

BANDIUNINA

Secure Systems Design

Alfonso Conte M63001378

Daniele Fazzari M63001384

Vittorio De Iasio M63001388



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

BANDIUNINA

Si tratta di una **web-app** che permette la gestione completamente online di **bandi di concorso** dedicati a studenti dell'*Università Federico II di Napoli*.

Uno **studente** regolarmente iscritto all'ateneo, difatti, potrà registrarsi ed accedere al servizio, visualizzare i **bandi di concorso** attualmente attivi e, tramite un semplice *click*, inoltrare la propria candidatura ad essi. Successivamente potrà monitorare lo stato delle partecipazioni inoltrate, gestite dal rispettivo **operatore** responsabile.



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II

INDICE

1. Specifica dei **requisiti**
2. Design **architetturale e deploy**
3. Web-app **functional demo**
4. **Tecnologie** utilizzate
5. **Threat analysis and assessment**
6. “**Access Control**” Control Family
7. “**Audit And Accountability**” Control Family
8. “**Identification and Authentication**” Control Family
9. “**System and communication protection**” Control Family

1. SPECIFICA DEI REQUISITI

UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II



FUNCTIONAL REQUIREMENTS

- Uno **studente** deve poter anzitutto **registrarsi** al servizio web, utilizzando informazioni personali (come Nome e Cognome) ed informazioni istituzionali (come Matricola ed email istituzionale).
- Uno **studente** registrato deve poter effettuare **l'accesso** all'applicativo web. Dopo averlo effettuato, deve poter **visualizzare** tutti i bandi di ateneo attualmente attivi, i quali avranno informazioni essenziali come un titolo ed una descrizione (che permetteranno allo studente di selezionare il bando corretto) ed un collegamento ipertestuale alla relativa documentazione ufficiale.
- Lo **studente** deve dunque poter inoltrare la propria **candidatura** ai bandi di concorso, la quale può essere **monitorata** in seguito. Difatti, una **partecipazione** può avere esito positivo (se lo studente è risultato tra i **vincitori** del bando) o esito negativo, e lo studente ne deve poter conoscere l'esito.
- Un **supervisore** deve poter registrarsi alla piattaforma utilizzando informazioni personali (come Nome e Cognome) ed informazioni istituzionali (come un Badge Number). Una volta che il suo account verrà **validato** dall'admin della piattaforma, esso deve poter accedervi ed iniziare a caricare bandi di concorso di ateneo.
- Un **supervisore** deve poter visualizzare la lista dei bandi di concorso di cui è **responsabile**, senza che questa contenga quella relativa ad altri responsabili. Inoltre, deve poter visualizzare le partecipazioni relative ad un bando specifico (con tutte le informazioni personali dello studente necessarie alla valutazione della partecipazione stessa) e deve avere la possibilità di **approvare** o **declinare** la partecipazione dei singoli studenti.
- L'**admin** della piattaforma deve poter visualizzare tutti gli utenti registrati e deve poter **abilitarne** o **disabilitarne** l'account

OVERVIEW SECURITY REQUIREMENTS

- **Confidentiality** (Riservatezza) - Assicurare che le informazioni non siano rese disponibili o divulgiate ad individui, entità o processi non autorizzati - Misure di sicurezza: Crittografia dei dati, controlli di accesso, gestione delle autorizzazioni etc.
- **Integrity** (Integrità) - Garantire che le informazioni non siano alterate in modo non autorizzato o accidentale - Misure di sicurezza: Controllo degli accessi, firme digitali, controlli di modifica etc.
- **Availability** (Disponibilità) - Garantire che il sistema e le risorse siano disponibili (a individui, entità o processi) quando necessario ed in un tempo appropriato - Misure di sicurezza: Ridondanza, backup regolari, protezione contro DoS etc.
- **Authentication** (Autenticazione) - Verificare l'identità degli utenti che cercano di accedere al sistema - Misure di sicurezza: Password, autenticazione a due fattori, biometria.
- **Authorization** (Autorizzazione) - Definire i privilegi e i livelli di accesso di utenti (individui, entità o processi) al sistema - Misure di sicurezza: Gestione delle autorizzazioni, ruoli utente, controlli di accesso etc.
- **Accountability** (Responsabilità) - l'abilità di dare spiegazioni. Registrare le azioni compiute (da individui, entità o processi) al fine di poter ricostruire uno storico di interazioni col sistema - Misure di sicurezza: Registrazione delle attività, audit trail, attribuzione degli accessi etc.

2. DESIGN ARCHITETTURALE E DEPLOY

Le scelte architetturali e di deployment sono state fatte seguendo un approccio **security-oriented**, garantendo di raggiungere determinati security requirements già in fase di progettazione (security by design)



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II



API GATEWAY

L'utilizzo di un **API gateway**, come Nginx nel nostro caso, in un'applicazione web può offrire diversi vantaggi in termini di **sicurezza**. Ecco alcuni dei benefici più significativi di cui si può usufruire:

- **Terminazione SSL/TLS** - L'API gateway può gestire la terminazione SSL/TLS, cioè la decodifica del traffico crittografato prima che raggiunga il server di destinazione. Questo semplifica la gestione dei certificati SSL/TLS e consente di applicare politiche di sicurezza a livello di gateway, inclusi controlli come la verifica dell'integrità e l'autenticazione del client.
- **Protezione contro attacchi DDoS** - Nginx, come API gateway, può essere configurato per mitigare gli attacchi distribuiti di tipo Denial of Service (DDoS). Fornisce funzionalità di throttling e rate limiting per limitare il numero di richieste che un singolo utente o indirizzo IP può effettuare in un determinato periodo di tempo, contribuendo a prevenire il sovraccarico del server.
- **Centralizzazione** - Un API gateway può consentire il logging centralizzato delle richieste e delle risposte, semplificando il monitoraggio e la rilevazione di minacce alla sicurezza. In generale offre un punto di controllo centralizzato che migliora la visibilità e la gestibilità della web app, semplificando dunque la gestione delle politiche di sicurezza.
- **Validazione delle richieste** - Un API gateway può eseguire la validazione delle richieste in ingresso, rifiutando quelle non conformi alle specifiche dell'API (è dunque possibile ridurre il rischio di attacchi di injection filtrando e validando le richieste in ingresso)

