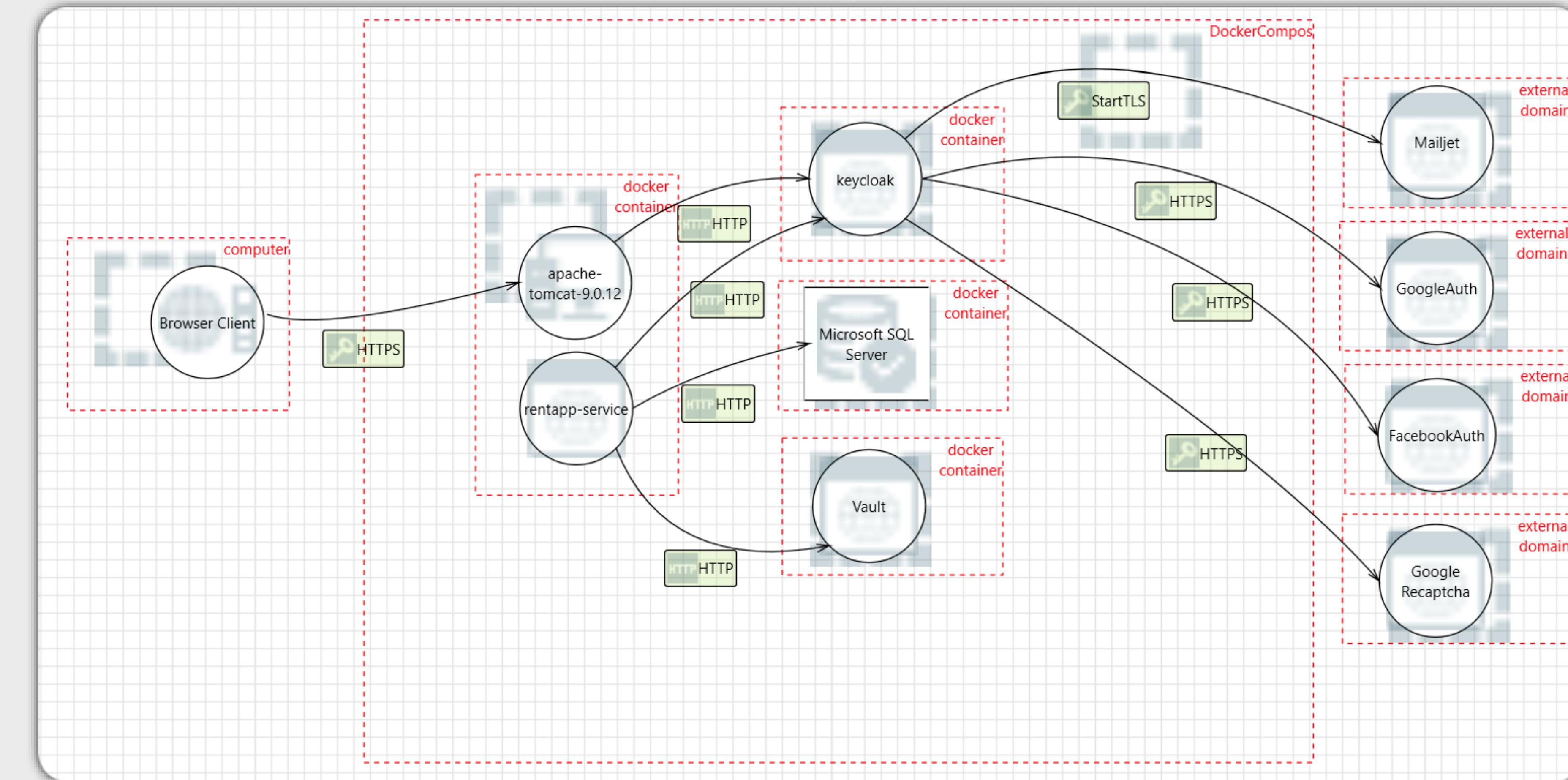
# Threat Analysis

| ID | Title   | Category               | Diagram   | Interaction       | Priority | State       | Changed By                 | Description  |
|----|---|------------------------|-----------|-------------------|----------|-------------|----------------------------|--|
| 2  | Potential Lack of Input Validation for rentapp-tomcat                               | Tampering              | Diagram 1 | HTTP              | High     | Not Started | HTTPS                      | Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against rentapp-tomcat or an elevation of privilege.       |
| 11 | Potential Lack of Input Validation for Spring_security                              | Tampering              | Diagram 1 | HTTP              | High     | Not Started |                            | Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Spring_security or an elevation of privilege.      |
| 55 | Potential SQL Injection Vulnerability for Microsoft SQL Server Database             | Tampering              | Diagram 1 | JPA Query         | High     | Not Started | Spring Security Deprecated | SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any pr     |
| 54 | Risks from Logging  | Tampering              | Diagram 1 | JPA Query         | High     | Not Started |                            | Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to    |
| 93 | Potential SQL Injection Vulnerability for Microsoft SQL Server Database             | Tampering              | Diagram 1 | JPA Query         | High     | Not Started | Keycloak                   | SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any pr     |
| 92 | Risks from Logging  | Tampering              | Diagram 1 | JPA Query         | High     | Not Started |                            | Log readers can come under attack via log files. Consider ways to canonicalize data in all logs. Implement a single reader for the logs, if possible, in order to    |
| 86 | Spoofing the Browser Client Process   | Spoofing               | Diagram 1 | HTTP              | High     | Not Started | Keycloak                   | Browser Client may be spoofed by an attacker and this may lead to unauthorized access to rentapp-tomcat. Consider using a standard authentication mecha              |
| 1  | Spoofing the rentapp-tomcat Process   | Spoofing               | Diagram 1 | HTTP              | High     | Not Started | Keycloak                   | rentapp-tomcat may be spoofed by an attacker and this may lead to information disclosure by Browser Client. Consider using a standard authentication med             |
| 10 | Spoofing the Spring_security Process  | Spoofing               | Diagram 1 | HTTP              | High     | Not Started | Spring Security Deprecated | Spring_security may be spoofed by an attacker and this may lead to information disclosure by rentapp-tomcat. Consider using a standard authentication med            |
| 53 | Spoofing of Destination Data Store Microsoft SQL Server Database                    | Spoofing               | Diagram 1 | JPA Query         | High     | Not Started | Keycloak                   | Microsoft SQL Server Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Microsoft SQL Server         |
| 84 | Spoofing the Utente External Entity   | Spoofing               | Diagram 1 | Generic Data Flow | High     | Not Started | Keycloak                   | Utente may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to i             |
| 91 | Spoofing of Destination Data Store Microsoft SQL Server Database                    | Spoofing               | Diagram 1 | JPA Query         | High     | Not Started |                            | Microsoft SQL Server Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Microsoft SQL Server         |
| 3  | Potential Data Repudiation by rentapp-tomcat  | Repudiation            | Diagram 1 | HTTP              | High     | Not Started | Keycloak                   | rentapp-tomcat claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and      |
| 12 | Potential Data Repudiation by Spring_security                                       | Repudiation            | Diagram 1 | HTTP              | High     | Not Started | Spring Security Deprecated | Spring_security claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and     |
| 59 | Potential Weak Protections for Audit Data   | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure acc               |
| 58 | Insufficient Auditing   | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is su           |
| 57 | Data Logs from an Unknown Source  | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.                    |
| 56 | Lower Trusted Subject Updates Logs  | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. C |
| 97 | Potential Weak Protections for Audit Data   | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Consider what happens when the audit mechanism comes under attack, including attempts to destroy the logs, or attack log analysis programs. Ensure acc               |
| 96 | Insufficient Auditing   | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Does the log capture enough data to understand what happened in the past? Do your logs capture enough data to understand an incident after the fact? Is su           |
| 95 | Data Logs from an Unknown Source  | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | Do you accept logs from unknown or weakly authenticated users or systems? Identify and authenticate the source of the logs before accepting them.                    |
| 94 | Lower Trusted Subject Updates Logs  | Repudiation            | Diagram 1 | JPA Query         | High     | Not Started |                            | If you have trust levels, is anyone other outside of the highest trust level allowed to log? Letting everyone write to your logs can lead to repudiation problems. C |
| 4  | Data Flow Sniffing  | Information Disclosure | Diagram 1 | HTTP              | High     | Not Started | HTTPS                      | Data flowing across HTTP may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the syst        |
| 13 | Data Flow Sniffing  | Information Disclosure | Diagram 1 | HTTP              | High     | Not Started |                            | Data flowing across HTTP may be sniffed by an attacker. Depending on what type of data an attacker can read, it may be used to attack other parts of the syst        |
| 14 | Weak Authentication Scheme  | Information Disclosure | Diagram 1 | HTTP              | High     | Not Started | Keycloak                   | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily gue                     |
| 61 | Weak Credential Storage   | Information Disclosure | Diagram 1 | JPA Query         | High     | Not Started | Vault                      | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a s     |
| 60 | Authorization Bypass  | Information Disclosure | Diagram 1 | JPA Query         | High     | Not Started |                            | Can you access Microsoft SQL Server Database and bypass the permissions for the object? For example by editing the files directly with a hex editor, or reac         |
| 87 | Weak Authentication Scheme  | Information Disclosure | Diagram 1 | HTTP              | High     | Not Started | Spring Security Deprecated | Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily gue                     |
| 98 | Weak Credential Storage   | Information Disclosure | Diagram 1 | JPA Query         | High     | Not Started | Vault/Keycloak             | Credentials held at the server are often disclosed or tampered with and credentials stored on the client are often stolen. For server side, consider storing a s     |
| 7  | Elevation Using Impersonation   | Elevation Of Privilege | Diagram 1 | HTTP              | High     | Not Started |                            | rentapp-tomcat may be able to impersonate the context of Browser Client in order to gain additional privilege.   |
| 8  | rentapp-tomcat May be Subject to Elevation of Privilege Using Remote Code Execution | Elevation Of Privilege | Diagram 1 | HTTP              | High     | Not Started |                            | Browser Client may be able to remotely execute code for rentapp-tomcat.  |



# Threat Analysis

Nel momento in cui si è migrati verso l'architettura dockerizzata a microservizi è stata effettuata un'ulteriore modellazione del software e successiva analisi dei possibili threat.





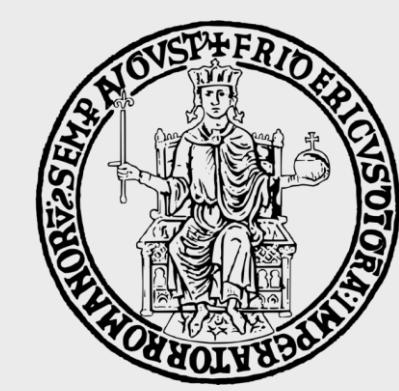
# Threat Analysis - Assessment

Ancora una volta sono state identificati i Threat.

| ID | Diagram | Changed By | Last Modified | Title            | Category         | Description     | Justification | Interaction | Priority |
|----|---------|------------|---------------|------------------|------------------|-----------------|---------------|-------------|----------|
| 11 |         | Generated  | Not Started   | Spoofing the ap  | Spoofing         | apache-tomcat-  |               | HTTP        | High     |
| 12 |         | Generated  | Not Started   | Spoofing the ke  | Spoofing         | keycloak may b  |               | HTTP        | High     |
| 13 |         | Generated  | Not Started   | Potential Lack o | Tampering        | Data flowing ac |               | HTTP        | High     |
| 14 |         | Generated  | Not Started   | apache-tomcat-   | Tampering        | If apache-tomc  |               | HTTP        | High     |
| 15 |         | Generated  | Not Started   | Potential Data F | Repudiation      | keycloak claims |               | HTTP        | High     |
| 16 |         | Generated  | Not Started   | Data Flow Sniffi | Information Dis  | Data flowing ac |               | HTTP        | High     |
| 17 |         | Generated  | Not Started   | Potential Proce  | Denial Of Servic | keycloak crashe |               | HTTP        | High     |
| 18 |         | Generated  | Not Started   | Data Flow HTTF   | Denial Of Servic | An external age |               | HTTP        | High     |
| 19 |         | Generated  | Not Started   | Elevation Using  | Elevation Of Pri | keycloak may b  |               | HTTP        | High     |
| 20 |         | Generated  | Not Started   | keycloak May b   | Elevation Of Pri | apache-tomcat-  |               | HTTP        | High     |
| 21 |         | Generated  | Not Started   | Elevation by Ch  | Elevation Of Pri | An attacker may |               | HTTP        | High     |
| 22 |         | Generated  | Not Started   | Spoofing the re  | Spoofing         | rentapp-service |               | HTTP        | High     |

All'interno della lista poi sono stati selezionati quelli effettivi e si è proceduto con il confronto con il file NIST SP 800-53 v.5 al fine di poter identificare i possibili controlli di sicurezza.