IDENTITY AND ACCESS MANAGEMENT SYSTEM

L'utilizzo di un **Identity and Access Management (IAM) system**, come **Keycloak**, in una web app può migliorare significativamente la **sicurezza** complessiva dell'applicazione. Ecco alcuni dei benefici più significativi

- **Autenticazione centralizzata** - Keycloak fornisce un sistema centralizzato per gestire e semplificare l'autenticazione degli utenti, riducendo i rischi derivanti dalla gestione di credenziali in modo disperso nelle varie parti dell'applicazione.
- **Autorizzazione basata su ruoli** - Keycloak consente la gestione dei ruoli degli utenti, consentendo un controllo fine sulla loro autorizzazione alle risorse dell'applicazione. Ciò contribuisce a implementare il principio del privilegio minimo, garantendo che gli utenti abbiano solo i permessi di accesso necessari alle risorse di cui hanno bisogno.
- **Integrazione con standard di sicurezza** - Keycloak supporta standard di sicurezza come OAuth 2.0 e OpenID Connect, fornendo un framework robusto per l'autenticazione e l'autorizzazione. L'utilizzo di standard aperti contribuisce a garantire maggiore sicurezza oltre ad affidabilità e interoperabilità.
- **Fattori di autenticazione multipla (MFA)** - Keycloak supporta l'implementazione di autenticazione multi-fattore (questo può includere, ad esempio, l'uso di password, token temporanei, o verifiche tramite app mobile), quindi più sicura di un single factor.
- **Gestione centralizzata degli utenti e delle password** - Keycloak offre un'interfaccia di amministrazione per la gestione centralizzata degli utenti e delle loro credenziali. Ciò semplifica l'aggiunta, la modifica o la rimozione degli utenti e garantisce che le password siano memorizzate in modo sicuro mediante funzioni di hashing.
- **Auditing e registrazione** - Keycloak fornisce funzionalità di registrazione e auditing che consentono di monitorare le attività degli utenti

CONTAINERIZZAZIONE (Deploy)

I componenti della web app lato server vengono eseguiti in execution environments **containerizzati**. La containerizzazione offre diversi vantaggi dal punto di vista della **sicurezza**. Ecco alcuni dei principali benefici:

- **Isolamento dei processi** - aiuta a prevenire la contaminazione tra i processi e fornisce un ambiente più sicuro.
- **Isolamento delle risorse** - I container possono essere configurati per utilizzare risorse specifiche (CPU, memoria, rete, ecc.), limitando così l'impatto di un possibile attacco.
- **Esecuzione lightweight** - La rapidità di distribuzione e aggiornamento può contribuire a mantenere l'ambiente più sicuro, riducendo il tempo in cui le vulnerabilità sono esposte.
- **Controlli di accesso** - I container possono essere configurati con livelli di accesso granulari. Ad esempio, si possono limitare i privilegi di un container in modo che possa accedere solo a risorse specifiche o eseguire determinate azioni/funzioni. Questo offre un maggiore controllo sugli accessi e riduce la *attack surface*.
- **Scalabilità e ridondanza** - La containerizzazione facilita la scalabilità orizzontale, consentendo la distribuzione di più istanze di un'applicazione in modo dinamico in risposta alla domanda. Ciò non solo migliora le prestazioni, ma può anche aumentare la resilienza del sistema contro attacchi di tipo Denial of Service (DoS) distribuiti.

CLOUD PLATFORM (Deploy)

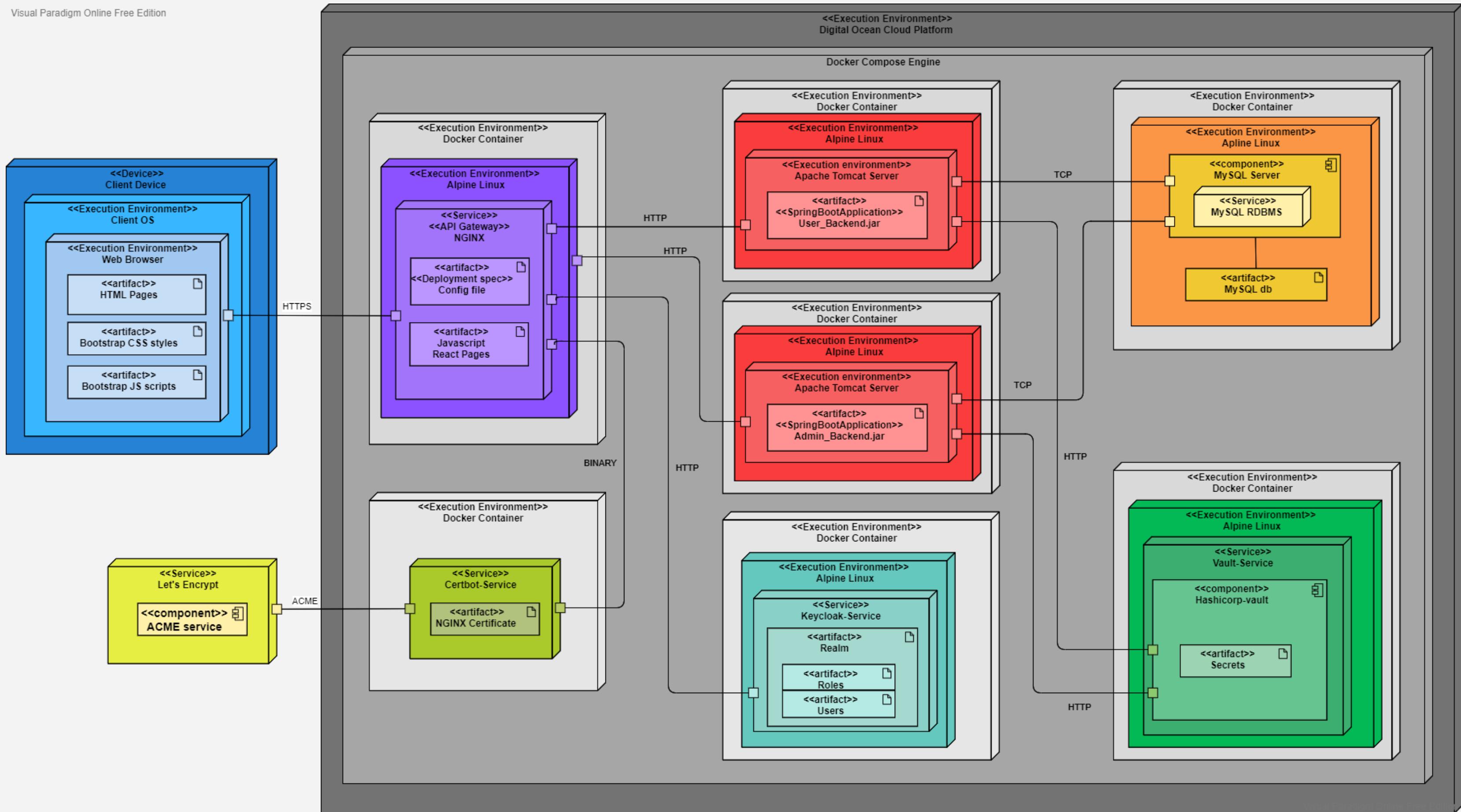
Il deploy di una web app su una **piattaforma cloud** può offrire diversi vantaggi in termini di **sicurezza**.

Alcuni di questi vantaggi includono (in generale):

- **Sicurezza fisica dei data center** - Le piattaforme cloud operano in data center altamente sicuri, con controlli di accesso fisico rigorosi, monitoraggio costante e protezione contro minacce fisiche (come incendi e alluvioni..)
- **Protezione contro attacchi DDoS** - Molte piattaforme cloud offrono servizi di mitigazione nei confronti di attacchi Distribuited Denial of Service (DDoS).
- **Audit e logging avanzati** - Le piattaforme cloud forniscono strumenti di logging e auditing avanzati, consentendo di monitorare attività sospette e raccogliere informazioni dettagliate sulle operazioni di sistema.
- **Patching e aggiornamenti automatici** - Le piattaforme cloud gestiscono spesso autonomamente gli aggiornamenti degli ambienti di esecuzione (degli OS per esempio) e delle rispettive patch di sicurezza.
- **Isolamento delle risorse** - Le piattaforme cloud forniscono ambienti di esecuzione virtualizzati che isolano le risorse di un'applicazione. Questo aiuta a prevenire che una vulnerabilità in un'app influenzi negativamente altre applicazioni o servizi nell'ambiente cloud.
- **Conformità normativa** - Molte piattaforme cloud sono certificate per varie normative di sicurezza e privacy