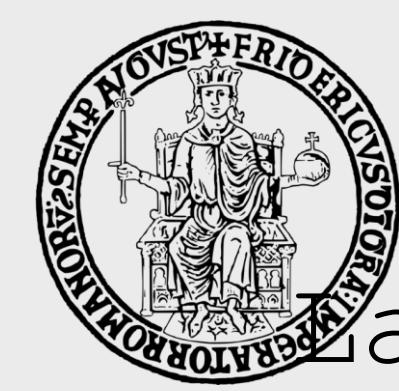
| Threat                               | STRIDE                 | Controlli di Sicurezza                          |
|--------------------------------------|------------------------|---|
| Spoofing the rentapp-service Process | Spoofing               | IA-2, IA-3, IA-4, IA-5, IA-7, AC-2, AC-4, SC-10 |
| Weak Authentication Scheme           | Information Disclosure | AC-2, AC-17(2), IA-5(6), IA-6, SC-13, SC-28     |
| ...                                  | ...                    | ...   |



# Threat Analysis - Assessment

Procedendo come appena visto per ogni possibile threat reale che si è voluto mitigare si è ricavata la seguente tabella di controlli del NIST da implementare al fine di 'eliminare' i possibili threat. L'assessment dell'applicazione, in accordo con il NIST, è stato effettuato per il livello di **impatto moderato**.

| STRIDE                 | Controlli di Sicurezza   |
|------------------------|--|
| Spoofing               | IA-2, IA-3, IA-4, IA-5, IA-7, IA-11, IA-12(2)(3)(5) <sub>SEP</sub> AC-2, AC-4, AC-7, AC-10, AC-12 <sub>SEP</sub> SC-10, SC-17, SC-23 |
| Tampering              | AC-3, AC-17(2) <sub>SEP</sub> SC-8, SC-12, SC-13, SC-23, SC-28   |
| Repudiation            | IA-2, IA-4, IA-5, IA-11, IA-12 <sub>SEP</sub> AC-2 <sub>SEP</sub> SC-17  |
| Information Disclosure | IA-5(6), IA-6<br>AC-2(12), AC-3, AC-4, AC-17(2), AC-20 <sub>SEP</sub> SC-8, SC-12, SC-13, SC-23, SC-28                               |
| Denial Of Service      |  |
| Elevation Of Privilege | AC-3, AC-6 <sub>SEP</sub> SC-2, SC-39  |



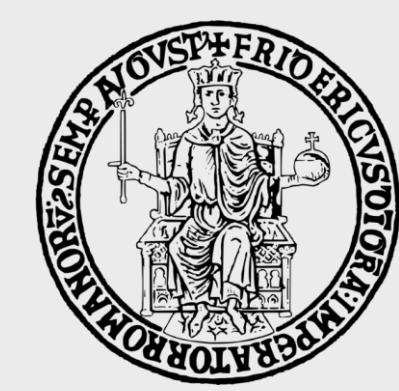
# NIST - Security Controls

La pubblicazione "NIST 800-53 v.5" fornisce un catalogo di controlli di sicurezza e privacy per sistemi informativi e aziende al fine di proteggere assets e operazioni organizzative, individui e altre organizzazioni da una serie di minacce come attacchi, errori umani, disastri naturali, fallimenti strutturali, entità di intelligence straniera e rischi per la privacy.

Il catalogo dei controlli presentato dal NIST affronta anche la sicurezza e la privacy dalle prospettive di funzionalità e garanzia al fine di rendere i prodotti sufficientemente affidabili.



**National Institute of  
Standards and Technology**



# NIST - AC: Access Control

Per Access Controls si intendono i controlli che gestiscono il processo di concessione o di rifiuto di richieste specifiche per :

- ▶ Ottener e utilizzare informazioni e relativi servizi di elaborazione delle informazioni.
- ▶ Accedere a strutture fisiche specifiche (ad esempio, edifici federali, stabilimenti militari, varchi di frontiera).

-NIST FIPS 201-3 .

Di seguito la trattazione dei controlli:

AC-2 (1) (3) (4) (5) (12), AC-3 (5) (7) (14), AC-4 (17) (24), AC-5, AC-6 (1) (5) (6) (10), AC-7, AC-8, AC-10, AC-12 (1) (2), AC-17 (1) (2) (3), AC-20.



# AC-2 : ACCOUNT MANAGEMENT

1. Definire e documentare i tipi di account permessi e specificare l'uso proibito all'interno del sistema
2. Assegnare un manager degli account
3. Richiedere prerequisiti e criteri per un determinato ruolo
4. Specificare :
  - Utenti autorizzati all'utilizzo del sistema
  - Appartenenza a gruppi e ruoli
  - Autorizzazioni di accesso per ciascun account (es: privilegi)
5. Richiedere l'approvazione da parte dell'organizzazione per le richieste di creazione di account
6. Avere la possibilità di creare, abilitare, modificare e rimuovere account in accordo con policy, procedure, prerequisiti e criteri definiti dall'organizzazione
7. Monitorare l'utilizzo degli account
8. Notificare gli account manager e il personale o ruolo definito dall'organizzazione nel caso in cui:
  - Gli account non sono più utilizzati
  - Gli utenti sono stati eliminati o trasferiti
  - Quando ci sono cambiamenti nell'utilizzo del sistema o di qualcosa di importante, che l'individuo deve sapere
9. Autorizzare l'accesso al sistema sulla base di :
  - Un'autorizzazione di accesso valida
  - Un utilizzo previsto del sistema
  - Attributi definiti dall'organizzazione
10. Rivedere gli account in conformità ai requisiti di gestione degli account
11. Stabilire e implementare un processo per la modifica degli autenticatori di account condivisi o



# AC-2 : ACCOUNT MANAGEMENT

1. Definire e documentare i tipi di account permessi e specificare l'uso proibito all'interno del sistema

Rentapp definisce due tipologie di account permessi identificati da due ruoli: **Gestori** e **Cliente**. Ogni account è identificato da un username e un indirizzo email univoco. Nel caso di registrazione con autenticazione federata (G-Auth o FacebookAuth) l'username risulta uguale all'email.

2. Assegnare un manager degli account

Un **Accounts Manager** è stato creato al fine di amministrare gli utenti registrati all'applicazione: Questo potrà creare utenti, modificarne gli attributi, richiederne azioni necessarie e assegnargli ruoli e privilegi.



# AC-2 : ACCOUNT MANAGEMENT

accounts manager

Enabled Action ▾

| Details   | Attributes | Credentials            | Role mapping | Groups | Consents | Identity provider links | Sessions |
|---|------------|------------------------|--------------|--------|----------|-------------------------|----------|
| <input type="text"/> Search by name → <input checked="" type="checkbox"/> Hide inherited roles <input type="button" value="Assign role"/> <input type="button" value="Unassign"/> 1 - 4 ▾ < > |            |                        |              |        |          |                         |          |
| <input type="checkbox"/> Name   | Inherited  | Description            |              |        |          |                         |          |
| <input type="checkbox"/> default-roles-rentapp  | False      | \${role_default-roles} |              |        |          |                         |          |
| <input type="checkbox"/> realm-management query-users   | False      | \${role_query-users}   |              |        |          |                         |          |
| <input type="checkbox"/> realm-management query-clients   | False      | \${role_query-clients} |              |        |          |                         |          |
| <input type="checkbox"/> realm-management manage-users  | False      | \${role_manage-users}  |              |        |          |                         |          |



# AC-2 : ACCOUNT MANAGEMENT

3. Richiedere prerequisiti e criteri per un determinato ruolo

Ogni account di tipo cliente dopo la registrazione, come prerequisito, per accedere al servizio dovranno fornire al primo accesso una serie di dati identificativi (i.e., Numero Patente, Codice Fiscale, Data di Nascita...).

In assenza della compilazione del form, l'account, anche se registrato correttamente al servizio di Autenticazione, non avrà la possibilità di accedere alle funzionalità offerte dalla webApp. Inoltre, ogni utente che si registrerà dovrà confermare l'indirizzo email fornito, seguendo le istruzioni ricevute tramite email.



# AC-2 : ACCOUNT MANAGEMENT

4 . Specificare :

- Utenti autorizzati all'utilizzo del sistema
- Appartenenza a gruppi e ruoli
- Autorizzazioni di accesso per ciascun account (es: privilegi)

Ogni utente può accedere ad un set di funzionalità esclusive per il ruolo assegnatogli. Inoltre ognuno di essi oltre alle proprie informazioni personali, potrà accedere a dati relativi ad altri utenti solo se questi sono condivisi con l'utente in esame.  
(es: Un gestore potrà vedere l'username dell'utente che ha prenotato un autoveicolo presente all'interno del suo parco auto).



# AC-2 : ACCOUNT MANAGEMENT

- 5.Richiedere l'approvazione da parte dell'organizzazione per le richieste di creazione di account

La richiesta per la creazione di un account di tipo cliente non deve essere approvata da un amministratore. Tuttavia, un account di tipo cliente, per ottenere il ruolo gestore dovrà fare richiesta (i.e., via mail) ad un amministratore di sistema ([rentappssd@gmail.com](mailto:rentappssd@gmail.com)).

Inoltre all'atto della creazione dell'account l'utente dovrà confermare l'indirizzo fornito aprendo il link di conferma inviatogli via email.



# AC-2 : ACCOUNT MANAGEMENT

6. Avere la possibilità di creare, abilitare, modificare e rimuovere account in accordo con policy, procedure, prerequisiti e criteri definiti dall'organizzazione

Per la gestione degli account è possibile utilizzare l'admin console di Keycloak che permette all'amministratore di sistema di monitorare gli utenti registrati fornendo informazioni sulla loro registrazione e sulle loro sessioni attive.

All'occorrenza l'amministratore di sistema può bloccare o eliminare un account. Non è stato prevista la possibilità di richiedere la disattivazione del proprio account.



# AC-2 : ACCOUNT MANAGEMENT

## 7. Monitorare l'utilizzo degli account

Il monitoraggio delle azioni degli utenti può essere controllato tramite la sezione Events di keycloak da parte dell'amministratore di sistema.

**Events**

Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events Admin events

Search user event Refresh 1 - 4

| Time                           | User                                 | Event type            | IP address | Client         |
|--------------------------------|--------------------------------------|-----------------------|------------|----------------|
| » December 17, 2022 at 1:40 PM | 985e2c2f-399c-4990-af29-121df78b50d5 | ✓ CODE_TO_TOKEN       | 172.21.0.2 | rentapp_client |
| » December 17, 2022 at 1:40 PM | 985e2c2f-399c-4990-af29-121df78b50d5 | ✓ LOGIN               | 172.21.0.1 | rentapp_client |
| » December 17, 2022 at 1:39 PM | 985e2c2f-399c-4990-af29-121df78b50d5 | ⚠ LOGIN_ERROR         | 172.21.0.1 | rentapp_client |
| » December 17, 2022 at 1:39 PM | 985e2c2f-399c-4990-af29-121df78b50d5 | ✓ SEND_RESET_PASSWORD | 172.21.0.1 | rentapp_client |



# AC-2 : ACCOUNT MANAGEMENT

8. Notificare gli account manager e il personale o ruolo definito dall'organizzazione nel caso in cui:

- Gli account non sono più utilizzati
- Gli utenti sono stati eliminati o trasferiti
- Quando ci sono cambiamenti nell'utilizzo del sistema o di qualcosa di importante, che l'individuo deve sapere

L'amministratore di sistema deve notificare agli utenti le particolari azioni che devono essere intraprese sul proprio account.

In particolare, nel caso in cui sono cambiati i termini e codizioni dell'applicazione selezionando la voce 'Terms and Condition' all'accesso successivo l'utente dovrà accettare nuovamente i termini

|                       |  |
|-----------------------|--|
| Username *            | ne_ne.12.06@hotmail.it                       |
| Email                 | ne_ne.12.06@hotmail.it                       |
| Email verified        | <input type="checkbox"/> Off                 |
| First name            | Nello  |
| Last name             | Ambrosio                                     |
| Required user actions | <input type="button" value="Select action"/> |

- [Configure OTP](#)
- [Terms and Conditions](#)
- [Update Password](#)
- [Update Profile](#)
- [Verify Email](#)
- [Delete Account](#)
- [Webauthn Register](#)
- [Webauthn Register Passwordless](#)
- [Update User Locale](#)



# AC-2 : CONTROL ENHANCEMENTS

AC-2 (1) : supporta la gestione degli account utilizzando meccanismi automatizzati.

È stata affidata la creazione in maniera automatizzata degli account ad un sistema di autenticazione esterno all'applicazione (i.e. Keycloak). AC-2 (3) : disabilita gli account in un determinato periodo o nel caso in cui:

- Sono Scaduti
- Non sono più associati ad un utente o un individuo
- Violano le policy dell'organizzazione
- Sono inattivi per un determinato periodo

L'Accounts Manager può provvedere a eliminare gli account dalla console di amministrazione di Keycloak. Questo processo viene fatto manualmente, nel caso in cui fosse stato un processo automatico



# AC-2 : CONTROL ENHANCEMENTS

AC-2 (4) : il sistema salva automaticamente le azioni di creazione, modifica, abilitazione, disabilitazione e rimozione degli account.

Tutte le azioni compiute dall'Account's Manager vengono salvate automaticamente dal tool Keycloak. Inoltre l'IAM salva in automatico gli utenti in fase di sign-up.

AC-2 (5) : è necessario il log-out dell'utente quando è trascorso un determinato periodo di tempo di inattività

Il sistema è stato settato per terminare le sessioni attive automaticamente dopo 30 minuti di inattività.

**SSO Session Settings**

SSO Session Idle ② 30 Minutes ▾



# AC-2 : CONTROL ENHANCEMENTS

AC-2 (12) : monitorare gli account di sistema per un uso atipico o violazioni di policy

Tramite la sezione Events è possibile monitorare anche le azioni intraprese dagli amministratori del sistema. Dal report fornito è inoltre possibile vedere l'ip d'accesso al sistema, che potrebbe corrispondere ad una posizione geografica atipica per il

**Events**  
Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events Admin events

Search admin event Refresh

1 - 10

| Time                         | Resource path                             | Resource type       | Operation ty... | User                                 |
|------------------------------|---|---------------------|-----------------|--------------------------------------|
| December 17, 2022 at 2:04 PM | groups/baae5ff5-88d8-41a9-96f7-9cc3351... | GROUP               | DELETE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 2:04 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | GROUP_MEMBERSHIP    | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 2:03 PM | groups/baae5ff5-88d8-41a9-96f7-9cc3351... | GROUP               | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:58 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | USER                | ACTION          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:54 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | CLIENT_ROLE_MAPPING | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:54 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | CLIENT_ROLE_MAPPING | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:54 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | CLIENT_ROLE_MAPPING | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:54 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | REALM_ROLE_MAPPING  | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |

| Time                         | Resource path                             | Resource type    | Operation ty... | User                                 |
|------------------------------|---|------------------|-----------------|--------------------------------------|
| December 17, 2022 at 2:04 PM | groups/baae5ff5-88d8-41a9-96f7-9cc3351... | GROUP            | DELETE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 2:04 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | GROUP_MEMBERSHIP | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 2:03 PM | groups/baae5ff5-88d8-41a9-96f7-9cc3351... | GROUP            | CREATE          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| December 17, 2022 at 1:58 PM | users/6c66f77f-d459-44ff-8204-f4bc7020... | USER             | ACTION          | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |

**Auth**

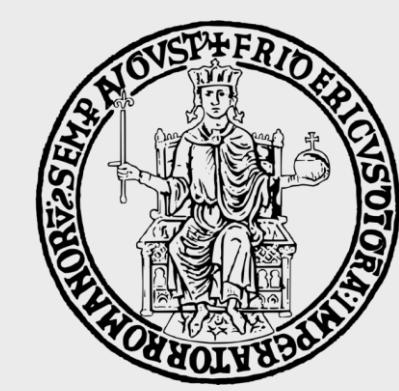
| Attribute  | Value                                |
|------------|--------------------------------------|
| Realm      | 4107c011-9a60-474a-b3fb-9ee66426adb5 |
| Client     | 7dff67f1-da20-4882-a57c-22e4573062d8 |
| User       | 86155b5e-b903-4157-9cd5-11d4f55cfe92 |
| IP address | 172.21.0.1                           |



# AC-3 : ACCESS ENFORCEMENT

Imposizione delle autorizzazioni approvate per l'accesso logico alle informazioni e alle risorse di sistema in conformità alle policy di controllo degli accessi applicabili.