BANDIUNINA - DEPLOYMENT DIAGRAM

Visual Paradigm Online Free Edition

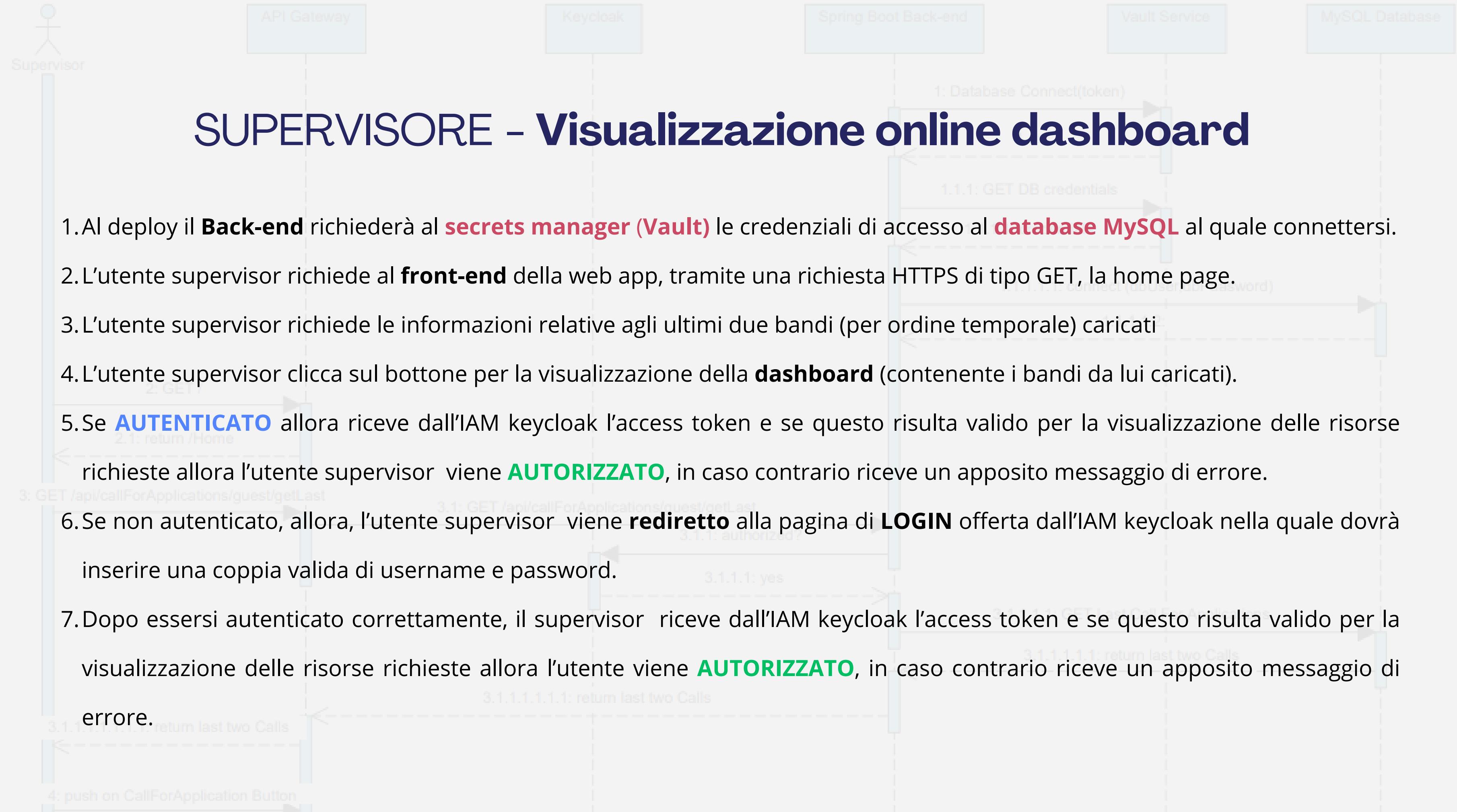


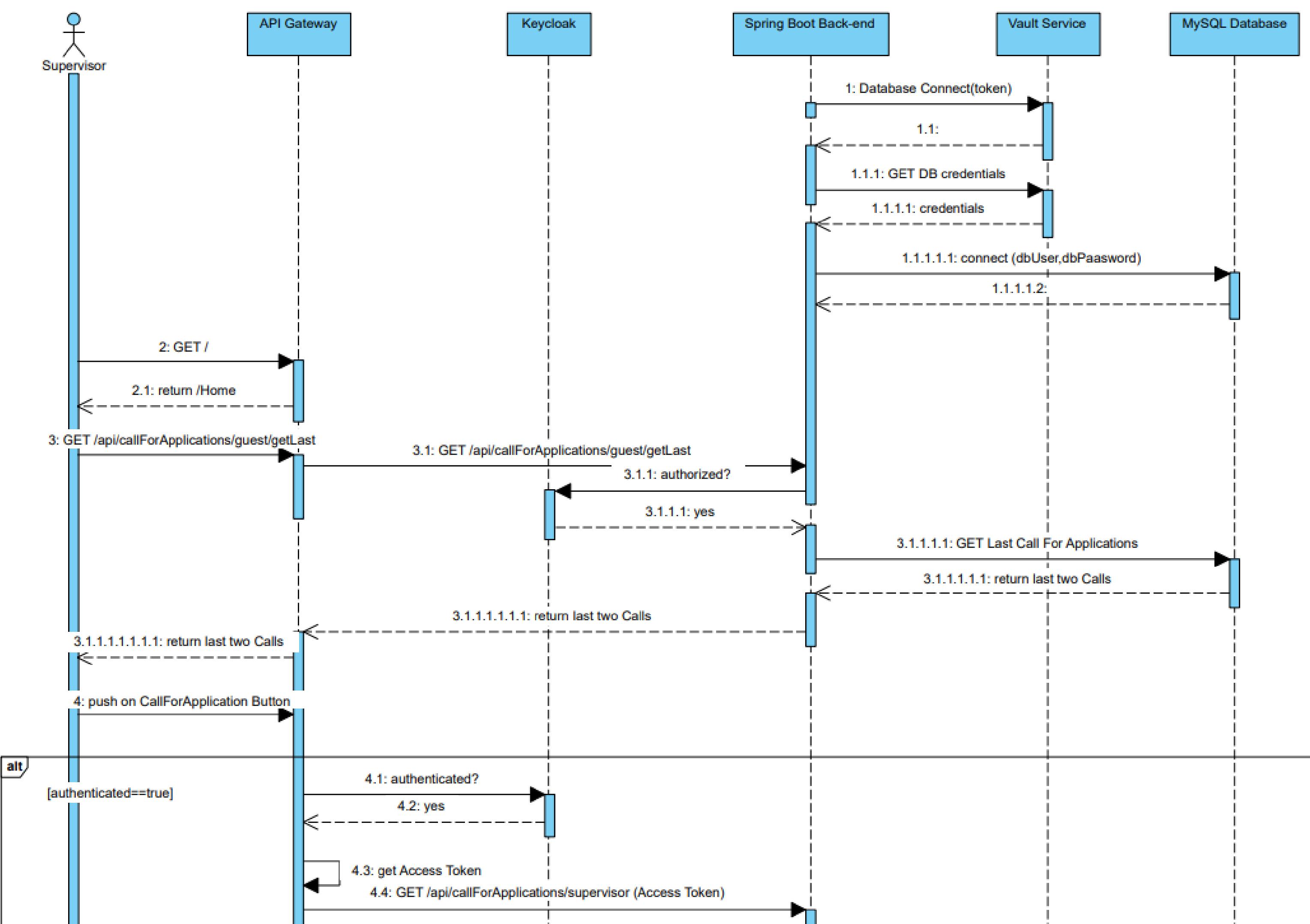
3. WEB-APP FUNCTIONAL DEMO

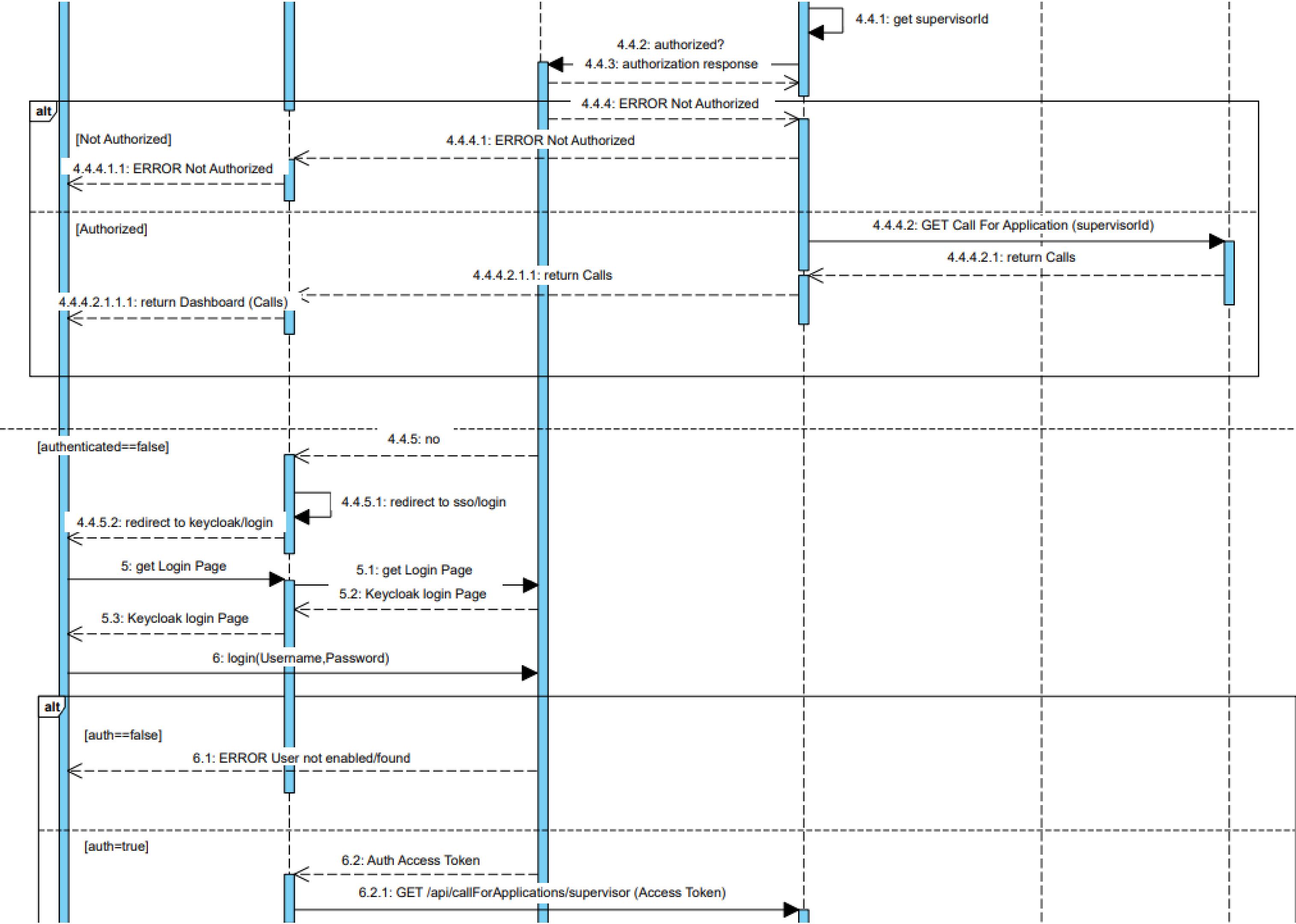


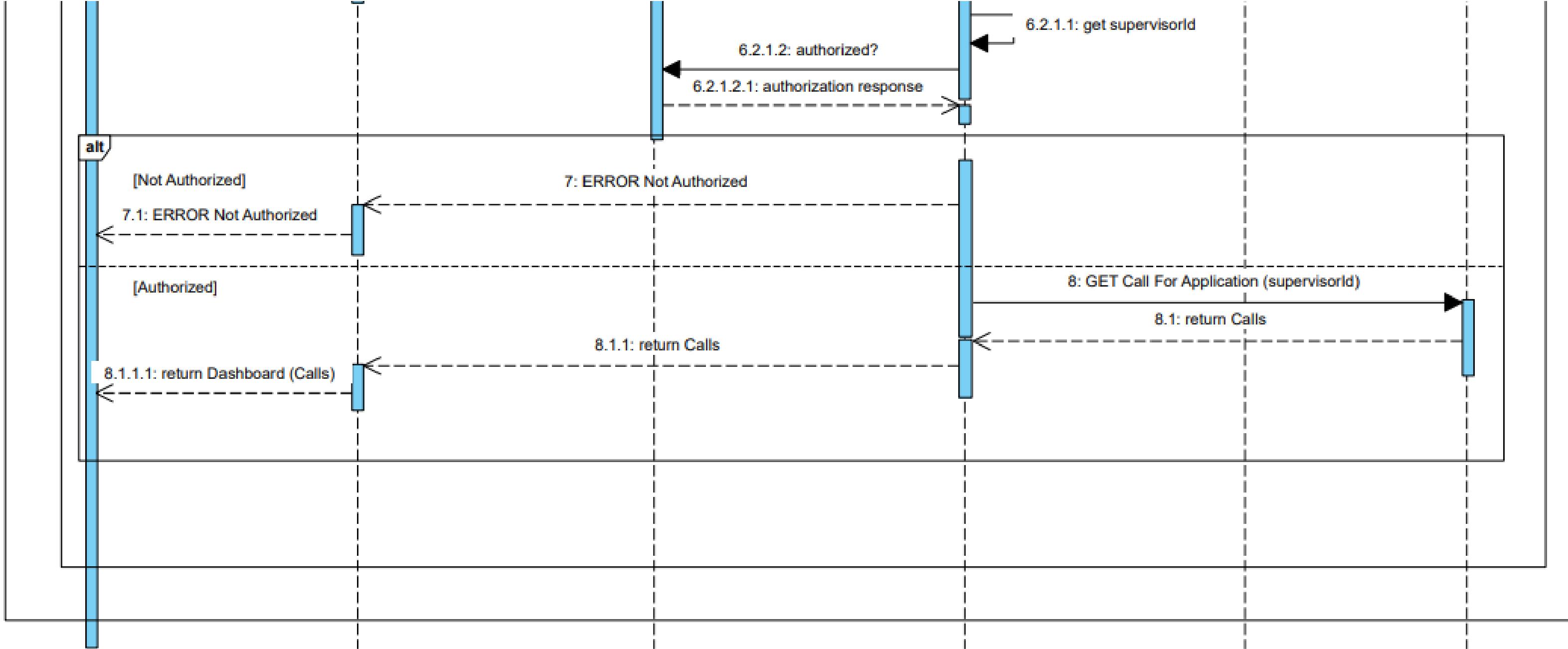
UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II