L'enforcement delle autorizzazioni per l'accesso logico alle informazioni e alle risorse del sistema è stato effettuato secondo le policy di controllo degli accessi applicabili: sono stati definiti su Keycloak scopes associati, permission sugli scopes. L'abilitazione dell'enforcement delle policy da parte di keycloak e la protezione dei path ad accesso ristretto della web-app è stata gestita tramite gli adapter di Tomcat per keycloak e definiti nel file web.xml della web app.



# AC-3 : CONTROL ENHANCEMENTS

AC-3 (5) : prevenire l'accesso a informazioni di sicurezza rilevanti eccetto durante stati sicuri del sistema.

La webapp impiega meccanismi per proteggere i dati e applica la crittografia a livello trasporto tramite TLS per tutte le comunicazioni con entità esterne al “perimetro di sicurezza” delimitato dalla rete virtuale privata realizzata da docker compose.

In aggiunta, Keycloak impiega un servizio di Identity & Access Management con il fine di garantire l'accesso alle risorse del sistema solo da parte delle entità autorizzate.



# AC-3 : CONTROL ENHANCEMENTS

AC-3 (7) : definire una policy di accesso alle risorse del sistema di tipo role based.

Il servizio di Identity & Access management Keycloak impone l'accesso agli oggetti e alle funzioni del sistema in base al ruolo di appartenenza dell'utente interessato all'accesso. I ruoli **gestore** e **cliente** accedono a parti distinte del sistema "dashboard\_gestore" e "dashboard\_cliente" che danno accesso ad un insieme di funzioni differenti. AC-3 di (14) fornisce meccanismi per permettere agli utenti l'accesso alle loro informazioni personali identificabili conservate dal sistema.

Ogni utente che registra i propri dati all'interno dell'applicazione può visualizzarli in una view di riepilogo. Ciò aiuta gli utenti a comprendere come le loro informazioni personali sensibili vengono elaborate e conservate.



# AC-4 : INFORMATION FLOW ENFORCEMENT

Applicazione di autorizzazioni per il controllo del flusso di informazioni all'interno del sistema e dei sistemi collegati.

Sono stati implementati meccanismi di controllo del flusso di informazioni all'interno del sistema e dei sottosistemi connessi tramite il controllo delle sessioni degli utenti .



# AC-4 : CONTROL ENHANCEMENTS

AC-4 (17) : identificare univocamente e autenticare sorgente e destinazione di ogni trasferimento di informazioni.

Il processo di sign-up e sign-in previsto dall'applicazione permette di identificare univocamente l'utente che instaura una comunicazione con il server la quale comporta un trasferimento di informazioni.

Le comunicazioni tra un utente e il server dell'applicazione AC-4 (24) : il trasferimento di informazioni tra diversi domini di sicurezza possono essere monitorate dalla sezione "Sessioni" della console admin di Reycloak. comporta un analisi preventiva dei dati in ingresso al fine di rigenerare i dati in un formato normalizzato interno coerente con le specifiche previste.

All'interno dell'applicazione i dati in input vengono controllati al fine di rispettare dei vincoli imposti per la loro corretta memorizzazione. (i.e., Un parser java trasforma le date in un



# AC-5 : SEPARATION OF DUTIES

L'organizzazione definisce le autorizzazioni di accesso alle funzionalità del sistema attraverso **separazione dei compiti tra diversi utenti o ruoli**.

Gli utenti all'interno dell'applicazione possono assumere due tipi di ruoli: Cliente e Gestore.

L'insieme delle funzionalità del sistema e delle risorse a disposizione risulta disgiunto, infatti un cliente può accedere alla sezione "dashcliente" effettuando una prenotazione, o semplicemente visualizzando il proprio storico.

L'utente di tipo Gestore invece, accedendo alla sezione "dashgestore" può creare un parco auto, inserire all'interno di quest'ultimo un nuovo autoveicolo o visualizzare le prenotazioni relative a uno dei propri parchi auto.



## AC-6 : LEAST PRIVILEGE

Adottare il principio del privilegio minimo, concedendo agli utenti solo le azioni necessarie per portare a termine il loro compiti

Ogni utente dell'applicazione può svolgere solo le azioni relative al ruolo che gli compete, senza "overlapping" di funzionalità e responsabilità.



# AC-6: CONTROL ENHANCEMENTS

AC-6 (1) : autorizzare l'accesso alle funzioni di sicurezza e ai dati relativi alla sicurezza.

Le informazioni e le funzionalità relative alla sicurezza come la gestione delle policy, dei privilegi, dei permessi e la creazione di account di sistema sono accessibili, previa autenticazione, solo all'amministratore di sistema tramite Keycloak e agli sviluppatori.

AC-6 (5) : limitare l'utilizzo di account privilegiati soltanto al personale autorizzato

Soltanto l'amministratore di sistema ha privilegi sugli altri utenti, ma, in ogni caso, nemmeno quest'ultimo può modificare/eliminare informazioni di altri utenti quali prenotazioni, parchi auto o veicoli. Ogni utente gestisce di per sé i dati ottenuti dalle interazioni con il sistema che sono "incapsulati" nel contesto dell'utente stesso. L'unico che ha accesso alle informazioni di tutti gli utenti è il DBAdmin che può

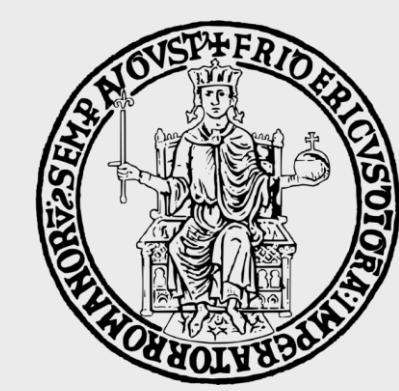


# AC-6: CONTROL ENHANCEMENTS

AC-6 (6) : Revisionare periodicamente i privilegi assegnati a ruoli o utenti al fine di validare la necessità di tali privilegi e, se necessario, modificarli al fine di adattarli alle esigenze.

Tramite l'inserimento del software Keycloak quest'operazione è resa molto semplice all'owner del sistema che in ogni momento, e quindi anche periodicamente con una certa cadenza, può ridefinire i ruoli e i privilegi assegnati agli utenti e al personale. In particolare:

- i ruoli e i privilegi amministrativi sugli utenti possono essere ridefiniti dalla dashboard dell'admin del Realms di Keycloak.
- i path, e quindi le funzioni permesse, per i vari utenti possono essere ridefiniti dal file web.xml di tomcat.

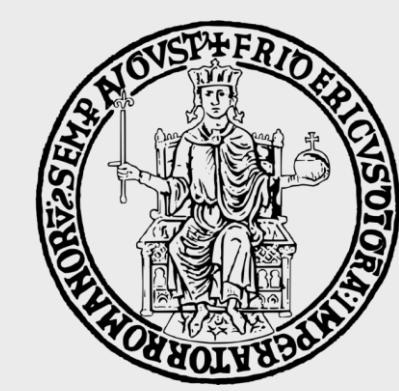


# AC-6: CONTROL ENHANCEMENTS

AC-6 (10) : vietare l'esecuzione di funzioni privilegiate ad utenti non privilegiati

Soltanto gli utenti di tipo gestore possono creare parchi auto e inserire veicoli all'interno di essi tramite la dashgestore, motivo per cui verrà restituito un messaggio di errore 403 all'utente che senza ruolo adeguato prova l'accesso a queste funzionalità.

(N.B AC-3 Enforcement degli accessi rafforza questo enhancement)



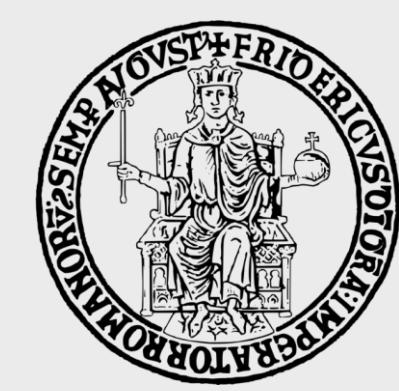
# AC-7: UNSUCCESSFUL LOGON ATTEMPTS

Rafforza il limite di tentativi di accesso non validi consecutivi da parte di un utente durante un frangente di tempo definito dall'organizzazione. Automaticamente blocca l'account per un determinato intervallo di tempo prestabilito o finché non viene sbloccato dall'amministratore.

Keycloak permette la gestione e la configurazione in maniera semplice di una serie di parametri che forniscono una maggiore sicurezza agli utenti registrati al sistema contro attacchi a Dizionario o Brute force.

Infatti è possibile configurare il software affinché identifichi tentativi di accesso ravvicinati falliti e disabiliti gli account interessati nell'insicurezza di un presunto attacco.

L'applicazione è stata settata per bloccare temporaneamente l'account dopo 5 tentativi falliti consecutivi.



# AC-7: UNSUCCESSFUL LOGON ATTEMPTS

I tentativi consecutivi effettuati si resetteranno ogni 5 ore. Il tempo di blocco è definito in maniera incrementale, ad ogni 5 tentativi di accesso consecutivi falliti l'applicazione bloccherà l'account per 12 ore in più rispetto al tempo dell'ultimo blocco per un massimo di 90 giorni.

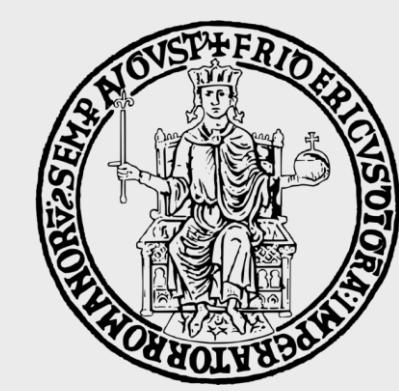
Inoltre ad ogni tentativo d'accesso fallito l'utente verrà

~~avvisato tramite email~~

**R Rentapp** Cestino - Google l'altro ieri, 13:39  
Login error A: Nello Ambrosio,  
Rispondi a: Rentapp

 Il messaggio fa parte di una mailing list. Annulla iscrizione X

A failed login attempt was detected to your account on Sat Dec 17 12:39:39 UTC 2022 from 172.21.0.1. If this was not you, please contact an administrator.



# AC-7: UNSUCCESSFUL LOGON ATTEMPTS

Il tempo di blocco è stato scelto come conseguenza dell'ulteriore  
requisito di sicurezza: Infatti se avessimo impostato un tempo di  
blocco minore, un utente malintenzionato avrebbe potuto utilizzare  
consapevolmente il software per saturare la casella mail  
dell'utente.

Realm settings are settings that control the options for users, applications, roles, and groups in the current realm. [Learn more](#)

General Login Email Themes Keys Events Localization Security defenses Sessions Tokens Client >

Headers Brute force detection

Enabled  On

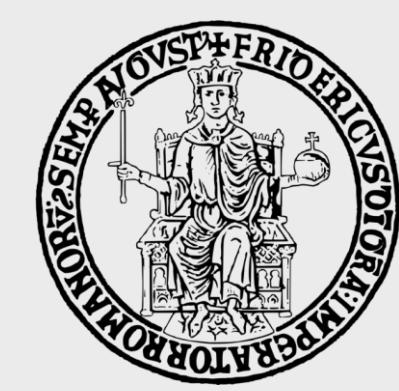
Max login failures

Permanent lockout  Off

Wait increment   Hours

Max wait  Days

Failure reset time  Hours



# AC-7: UNSUCCESSFUL LOGON ATTEMPTS

Inoltre è stata impostata una finestra temporale di 1 secondo come minimo tempo che deve intercorrere tra due tentativi di accesso consecutivi, in quanto al di sotto di questa soglia l'azione non può essere stata intrapresa da un utente umano e quindi di conseguenza è un sistema di protezione in più contro un attaccante malintenzionato. Se vengono rilevati due tentativi di accesso

nella stessa finestra temporale di 1 secondo

blocca  
**Quick login check**  
milliseconds

- 1000 +

**Minimum quick login**  
wait

Minutes

Sign in to your account

**Account is disabled, contact your administrator.**

Username or email

nello97

Password

.....

Remember me

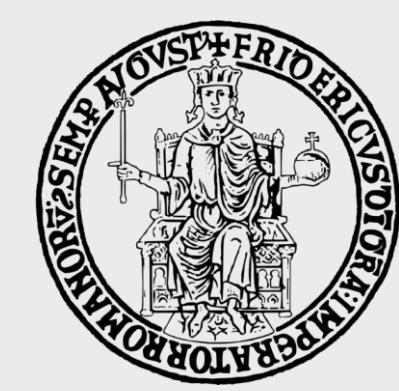
[Forgot Password?](#)

SessionTabId=D08cbWceBqE

2022-12-19 12:05:45 2022-12-19 11:05:45,288 WARN [org.keycloak.services] (Brute Force Protector)

KC-SERVICES0053: login failure for user 985e2c2f-399c-4990-af29-121df78b50d5 from ip 172.21.0.1

2022-12-19 12:05:45 2022-12-19 11:05:45,298 WARN [org.keycloak.events] (executor-thread-0) type=L



# AC-8 : SYSTEM USE NOTIFICATION

- a) Mostrare un messaggio/banner a tutti gli utenti prima che effettuino l'accesso alla piattaforma. Tale messaggio avvisa gli utenti sulla privacy e sulla sicurezza in maniera conforme alle leggi, le direttive, le regole , le politiche , gli standard e le linee guida applicabili. Inoltre bisogna informare l'utente che le sue attività all'interno del sistema saranno monitorate, registrate e soggette a revisione.
- b) Mantenere il messaggio sullo schermo finché l'utente non accetta le condizioni di utilizzo.