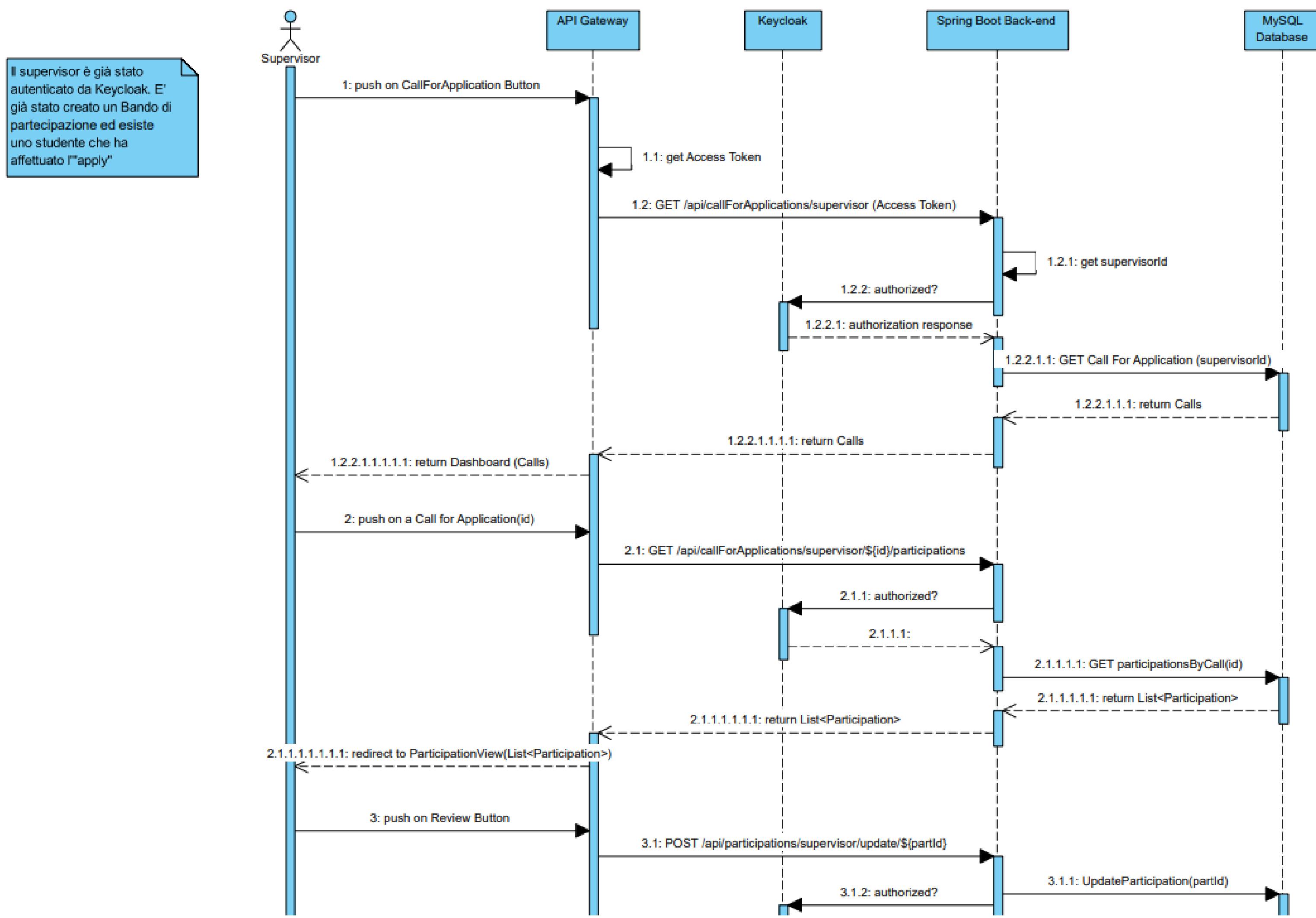


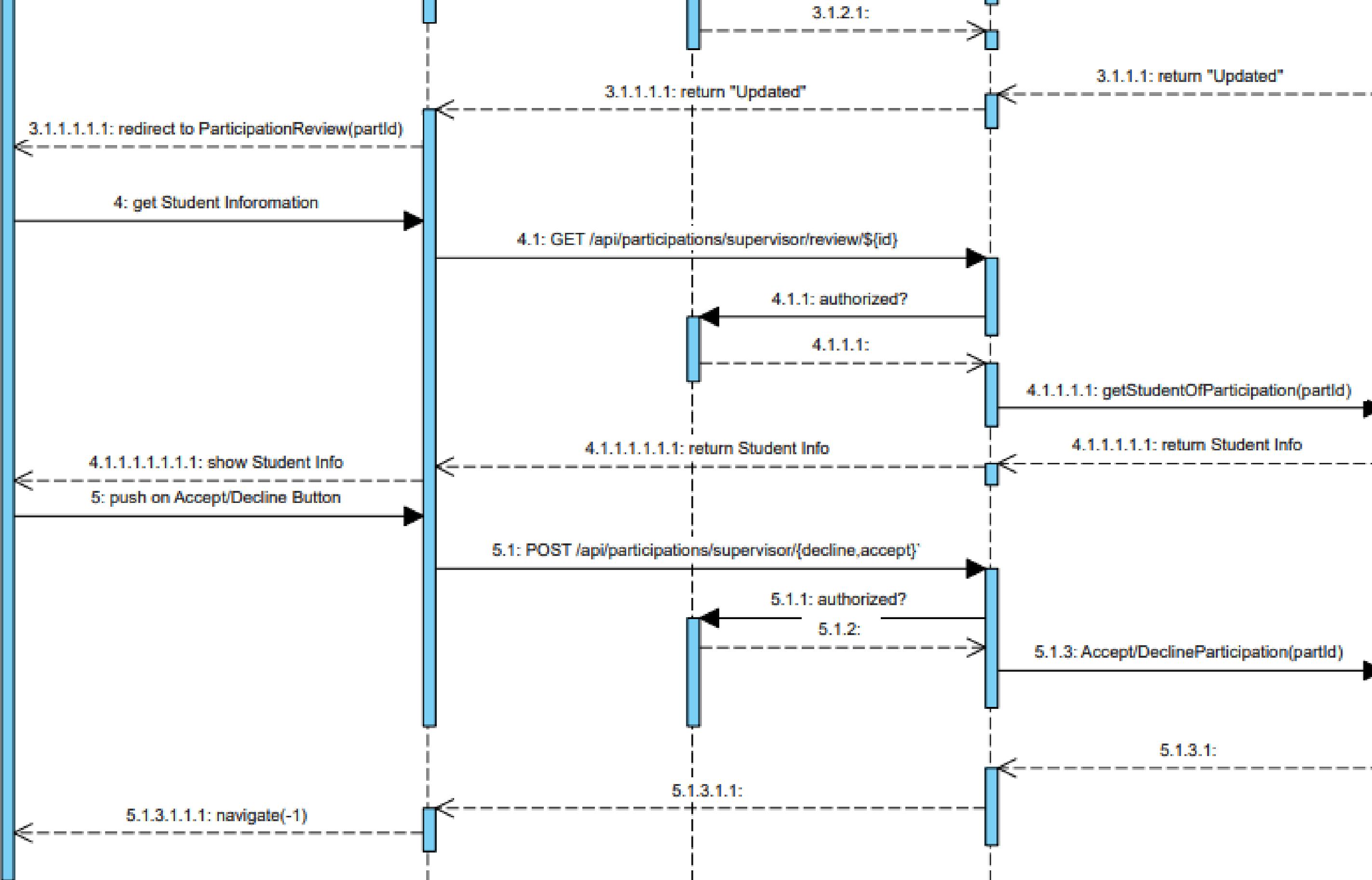




SUPERVISORE - Revisione Applicazione Bando

1. L'utente **supervisore**, già **AUTENTICATO**, accede alla dashboard richiedendo, dunque, tutti i **bandi** che ha già creato in precedenza (presupponendo che ne abbia creato almeno uno ed esista almeno uno **studente** che abbia fatto **application**)
2. L'utente supervisore **AUTORIZZATO** clicca sul bottone corrispondente al bando che vuole gestire venendo redirezionato ad una vista contenente la lista delle partecipazioni degli studenti a quel particolare bando (Vista **ParticipationView**).
3. L'utente supervisore clicca un apposito pulsante che scatena la redirezione verso la pagina di revisione della partecipazione (Vista **ParticipationReview**) all'interno della quale visualizzerà le **info** dello studente che l'ha sottomessa e i pulsanti per accettarla o declinarla.
4. Al click di uno dei due pulsanti lo stato della partecipazione sarà aggiornato e l'utente supervisore rediretto verso la vista delle partecipazioni.