Nel sistema Rentapp, al fine di completare la registrazione di un nuovo account, l'utente deve obbligatoriamente accettare e visionare le Terms and Conditions. La funzione è resa disponibile da Keycloak e attivabile per farla comparire durante il flusso di registrazione al servizio.



# AC-8 : SYSTEM USE NOTIFICATION

## Authentication

Authentication is the area where you can configure and manage different credential types. [Learn more](#)

| Required actions     | Enabled                                | Set as default action                  |
|----------------------|--|--|
| Configure OTP        | <input checked="" type="checkbox"/> On | <input checked="" type="checkbox"/> On |
| Terms and Conditions | <input checked="" type="checkbox"/> On | <input checked="" type="checkbox"/> On |

Inoltre è possibile richiedere di accettare nuovamente i temini e condizioni nel caso quest'ultimi cambino per l'applicazione (in accordo con l'Enhancements AC-1).

Required user actions

Terms and Conditions x

Select action

? X ▼



# AC-8 : SYSTEM USE NOTIFICATION

The screenshot shows the interior of a car with a Kia logo on the steering wheel. The infotainment screen displays the Rentapp website. At the top, it says "RENTAPP". Below that, there is a blurred background image of a city street at night. The main content area is titled "Terms and Conditions". Under this title, there is a section titled "Terms and Conditions" with the following text:

Welcome to Rentapp!

These terms and conditions outline the rules and regulations for the use of Rentapp's Website, located at localhost:9001/rentapp.

By accessing this website we assume you accept these terms and conditions. Do not continue to use Rentapp if you do not agree to take all of the terms and conditions stated on this page.

The following terminology applies to these Terms and Conditions, Privacy Statement and Disclaimer Notice and all Agreements: "Client", "You" and "Your" refers to you, the person log on this website and compliant to the Company's terms and conditions. "The Company", "Ourselves", "We", "Our" and "Us", refers to our Company. "Party", "Parties", or "Us", refers to both the Client and ourselves. All terms refer to the offer, acceptance and consideration of payment necessary to undertake the process of our assistance to the Client in the most appropriate manner for the express purpose of meeting the Client's needs in respect of provision of the Company's stated services, in accordance with and subject to, prevailing law of Netherlands. Any use of the above terminology or other words in the singular, plural, capitalization and/or he/she or they, are taken as interchangeable and therefore as referring to same.

## Disclaimer

To the maximum extent permitted by applicable law, we exclude all representations, warranties and conditions relating to our website and the use of this website. Nothing in this disclaimer will:

limit or exclude our or your liability for death or personal injury;  
limit or exclude our or your liability for fraud or fraudulent misrepresentation;

limit any of our or your liabilities in any way that is not permitted under applicable law; or

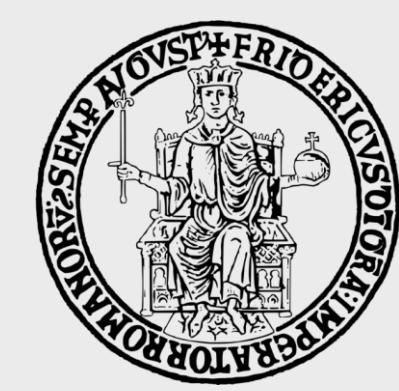
exclude any of our or your liabilities that may not be excluded under applicable law.

The limitations and prohibitions of liability set in this Section and elsewhere in this disclaimer: (a) are subject to the preceding paragraph; and (b) govern all liabilities arising under the disclaimer, including liabilities arising in contract, in tort and for breach of statutory duty.

As long as the website and the information and services on the website are provided free of charge, we will not be liable for any loss or damage of any nature.

Accept

Decline

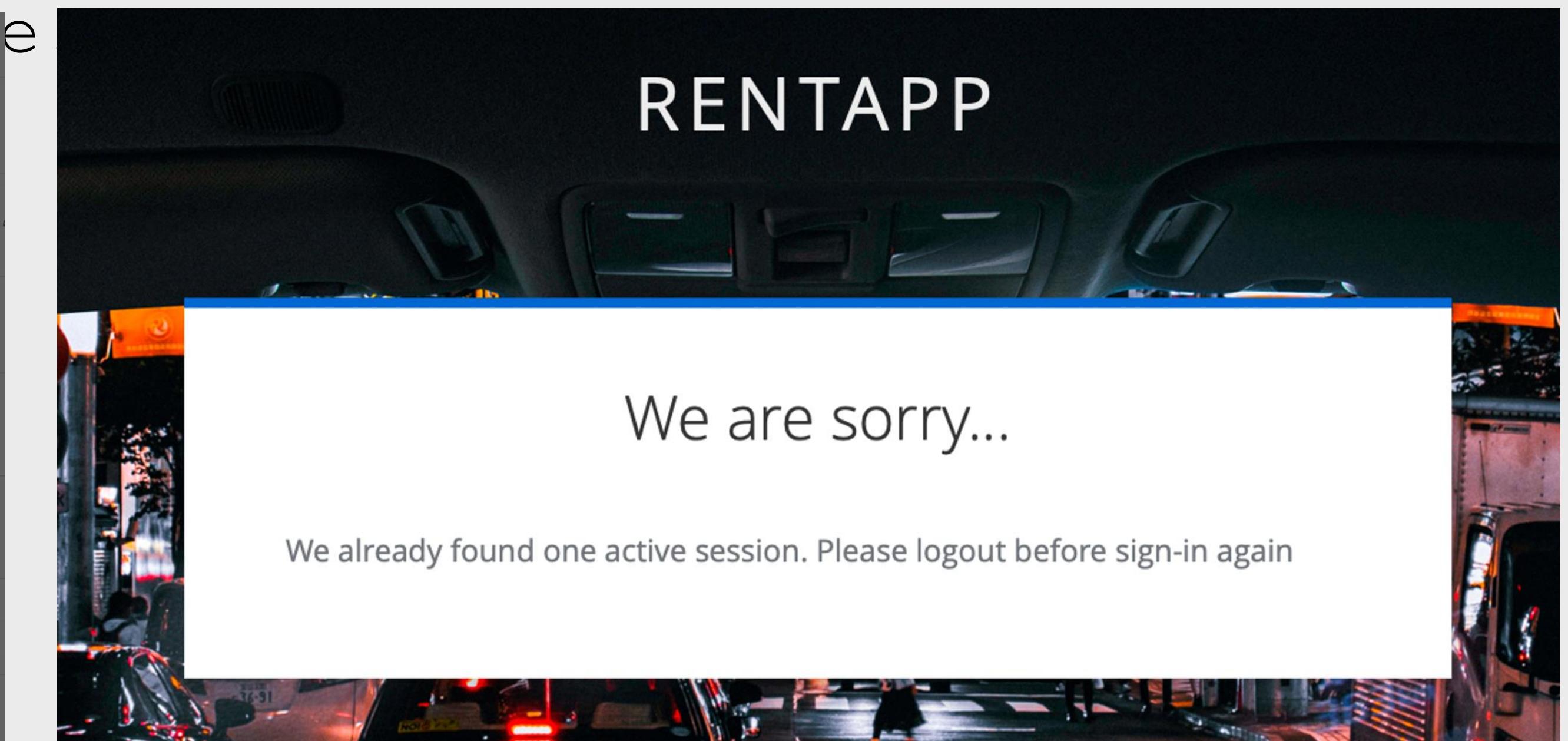


# AC-10: CONCURRENT SESSION CONTROL

Imporre un limite sul numero massimo di sessioni correnti/contemporanee per ogni utente a un numero predefinito dall'organizzazione.

Il numero di sessioni correnti massime per ogni utente è stato impostato ad un limite massimo di una. Per l'implementazione di questo limite è stato ridefinito il flow di autenticazione tramite browser aggiungendo un subflow nel processo che effettua il

The screenshot shows the 'User session count limiter config' dialog box. It includes fields for 'Alias' (set to 'Massimo una sessione attiva'), 'Maximum concurrent sessions for each user within this realm' (set to '1'), 'Maximum concurrent sessions for each user per keycloak client' (set to '0'), and 'Behavior when user session limit is exceeded' (set to 'Deny new session'). There is also an 'Optional custom error message' field containing the text: 'We already found one active session. Please logout before sign-in again...'. At the bottom are 'Save', 'Cancel', and 'Clear' buttons.





# AC-12 : SESSION TERMINATION

Far terminare automaticamente una sessione utente dopo il verificarsi di una condizione stabilita o dell'innesto di un evento che richiede la disconnessione della sessione

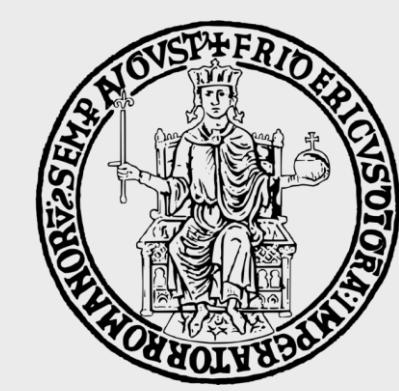
Il sistema è stato settato per terminare le sessioni attive automaticamente:

- ° Dopo 30 minuti di inattività (SSO Session Idle) .
- ° Per sessioni lunghe più di 10 ore (SSO Session Max) .
- ° Il Remember Me non è previsto.

**SSO Session Settings**

|                           |                                 |                                  |                                  |         |                                  |
|---------------------------|---------------------------------|----------------------------------|----------------------------------|---------|----------------------------------|
| <b>SSO Session Idle</b> ⓘ | <input type="text" value="30"/> | <input type="button" value="▼"/> | <input type="button" value="▲"/> | Minutes | <input type="button" value="▼"/> |
| <b>SSO Session Max</b> ⓘ  | <input type="text" value="10"/> | <input type="button" value="▼"/> | <input type="button" value="▲"/> | Hours   | <input type="button" value="▼"/> |

|                         |                                |                                  |                                  |         |                                  |
|-------------------------|--------------------------------|----------------------------------|----------------------------------|---------|----------------------------------|
| <b>SSO Session Idle</b> | <input type="text" value="0"/> | <input type="button" value="▼"/> | <input type="button" value="▲"/> | Minutes | <input type="button" value="▼"/> |
| <b>SSO Session Max</b>  | <input type="text" value="0"/> | <input type="button" value="▼"/> | <input type="button" value="▲"/> | Minutes | <input type="button" value="▼"/> |



# AC-12 : SESSION TERMINATION

Il tempo di vita dell'access token è impostato a 5 minuti, dopodiché bisognerà ripetere il processo di login da capo.

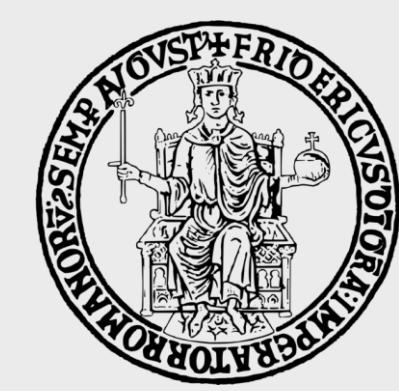
Il processo di login da parte del client deve essere concluso in 1 minuto altrimenti il token viene invalidato e il login dovrà essere ripetuto da capo.

**Access tokens**

**Access Token Lifespan**  Minutes ? It is recommended for this value to be shorter than the SSO session idle timeout: 30 minutes

**Access Token Lifespan For Implicit Flow**  Minutes ?

**Client Login Timeout**  Minutes ?

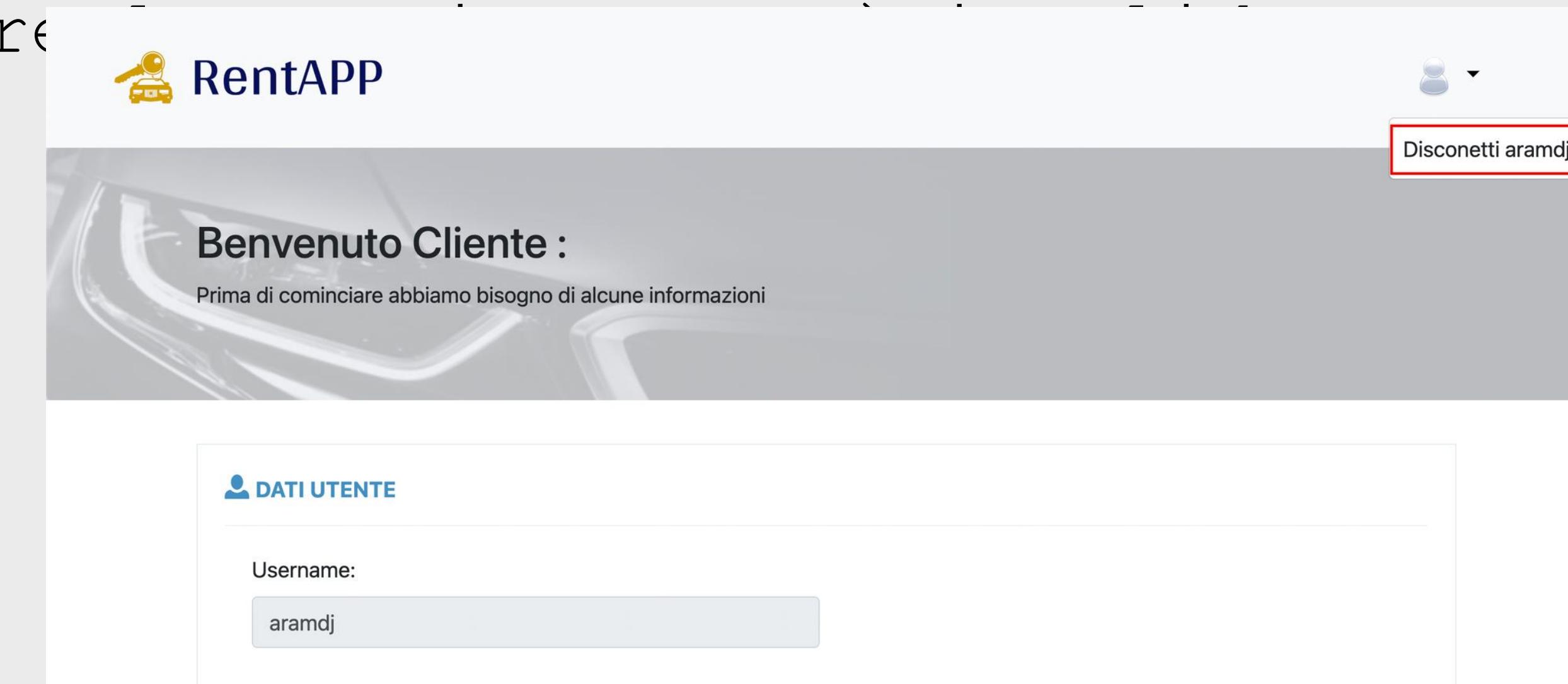


# AC-12: CONTROL ENHANCEMENTS

AC-12 (1) : Fornire la possibilità di effettuare il log-out per una sessione utente già iniziata anche quando l'autenticazione è usata per ottenere il controllo alle risorse informative dell'organizzazione.