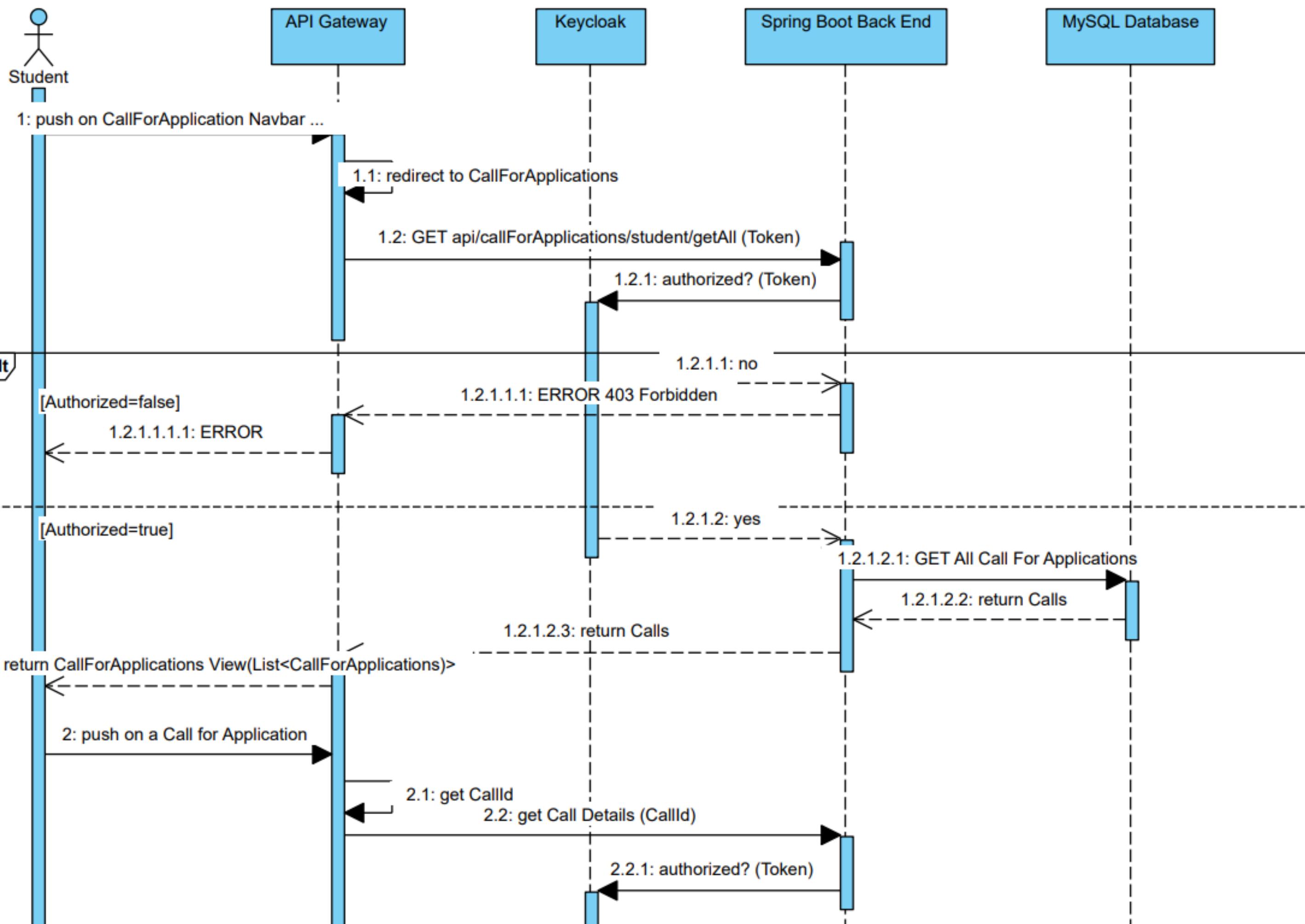


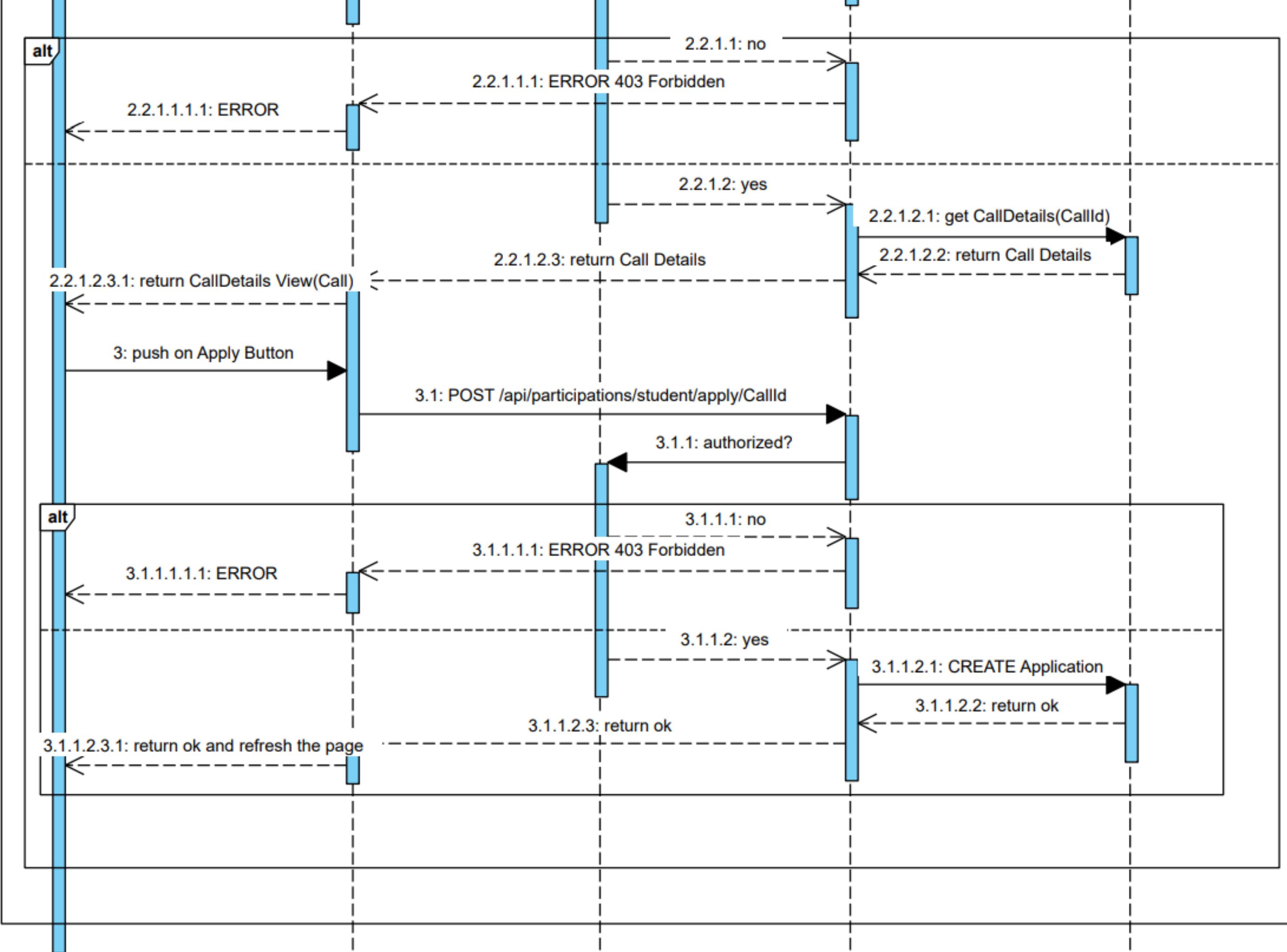


STUDENTE - Applicazione ad un bando

1. L'utente **studente AUTENTICATO**, utilizzando un apposito pulsante sulla **Navbar**, viene rediretto verso la vista di partecipazione ai bandi di concorso (Vista CallforApplications)
2. Se **AUTORIZZATO** allora il back-end richiede al database tutti bandi di concorso al quale uno studente può fare applicazione e ne restituisce una lista che il front-end invia alla vista dell'utente.
3. Quando l'utente studente clicca su un bando per fare application, se **AUTORIZZATO**, viene rediretto ad una vista contenente le **informazioni del bando** specifico ed un pulsante per inoltrare l'application (Vista CallDetails).
4. Alla pressione del pulsante per inoltrare **candidatura**, se **AUTORIZZATO**, viene creata nel database una istanza della partecipazione dell'utente studente al bando specificato.
5. La vista dell'utente viene infine aggiornata automaticamente

Lo studente è già autenticato, ovvero ha già effettuato il Login attraverso Keycloak e ha ricevuto un token valido. Inoltre un supervisor ha già provveduto a creare un Bando di partecipazione