È stato reso disponibile all'utente la possibilità di effettuare il log-out dalla propria dashboard.

L'html button sarà gestito dal controller che provvederà a costruire il corretto url da invocare per effettuare il logout su Keycloak. Inoltre

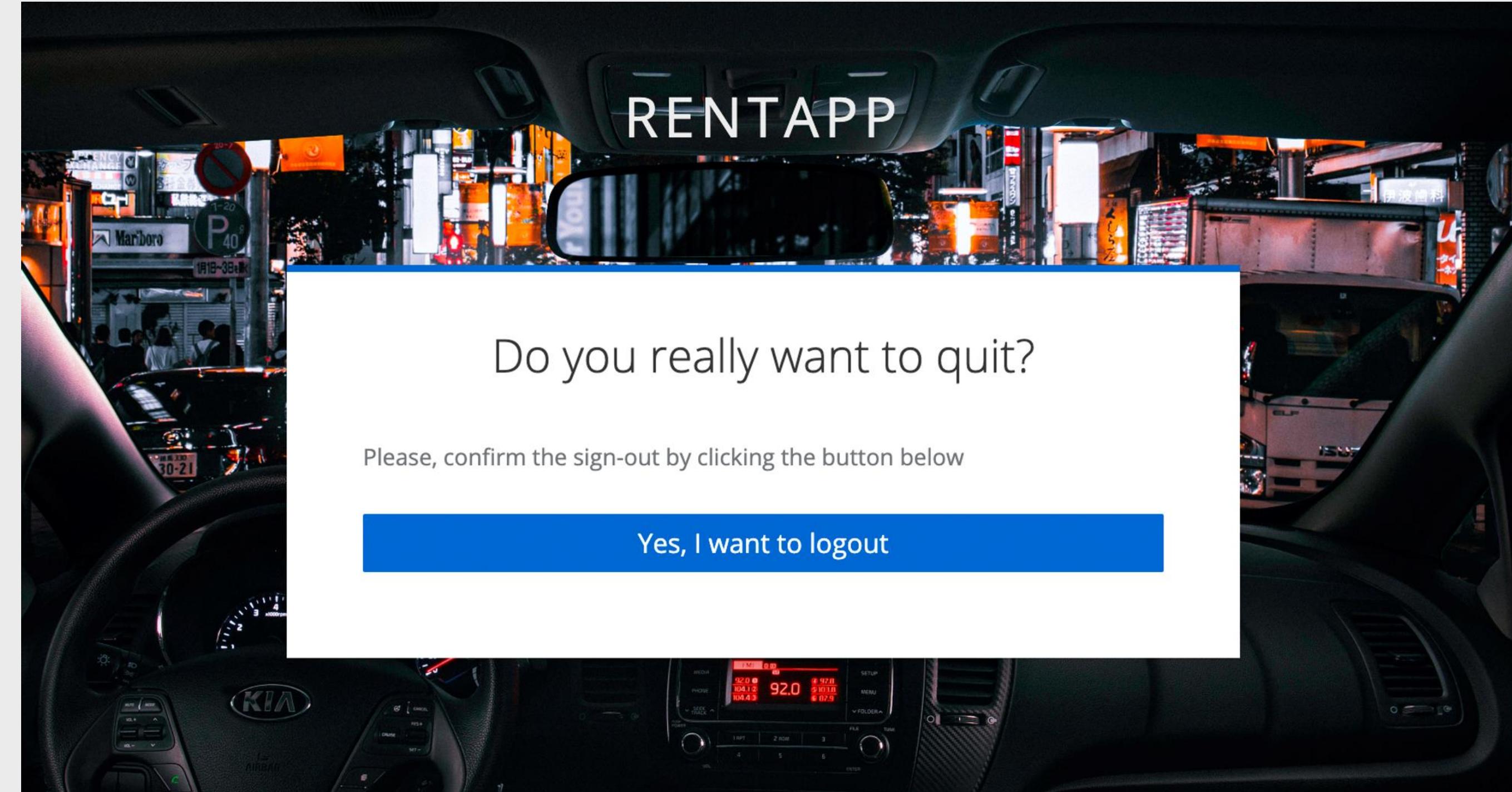


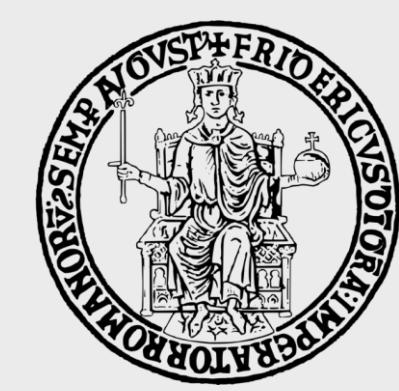


# AC-12: CONTROL ENHANCEMENTS

AC-12(2) : Mostrare un messaggio esplicito di log-out agli utenti, indicando la terminazione della sessione di comunicazione autenticata.

Keycloak chiederà all'utente di confermare l'operazione di log-out.

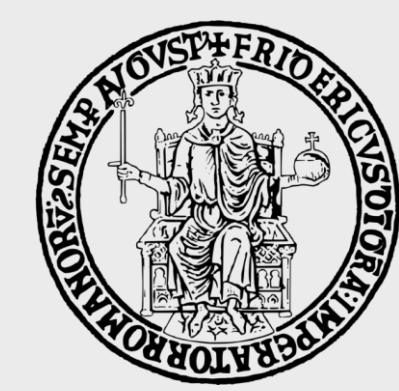




# AC-12: CONTROL ENHANCEMENTS

Keycloak dopo aver effettuato il log-out, e quindi dopo aver invalidato la sessione, effettuerà il redirect ad una pagina di estensione .jsp che notificherà all'utente che il log-out è avvenuto correttamente.

The screenshot shows a web page for 'RentAPP'. At the top left is the logo, which includes a small icon of a car and the text 'RentAPP'. The main content area has a large, semi-transparent background image of a car's front end. Overlaid on this image is the text 'Log out avvenuto con successo!' in bold black font. Below this text is a green rectangular button with the white text 'Torna alla Homepage!'. At the bottom left of the page, there is some small, faint text: '© 2021 by aVerySadProject. Termini & Condizioni Chi Siamo'.



# AC-17: REMOTE ACCESS

- a) Stabilire le restrizioni di utilizzo e i requisiti di connessione per ogni tipologia di accesso remoto consentita.
- b) Autorizzare ogni topologia di accesso remoto al sistema prima di consentire la connessione.

L'applicazione consente agli utenti di accedere al server tramite una connessione HTTPS garantendo segretezza e autenticità della comunicazione tra il sistema e l'utilizzatore .  
Il sistema di autorizzazione si interpone tra tutti i servizi fruibili e in tutte le richieste di accesso remoto garantendone l'accesso esclusivo.



# AC-17: CONTROL ENHANCEMENTS

AC-17(1) : impiegare meccanismi automatici per osservare e tenere sotto controllo i metodi d'accesso remoto.

Il sistema di monitoring automatico fornito dall'admin console di Keycloak permette di tracciare e di notificare eventuali tentativi di azioni illegali commesse da un accesso remoto. Inoltre le attività di accesso sono registrate dai logger dei microservizi del sistema.

AC-17(2) : implementare meccanismi crittografici per garantire la confidenzialità e l'integrità delle sessioni ad accesso remoto.

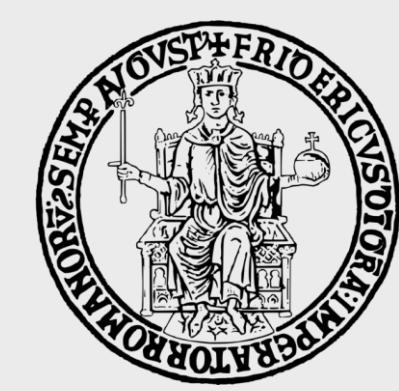
Tutte i flussi di informazione dall'applicazione e verso quest'ultima viaggiano tramite HTTPS sfruttando il protocollo TLS che protegge i dati con la crittografia al fine di garantire



# AC-17: CONTROL ENHANCEMENTS

AC-17(3) : Instradare gli accessi remoti tramite punti di controllo autorizzati della rete di accesso

Le richieste ai micro servizi della rete interna privata vengono instradate da tomcat che prevede quale di questi ultimi invocare.



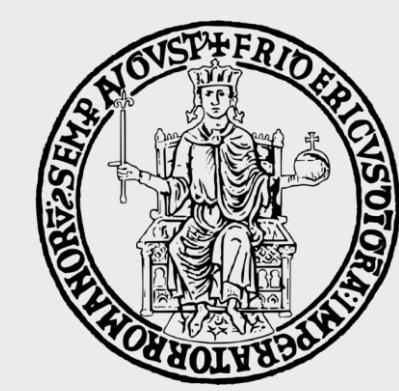
# AC-20 : USE OF EXTERNAL SYSTEMS

Stabilire, identificare con fiducia le relazioni stabilite con altre organizzazioni che possiedono operano o mantengono con sistemi esterni autorizzandoli a :

- a) Accedere al sistema tramite sistemi esterni
- b) Processare, conservare o trasmettere le informazioni controllate utilizzando sistemi esterni
- c) Proibire l'uso di alcuni tipi di sistemi esterni

I sistemi esterni all'intero dell'applicazione sono :

- Il server SMTP utilizzato da Keycloak "Mailjet". Quest'ultimo si occupa della gestione dell'invio delle email per conto di Keycloak stesso. La configurazione del servizio avviene dalla dashboard di keycloak nella quale andranno specificati:
  - l'indirizzo del server SMTP
  - la porta dedicata al servizio
  - il protocollo di comunicazione con il server SMTP
  - username e password per usufruire del servizio

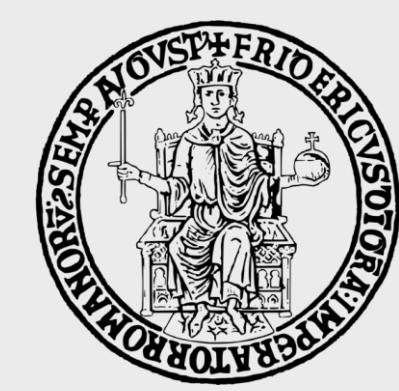


# AC-20 : USE OF EXTERNAL SYSTEMS

## Connection & Authentication

|                       |  |
|-----------------------|--|
| <b>Host *</b>         | in-v3.mailjet.com  |
| <b>Port</b>           | 587  |
| <b>Encryption</b>     | <input type="checkbox"/> Enable SSL<br><input checked="" type="checkbox"/> Enable StartTLS |
| <b>Authentication</b> | <input checked="" type="button"/> Enabled  |
| <b>Username *</b>     | 75a26f820187c089834089fa3c9ae54f   |
| <b>Password *</b> ⓘ   | ..... <input type="button"/>   |

- il servizio G-Auth che si occupa dell'autenticazione federata al sistema.
- il servizio Facebook Auth che si occupa dell'autenticazione federata al sistema.



# AC : CONCLUSIONI

Utilizzando come metrica di paragone il **"Moderate Security Baseline"** per il calcolo del livello di impatto sulla sicurezza, in base ai controlli effettuati, avremmo un livello di sicurezza **'Moderate'**.

| No.   | Control Name   | Low-Impact | Moderate-Impact                  | High-Impact                                | Privacy Control Baseline |
|-------|--|------------|----------------------------------|--|--------------------------|
| AC-1  | POLICY AND PROCEDURES                                      | AC-1       | AC-1                             | AC-1                                       | AC-1                     |
| AC-2  | ACCOUNT MANAGEMENT   | AC-2       | AC-2 (1) (2) (3) (4)<br>(5) (13) | AC-2 (1) (2) (3) (4) (5)<br>(11) (12) (13) |                          |
| AC-3  | ACCESS ENFORCEMENT   | AC-3       | AC-3                             | AC-3                                       | AC-3 (14)                |
| AC-4  | INFORMATION FLOW ENFORCEMENT                               |            | AC-4                             | AC-4 (4)                                   |                          |
| AC-5  | SEPARATION OF DUTIES                                       |            | AC-5                             | AC-5                                       |                          |
| AC-6  | LEAST PRIVILEGE  |            | AC-6 (1) (2) (5) (7)<br>(9) (10) | AC-6 (1) (2) (3) (5) (7)<br>(9) (10)       |                          |
| AC-7  | UNSUCCESSFUL LOGON ATTEMPTS                                | AC-7       | AC-7                             | AC-7                                       |                          |
| AC-8  | SYSTEM USE NOTIFICATION                                    | AC-8       | AC-8                             | AC-8                                       |                          |
| AC-11 | DEVICE LOCK  |            | AC-11 (1)                        | AC-11 (1)                                  |                          |
| AC-12 | SESSION TERMINATION  |            | AC-12                            | AC-12                                      |                          |
| AC-14 | PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION | AC-14      | AC-14                            | AC-14                                      |                          |
| AC-17 | REMOTE ACCESS  | AC-17      | AC-17 (1) (2) (3) (4)            | AC-17 (1) (2) (3) (4)                      |                          |
| AC-18 | WIRELESS ACCESS  | AC-18      | AC-18 (1) (3)                    | AC-18 (1) (3) (4) (5)                      |                          |
| AC-19 | ACCESS CONTROL FOR MOBILE DEVICES                          | AC-19      | AC-19 (5)                        | AC-19 (5)                                  |                          |
| AC-20 | USE OF EXTERNAL SYSTEMS                                    | AC-20      | AC-20 (1) (2)                    | AC-20 (1) (2)                              |                          |
| AC-21 | INFORMATION SHARING  |            | AC-21                            | AC-21                                      |                          |
| AC-22 | PUBLICLY ACCESSIBLE CONTENT                                | AC-22      | AC-22                            | AC-22                                      |                          |

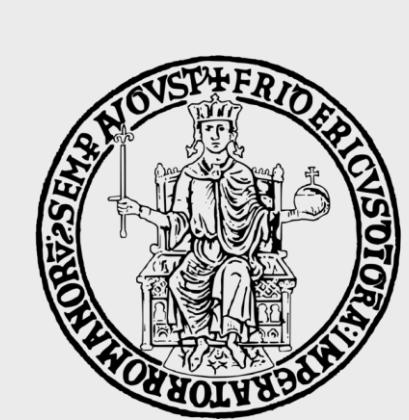


# NIST - SC: SYSTEM AND COMMUNICATIONS PROTECTION

Per System and Communications Protection si intendono i controlli che gestiscono e garantiscono la protezione dei sistemi e delle comunicazioni con e fra quest'ultimi.

Di seguito la trattazione dei controlli:

SC-2 (1), SC-7 (3), SC-8 (1) (3), SC-10, SC-12, SC-13, SC-17, SC-18, SC-23, SC-28, SC-39.



# SC-2 : SEPARATION OF SYSTEM AND USER FUNCTIONALITY

Il sistema separa la funzionalità fruibili all'utente (tra cui l'interfaccia dedicata a quest'ultimo) dalle funzionalità di gestione del sistema stesso.

Il sistema separa le funzioni e le interfacce appartenenti agli utenti dalle funzionalità di gestione del database dedicate all'amministratore di sistema.

La gestione dell'IAM è affidata all'amministratore di sicurezza.



# SC-2: CONTROL ENHANCEMENTS

SC-2 (1) : Prevenire che agli utenti non privilegiati vengano presentate interfacce di funzionalità per la gestione del sistema.

È previsto da Keycloak l'utilizzo di due schermate di accesso differenti a seconda se si voglia accedere alla dashboard di amministrazione del servizio oppure si voglia accedere alle funzionalità offerte dalla web-app. Infatti:

- L'amministratore di sistema per modificare il realm accederà alle funzionalità offerte da Keycloak tramite <http://localhost:8080/auth>.
- L'utente che vuole accedere al sistema invece accederà alla login page del sistema direttamente dalla web-app.

In nessun caso all'utente del sistema verrà mostrata la finestra di accesso alla dashboard di gestione dell'TAM.



# SC-7: BOUNDARY PROTECTION

- a) Monitorare e controllare le comunicazioni con le interfacce di gestione esterne al sistema e le principali interfacce all'interno del sistema.
- b) Implementare sottoreti per l'accesso alle componenti pubbliche del sistema che sono fisicamente o logicamente separate dalle reti interne.
- c) Connessione alle reti esterne o sistemi solo attraverso interfacce gestite da dispositivi di protezione perimetrale organizzati in un'architettura di sicurezza

I micro servizi che costituiscono l'applicazione si trovano all'interno di una rete privata realizzata con docker compose. Le connessioni in entrata sono connesse solo tramite la porta 9001 mappata successivamente sulla 8443 per l'HTTPS.

Il perimetro di sicurezza contiene al suo interno il webserver tomcat, l'applicazione rentapp, il server di keycloak, Hashicorp Vault e l'SQL server sul quale è presente il database.



# SC-7: CONTROL ENHANCEMENTS

SC-7 (3) : Limitare il numero di connessioni di rete ad un punto di ingresso del sistema

L'utente esterno che desidera collegarsi avrà come punto d'accesso il webserver tomcat che comunica con quest'ultimo tramite HTTPS ed è l'unico servizio esposto della sottorete.



# SC-8 : TRANSMISSION CONFIDENTIALITY AND INTEGRITY

Proteggere la confidenzialità e l'integrità delle informazioni trasmesse

L'integrità e la confidenzialità delle informazioni trasmesse sono garantite grazie all'utilizzo del protocollo HTTPS che consente il trasferimento dei dati tramite un canale TLS crittografato



# SC-8: CONTROL ENHANCEMENTS

SC-8 (1) : Implementare meccanismi crittografici per prevenire la divulgazione di informazioni e per rilevare modifiche delle informazioni durante la trasmissione

TLS garantisce che questo controllo venga applicato preservando l'integrità e la confidenzialità delle informazioni

SC-8 (3) : Implementare meccanismi crittografici per proteggere i messaggi esterni a meno che non siano protetti diversamente da controlli fisici.

L'abilitazione della comunicazione TLS per la comunicazione con il server SMTP garantisce l'integrità e la confidenzialità delle comunicazioni che avvengono con quest'ultimo. La comunicazione è configurata e viene

|                |  |
|----------------|--|
| Port           | 587  |
| Encryption     | <input type="checkbox"/> Enable SSL<br><input checked="" type="checkbox"/> Enable StartTLS |
| Authentication | <input type="button" value="Enabled"/>   |



# SC-10 : NETWORK DISCONNECT

Il sistema termina la connessione di rete associata ad una sessione di comunicazione al termine della sessione o dopo un periodo di inattività.

La terminazione di una connessione comporta la de-allocazione di porte e indirizzi TCP/IP a livello di sistema e di collegamenti di rete nel caso in cui ci siano molteplici sessioni che utilizzano la stessa connessione.

A generare la disconnessione possono essere un periodo di inattività prestabilito dall'organizzazione o la richiesta esplicita di log-out da parte dell'utente.

Si rimanda alla famiglia di controlli AC per le policy.



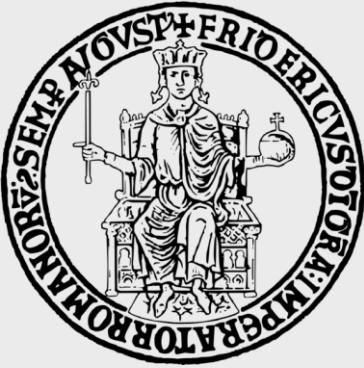
# SC-12: CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

L'organizzazione stabilisce e gestisce le chiavi crittografiche per la crittografia richiesta impiegata all'interno del sistema secondo i requisiti di generazione di chiavi, di distribuzione, di conservazione e di distruzione di queste ultime.

Le chiavi crittografiche utilizzano come algoritmo RSA. Essendo l'applicazione ospitata e in locale e quindi non presentando un dominio di rete gestito da un DNS, si è optato per l'utilizzo di certificati self-signed con store type PKCS12 a validità di un anno.

La connessione HTTPS al server è stata configurata all'interno del file server.xml di apache tomcat, dove è stato abilitato un connettore che permette l'utilizzo di tale protocollo sulla porta 8443.

Inoltre ogni tentativo di apertura di una connessione HTTP verrà



# SC-13 : CRYPTOGRAPHIC PROTECTION

- a) Determina i meccanismi di crittografia utilizzati.
- b) Implementa i tipi di crittografia richiesti per ogni uso crittografico richiesto dall'organizzazione

Viene utilizzato RSA per la generazione della coppia di chiavi pubblica e privata utilizzate nel protocollo HTTPS.

Le password dell'utente vengono immagazzinate assieme ad dati d'accesso in un database separato rispetto a quello dell'applicazione a gestito solo da keycloak: keycloak non memorizza le password come testo semplice ma come testo hash, utilizzando l'algoritmo di hashing PBKDF2.

Keycloak esegue 27.500 iterazioni di hashing, ovvero il numero di iterazioni consigliato dalla comunità della sicurezza.

Questo numero di iterazioni di hashing può influire negativamente sulle prestazioni poiché l'hashing PBKDF2 utilizza una quantità



# SC-13 : CRYPTOGRAPHIC PROTECTION

Inoltre, keycloak è stato configurato per supportare l'OTP: di default quest'ultimo viene generato con algoritmo SHA1 ma può essere configurato anche per lavorare con SHA256 e SHA512 che risultano più sicuri ma richiedono maggiore potenza di calcolo. Per la configurazione dell'OTP è stato optato per un algoritmo SHA256 time based che genera codici a 6 cifre validi per finestre temporali di 30 secondi.

Keycloak di default utilizza l'algoritmo di cifratura RSA256 per firmare i token per il realm scambiati con il client, quest'ultimo può essere facilmente modificato dalle impostazioni.

Inoltre la procedura di Unsealing di Vault Sfrutta l'algoritmo SHA e gli e

General

on funz

|                    |   |
|--------------------|---|
| Default Signature  | RS256   |
| Algorithm          | SHA256  |
| OTP type           | <input checked="" type="radio"/> Time based <input type="radio"/> Counter based |
| OTP hash algorithm | SHA256  |
| Number of digits   | <input checked="" type="radio"/> 6 <input type="radio"/> 8                      |
| Look ahead window  | - 1 +   |
| OTP Token period   | 30 Seconds  |



# SC-17 : PUBLIC KEY INFRASTRUCTURE CERTIFICATES

- a) Rilasciare un certificato a chiave pubblica con una policy certificata o ottieni i certificati a chiave pubblica da un fornitore approvato
- b) Includi solo gli “anchors” fidati o certificati salvati dall’organizzazione

La connessione SSL viene certificata tramite un certificato self-signed presente nei trust-store all’interno dell’applicazione. Questi ultimi sono protetti da password. Per quanto riguarda i certificati forniti dall’esterno, questi sono gestiti da fornitori approvati.



# SC-18 : MOBILE CODE

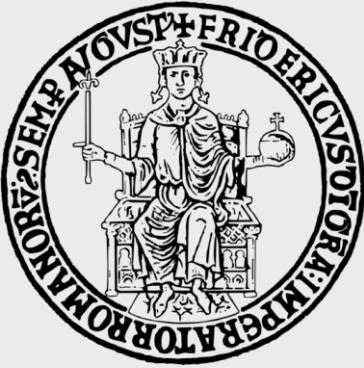
Bisogna definire il codice mobile accettabile, inaccettabile e le tecnologie utilizzate da quest'ultimo.

Definire le restrizioni sull'uso e le linee guida per l'implementazione di codice mobile accettabile.

Autorizzare, monitorare e controllare l'uso del codice mobile all'interno del sistema

Il codice mobile è trasmesso ed eseguito sul browser utilizzato, la sanificazione degli input avviene tramite le funzioni della libreria Java Validation Constraints. Le query al database MSSQL utilizzate dall'applicazione inoltre sono state sviluppate utilizzando i criteria builder di JPA messi a disposizione per Hibernate che limitano la possibilità di attacchi SQL injection.

Infatti questi come ad esempio HQL e JPQL evitano l'utilizzo di quei parametri che potrebbero portare all'esecuzione di codice malevolo iniettato da un malintenzionato.



# SC-23 : SESSION AUTHENTICITY

Proteggere l'autenticità delle comunicazioni di sessione

L'autenticità della sessione viene garantita tramite l'utilizzo dell HTTPS.

L'utilizzo di Keycloak consente di avere un meccanismo che nel momento di una corretta autenticazione genera un token di identità e un token di accesso firmato dal realm e contenente tutte le informazioni di accesso.

Open ID Connect consente di autenticare client in modi diversi per ricevere i token tramite l'utilizzo di un codice temporaneo che evita gli attacchi di tipo replay.

La durata degli access token è breve (5 minuti) alla scadenza questi vengono rigenerati tramite un refresh token che salva l'applicazione da attacchi di tipo Man In The Middle.



# SC-28 : PROTECTION OF INFORMATION AT REST

Proteggere l'integrità e la riservatezza delle informazioni degli utenti e del sistema scelte dall'organizzazione

Le informazioni degli utenti vengono salvate nel database interno di keycloak, mentre i dati necessari al funzionamento dell'applicazione vengono salvati nel database SQL.

In ogni caso vengono garantite riservatezza e integrità secondo i meccanismi di accesso ai dati illustrati precedentemente.

La configurazione di Vault permette di salvare le credenziali di accesso al DB.

Siccome Vault non è accessibile dall'esterno è garantita la riservatezza delle informazioni che esso custodisce.



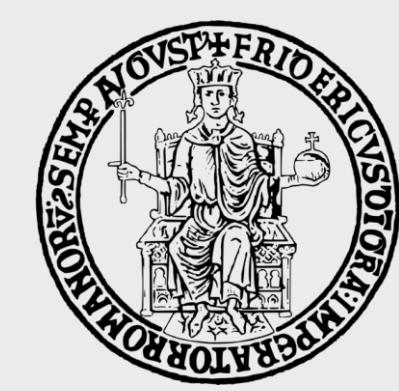
# SC-39 : PROCESS ISOLATION

Il sistema mantiene dei domini di esecuzione separati per ogni processo.

L'utilizzo di Docker Compose ha permesso di gestire tutti i servizi tramite l'utilizzo dei containers.

A livello di filesystem ogni container risulta completamente isolato dal sistema sottostante e da quello degli altri containers.

La stessa cosa vale a livello di rete dove i demoni, come ad esempio quello di tomcat per l'HTTP vengono "blindati" all'interno dello stesso container e ognuno di essi risulta avere il proprio indirizzo IP associato.



# SC : CONCLUSIONI

Utilizzando come metrica di paragone il **"Moderate Security Baseline"** per il calcolo del livello di impatto sulla sicurezza, in base ai controlli effettuati, avremmo un livello di sicurezza **'Low'**.

| No.   | Control Name   | Low-Impact | Moderate-Impact             | High-Impact                              | Privacy Control Baseline |
|-------|--|------------|-----------------------------|--|--------------------------|
| SC-1  | POLICY AND PROCEDURES  | SC-1       | SC-1                        | SC-1                                     |                          |
| SC-2  | SEPARATION OF SYSTEM AND USER FUNCTIONALITY                            |            | SC-2                        | SC-2                                     |                          |
| SC-3  | SECURITY FUNCTION ISOLATION  |            |                             | SC-3                                     |                          |
| SC-4  | INFORMATION IN SHARED SYSTEM RESOURCES                                 |            | SC-4                        | SC-4                                     |                          |
| SC-5  | DENIAL-OF-SERVICE PROTECTION   | SC-5       | SC-5                        | SC-5                                     |                          |
| SC-7  | BOUNDARY PROTECTION  | SC-7       | SC-7 (3) (4) (5) (7)<br>(8) | SC-7 (3) (4)<br>(5) (7) (8) (18)<br>(21) | SC-7 (24)                |
| SC-8  | TRANSMISSION CONFIDENTIALITY AND INTEGRITY                             |            | SC-8 (1)                    | SC-8 (1)                                 |                          |
| SC-10 | NETWORK DISCONNECT   |            | SC-10                       | SC-10                                    |                          |
| SC-12 | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT                         | SC-12      | SC-12                       | SC-12 (1)                                |                          |
| SC-13 | CRYPTOGRAPHIC PROTECTION   | SC-13      | SC-13                       | SC-13                                    |                          |
| SC-15 | COLLABORATIVE COMPUTING DEVICES AND APPLICATIONS                       | SC-15      | SC-15                       | SC-15                                    |                          |
| SC-17 | PUBLIC KEY INFRASTRUCTURE CERTIFICATES                                 |            | SC-17                       | SC-17                                    |                          |
| SC-18 | MOBILE CODE  |            | SC-18                       | SC-18                                    |                          |
| SC-20 | SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)          | SC-20      | SC-20                       | SC-20                                    |                          |
| SC-21 | SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | SC-21      | SC-21                       | SC-21                                    |                          |
| SC-22 | ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE      | SC-22      | SC-22                       | SC-22                                    |                          |
| SC-23 | SESSION AUTHENTICITY   |            | SC-23                       | SC-23                                    |                          |
| SC-24 | FAIL IN KNOWN STATE  |            |                             | SC-24                                    |                          |
| SC-28 | PROTECTION OF INFORMATION AT REST                                      |            | SC-28 (1)                   | SC-28 (1)                                |                          |
| SC-39 | PROCESS ISOLATION  | SC-39      | SC-39                       | SC-39                                    |                          |



# NIST - IA: IDENTIFICATION AND AUTHENTICATION

Per Identification and Authentication si intendono i controlli che regolano il processo relativo a stabilire l'identità di un'entità che interagisce con un sistema.

Di seguito la trattazione dei controlli:

IA-2 (1) (2) (8), IA-3, IA-4, IA-5(1) (6), IA-6, IA-7, IA-11, IA-12(2) (3) (5).



# IA-2 : IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Identificare e autenticare univocamente gli utenti ai processi che agiscono per conto di questi utenti

L'identificazione e l'autenticazione degli utenti all'interno del sistema viene gestita tramite l'IAM Keycloak, utilizzando il protocollo OIDC.

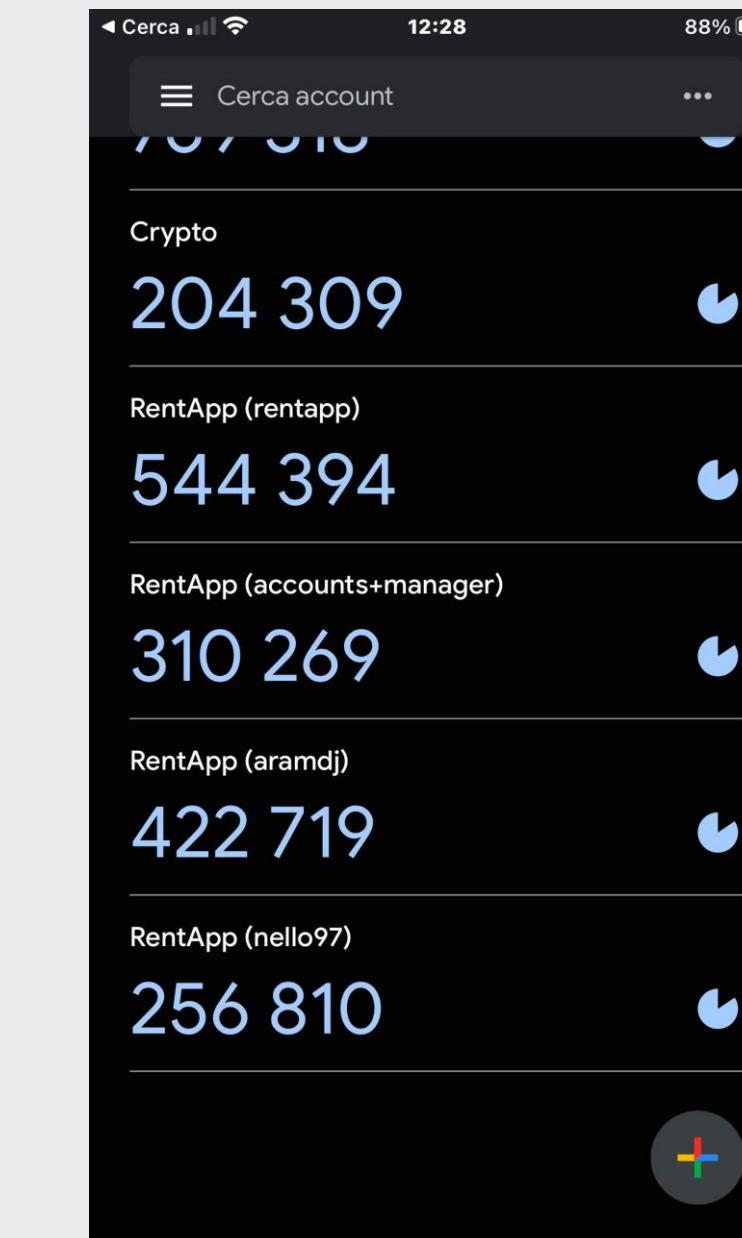
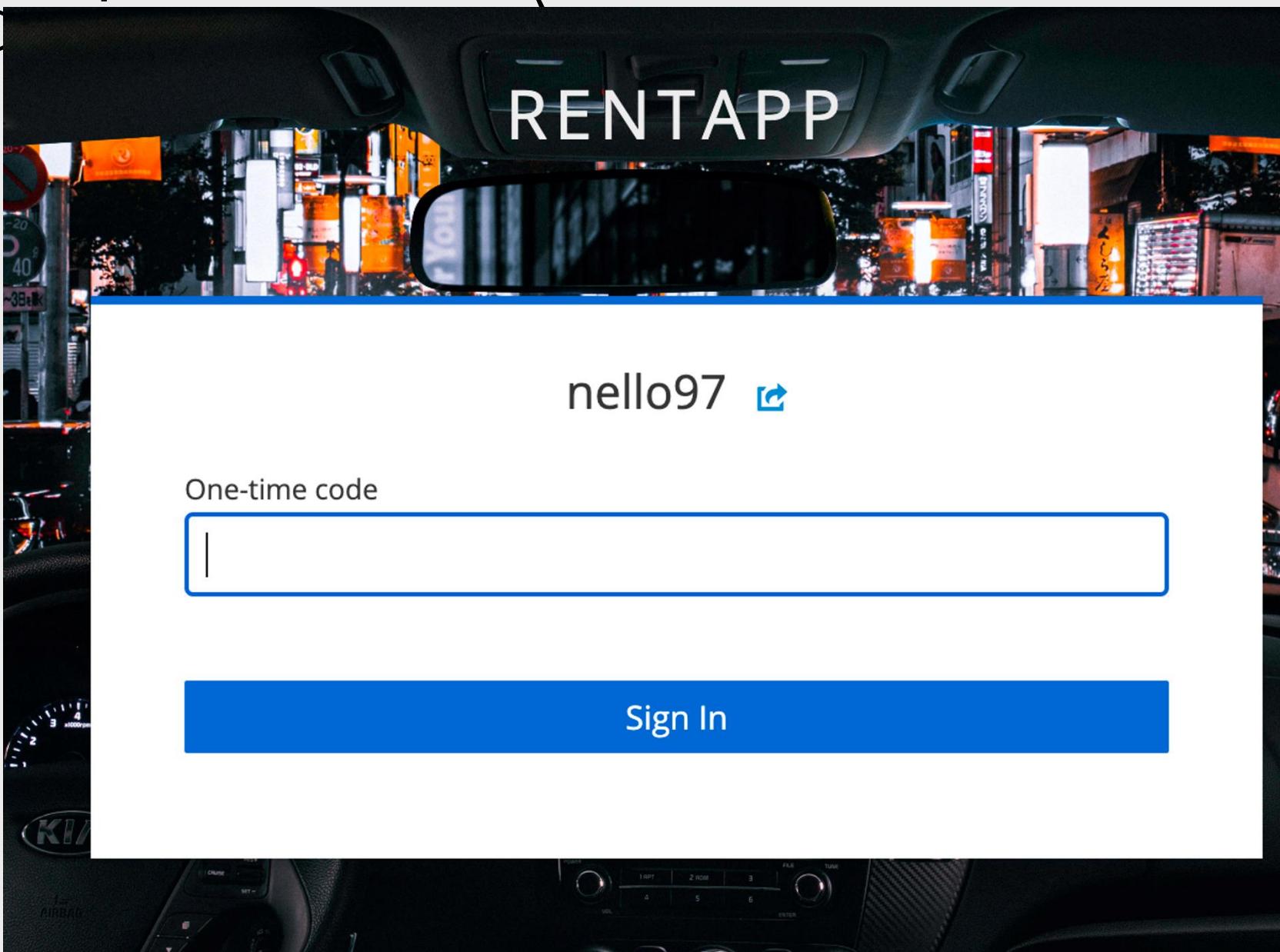
Gli utenti vengono identificati univocamente tramite credenziali di accesso personali.

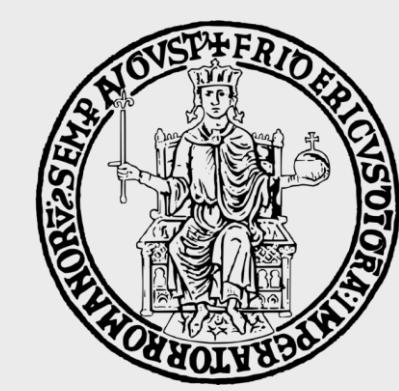


# IA-2: CONTROL ENHANCEMENTS

IA-2(1)(2) : Implementare un'autenticazione multifattoriale per gli account privilegiati e non

Tramite keycloak è implementata l'autenticazione a due fattori che prevede la generazione di un codice OTP a 6 cifre tramite l'utilizzo di un'app scelta dall'utente (Google Authenticator, OneLogin).





# IA-2: CONTROL ENHANCEMENTS

L'applicazione verrà configurata scansionando il codice QR mostrato nell'interfaccia di sign-up durante il primo log-in. Tramite il codice QR, verrà condivisa con l'applicazione la chiave di generazione dell'OTP utilizzata dall'algoritmo SHA256.

OTP Check

**⚠ You need to set up Mobile Authenticator to activate your account.**

1. Install one of the following applications on your mobile:  
Google Authenticator  
One Login Protect  
FreeOTP(Only Android System)  
2FA Authenticator (2FAS)
2. Open the application and scan the barcode:

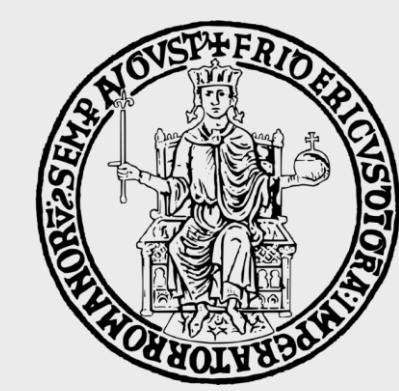
  
[Unable to scan?](#)

3. Enter the one-time code provided by the application and click Submit to finish the setup.

Provide a Device Name to help you manage your OTP devices.

**One-time code \***

**Device Name**



# IA-2: CONTROL ENHANCEMENTS

IA-2(8) : Implementare un meccanismo di protezione per gli attacchi di tipo replay

Il processo di autenticazione avviene tramite gli standard OAuth2.0 e OpenIDConnect, che funzionano tramite il protocollo challenge/response che li rende non vulnerabili agli attacchi di tipo replay a causa dell'utilizzo di nonces e token temporanei. OpenID Connect infatti scambia il nonce, che sarà valido esclusivamente una volta, con keycloak che rilascerà il token di sessione e di autorizzazione a validità singola. In aggiunta l'impiego del protocollo TLS prevede un ulteriore utilizzo dei nonces.



# IA-3 : DEVICE IDENTIFICATION AND AUTHENTICATION

Identificare e autenticare unicamente i dispositivi definiti prima di creare una connessione

Tramite l'impiego di keycloak è possibile monitorare le sessioni utente e quindi gli utenti autenticati e vedere gli indirizzi IP associati al momento della connessione. L'associazione permette di rendersi conto quando un account, associato ad un particolare token di sessione, utilizzo un indirizzo IP differente da quello con cui ha stabilito la connessione. Cio facilita eventuali operazioni di : sessions associate a un singolo account.

| Sessions         |                         |                         |            |                | Action |
|------------------|-------------------------|-------------------------|------------|----------------|--------|
| User             | Started                 | Last access             | IP address | Clients        |        |
| nello97          | 12/21/2022, 12:39:26 PM | 12/21/2022, 12:39:26 PM | 172.21.0.1 | rentapp_client | ⋮      |
| aramdj           | 12/21/2022, 12:39:44 PM | 12/21/2022, 12:39:44 PM | 172.21.0.1 | rentapp_client | ⋮      |
| rentapp          | 12/21/2022, 12:40:08 PM | 12/21/2022, 12:40:08 PM | 172.21.0.1 | rentapp_client | ⋮      |
| accounts manager | 12/21/2022, 12:40:39 PM | 12/21/2022, 12:40:39 PM | 172.21.0.1 | rentapp_client | ⋮      |



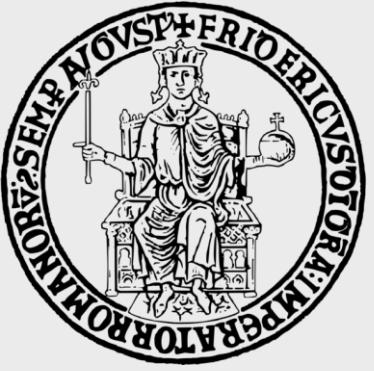
# IA-4 : IDENTIFIER MANAGEMENT

Gestire gli identificatori del sistema :

- a) Ricevendo l'autorizzazione dai ruoli definiti dell'organizzazione e assegnando un identificatore individuale di gruppo, ruolo, servizio o dispositivo
- b) Selezionare un identificatore che identifichi un individuo, gruppo, ruolo, servizio o dispositivo
- c) Assegnare l'identificatore all'individuo, gruppo, ruolo, servizio o dispositivo
- d) Impedire il riutilizzo degli identificatori per periodi stabiliti dall'organizzazione

All'atto della registrazione ad ogni account utente viene associato il proprio username che deve essere univoco.

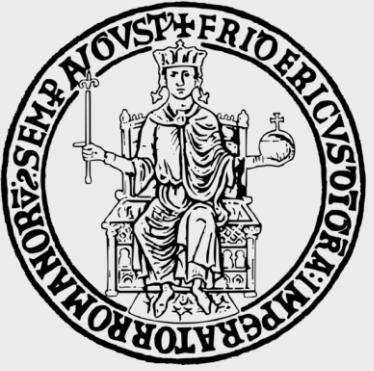
Anche l'email costituisce un tipo di identificativo univoco, e il meccanismo di conferma di quest'ultima risulta a supporto della sua unicità.



# IA-5 : AUTHENTICATOR MANAGEMENT

Gestire gli autenticatori di sistema :

- a) Stabilire il contenuto iniziale dell'autenticatore per tutti gli autenticatori emessi dall'organizzazione
- b) Garantire che gli autenticatori dispongano delle risorse sufficienti per l'uso previsto
- c) Stabilire e attuare procedure amministrative per la distribuzione iniziale dell'autenticatore, per gli autenticatori persi, compromessi o danneggiati e per la revoca degli autenticatori
- d) Modifica degli autenticatori predefiniti prima del primo utilizzo
- e) Modifica o aggiornamento degli autenticatori dopo un periodo definito dall'organizzazione o quando si verifica un evento definito dall'organizzazione
- f) Proteggere il contenuto dell'autenticatore da divulgazione e modifica non autorizzate
- g) Richiedere alle persone di adottare, e far sì che i dispositivi implementino, controlli specifici per proteggere gli autenticatori
- h) Modifica degli autenticatori per gli account di gruppo o di ruolo



# IA-5 : AUTHENTICATOR MANAGEMENT

Il sistema impone alcune regole in fase di generazione della password al fine di garantire un livello di protezione adeguato.

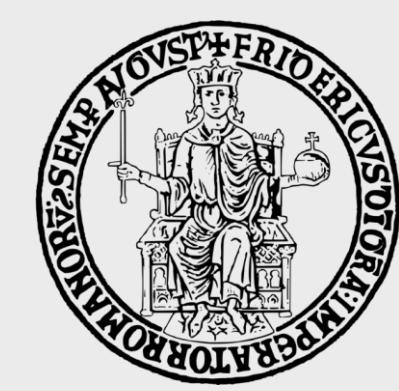
L'applicazione gestisce il caso in cui l'utente perda la password.



# IA-5: CONTROL ENHANCEMENTS

IA-5(1) : Definizione di regole per la corretta creazione, trasmissione e archiviazione delle password utilizzate

- Le policy di creazione della password prevedono:
  - Minimo 8 caratteri
  - La password non può essere la propria email
  - La password non può essere il proprio username
  - La password deve contenere almeno un carattere speciale
  - La password deve contenere almeno un carattere minuscolo
  - La password deve contenere almeno un carattere maiuscolo
  - La password deve contenere almeno un carattere numerico
  - La password scade ogni 365 giorni
  - La password viene processata con l'algoritmo pbkdf2-SHA256 e vengono effettuate 27500 iterazioni
  - Non può essere scelta una password precedente
  - C'è una blacklist delle password più comunemente utilizzate che l'utente non potrà scegliere, aggiornata secondo le 100.000 password più



# IA-5: CONTROL ENHANCEMENTS

Password policy    OTP Policy    Webauthn Policy    Webauthn Passwordless Policy

Add policy

Minimum Length \* ⓘ  - +

Not Username \* ⓘ  On

Not Email \* ⓘ  On

Special Characters \* ⓘ  - +

Lowercase Characters \* ⓘ  - +

Uppercase Characters \* ⓘ  - +

Digits \* ⓘ  - +

Expire Password \* ⓘ

Hashing Iterations \* ⓘ  - +

Not Recently Used \* ⓘ  - +

Hashing Algorithm \* ⓘ

Password Blacklist \* ⓘ



# IA-5: CONTROL ENHANCEMENTS

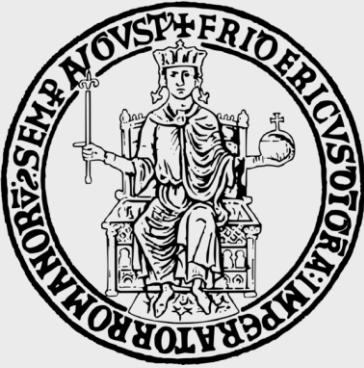
IA-5(6) : Proteggere gli autenticatori in base alla categoria di sicurezza delle informazioni a cui l'autenticazione permette l'accesso

Il controllo è soddisfatto da keycloak che prevede una comunicazione sicura e una memorizzazione affidabile delle password.

Al momento dell'autenticazione, il browser indirizza l'utente al server di keycloak dove verranno inserite le credenziali.

L'utente risulta quindi completamente isolato dall'applicazione che non ha bisogno di sapere le credenziali di keycloak quali le password, i codici OTP o le chiavi pubbliche WebAuth.

Le informazioni gestite da keycloak sono crittografate con l'algoritmo Password-Based Key Derivation Function 2 e custodite nel database di keycloak



# IA-6 : AUTHENTICATION FEEDBACK

Oscurare il feedback delle credenziali di autenticazione durante il processo di autenticazione al fine di proteggere l'informazione da individui non autorizzate

L'inserimento nel form di login delle credenziali sensibili come la password sono mascherati dai punti neri. Nel caso di inserimento errato, non viene restituita nessuna informazione riguardo i dati errati che sono stati inseriti, ma esclusivamente che i dati inseriti

orretti.

Sign in to your account

Username or email  
nello97

Password  
.....

Remember me      [Forgot Password?](#)

[Sign In](#)

Or sign in with

Google

Facebook

New user? [Register](#)

Sign in to your account

Username or email  
hello97 !

Invalid username or password.

Password  
.....

Remember me      [Forgot Password?](#)

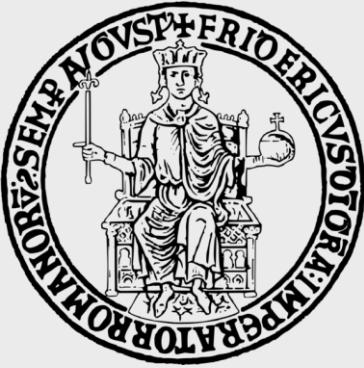
[Sign In](#)



# IA-7 : CRYPTOGRAPHIC MODULE AUTHENTICATION

Implementare meccanismi per l'autenticazione ad un modulo crittografico che soddisfino i requisiti delle leggi, degli ordini esecutivi, delle direttive, dei criteri, dei regolamenti, degli standard e delle linee guida applicabili per tale autenticazione.

Le comunicazioni per il processo di identificazione e autentificazione avvengono tramite HTTPS, quindi tutti i dati vengono crittografati secondo gli standard TLS.



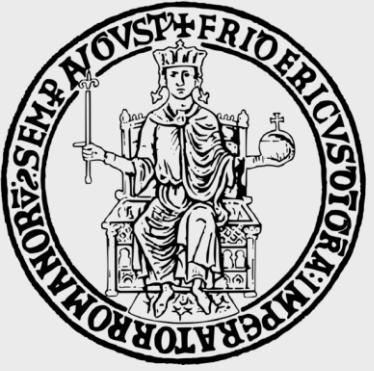
# IA-11 : RE-AUTHENTICATION

Richiedi agli utenti di eseguire nuovamente l'autenticazione in corrispondenza di determinati eventi.

L'utente resta autenticato anche all'atto della chiusura e successiva riapertura del browser, purché la sessione utente non rimanga inattiva per più di 30 minuti, in tal caso verrà chiesto all'utente di rieffettuare il login.

Inoltre verrà chiesto all'utente di rieffettuare il login al sistema se la sessione corrente ha una lifetime pari a 10 ore. La richiesta di autenticazione da parte del sistema verrà riproposta all'utente in

|                           |    |         |
|---------------------------|----|---------|
| <b>SSO Session Idle</b> ⓘ | 30 | Minutes |
| <b>SSO Session Max</b> ⓘ  | 10 | Hours   |

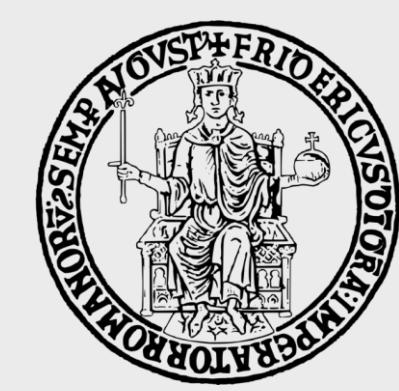


# IA-12 : IDENTITY PROOFING

- a) Gli utenti dimostrano la loro identità che è richiesta per l'accesso logico ai sistemi in base a requisiti di livello di garanzia dell'identità appropriati come specificato negli standard e nelle guide linea.
- b) Associare un utente ad un individuo univoco

Ad ogni account utente è associata un'unica identità dell'individuo che lo utilizza.

La prova d'identità è costituita dall'email che viene verificata.



# IA-12: CONTROL ENHANCEMENTS

IA-12 (2) (3): Richiedere che la prova dell'identificazione individuale sia presentata e convalidata all'autorità di registrazione.

Un account di tipo 'gestore', per essere attivato deve fare richiesta esplicita tramite email al servizio clienti 'rentappssd@gmail.com', che per verificare l'identità del gestore e la proprietà di un autonoleggio fisico potrà richiedere ulteriori dati personali con la relativa documentazione per attestarne la veridicità.

L'utente di tipo 'cliente' per accedere al servizio dovrà fornire numero di patente, partita iva e codice fiscale che lo identificano univocamente come individuo e che in caso di azioni sospette potrà essere richiesto da l'account manager una verifica dei dati forniti tramite prove da inviare via email.



# IA-12: CONTROL ENHANCEMENTS

IA-12 (5) : Richiedi che un codice di conferma registrazione venga consegnato attraverso un canale fuori banda per verificare l'indirizzo (fisico o digitale) registrato dagli utenti.

All'atto della registrazione verrà inviato all'utente via email un link per verificare che l'indirizzo email fornito in fase di registrazione sia valido.

The screenshot shows an email inbox with one message from "Rentapp". The subject of the email is "Verify email" and it includes the text "Posta in arrivo". The message body contains a message from "Rentapp" dated "19 dic" to "a me". It states: "Someone has created a account with this email address. If this was you, click the link below to verify your email address". Below this is a blue link "Link to e-mail address verification". The message continues: "This link will expire within 5 minutes." and "If you didn't create this account, just ignore this message." There are standard email controls like a star icon, a reply arrow, and a more options menu.

Verify email Posta in arrivo

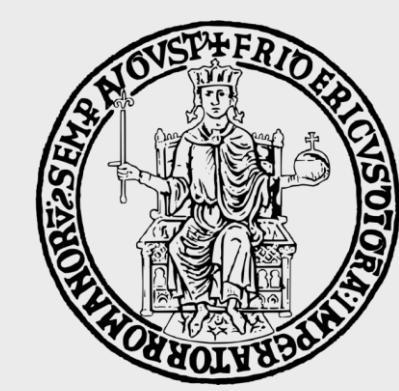
Rentapp 19 dic  
a me

Someone has created a account with this email address. If this was you, click the link below to verify your email address

[Link to e-mail address verification](#)

This link will expire within 5 minutes.

If you didn't create this account, just ignore this message.



# IA: CONCLUSIONI

Utilizzando come metrica di paragone il **"Moderate Security Baseline"** per il calcolo del livello di impatto sulla sicurezza, in base ai controlli effettuati, avremmo un livello di sicurezza **'Moderate'**.

| No.   | Control Name   | Low-Impact            | Moderate-Impact       | High-Impact               | Privacy Control Baseline |
|-------|--|-----------------------|-----------------------|---------------------------|--------------------------|
| IA-1  | POLICY AND PROCEDURES  | IA-1                  | IA-1                  | IA-1                      |                          |
| IA-2  | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)     | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (8) (12) | IA-2 (1) (2) (5) (8) (12) |                          |
| IA-3  | DEVICE IDENTIFICATION AND AUTHENTICATION                     |                       | IA-3                  | IA-3                      |                          |
| IA-4  | IDENTIFIER MANAGEMENT  | IA-4                  | IA-4 (4)              | IA-4 (4)                  |                          |
| IA-5  | AUTHENTICATOR MANAGEMENT                                     | IA-5 (1)              | IA-5 (1) (2) (6)      | IA-5 (1) (2) (6)          |                          |
| IA-6  | AUTHENTICATION FEEDBACK                                      | IA-6                  | IA-6                  | IA-6                      |                          |
| IA-7  | CRYPTOGRAPHIC MODULE AUTHENTICATION                          | IA-7                  | IA-7                  | IA-7                      |                          |
| IA-8  | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | IA-8 (1) (2) (4)      | IA-8 (1) (2) (4)      | IA-8 (1) (2) (4)          |                          |
| IA-11 | RE-AUTHENTICATION  | IA-11                 | IA-11                 | IA-11                     |                          |
| IA-12 | IDENTITY PROOFING  |                       | IA-12 (2) (3) (5)     | IA-12 (2) (3) (4) (5)     |                          |