The image shows a laptop and a smartphone displaying the homepage of the Università Federico II Selection Portal. The portal features a dark header with the university's name and navigation links. The main content area is titled "Portale di Selezione dell'Università" and includes a welcome message and a large "Inizia ora" button. Below this, there is a section titled "Ultimi Bandi di Selezione" showing two examples of recent announcements. The announcements are displayed in boxes with the university's logo, title, description, expiration date, and a "Candidati" button. The smartphone screen shows a similar layout with additional content visible below the fold.

Università Federico II Home Come Funziona Contatti

Portale di Selezione dell'Università

Benvenuto! Trova e candidati ai bandi di selezione dell'università.

Inizia ora

Ultimi Bandi di Selezione

BANDO PER MIGLIORE TESI MAGISTRALE
Bando
Expire: 2024-02-02
Candidati

Bando PART-TIME
Bando per lavoro part time studenti attualmente iscritti ad un corso di Laurea Federico II
Expire: 2024-03-01
Candidati

Università Federico II Home Come Funziona Contatti

Login Register

Portale di Selezione dell'Università

Benvenuto! Trova e candidati ai bandi di selezione dell'università.

Inizia ora

Ultimi Bandi di Selezione

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
BANDO PER MIGLIORE TESI MAGISTRALE
Expire: 2024-02-02

UNIVERSITÀ DEGLI STUDI DI NAPOLI FEDERICO II
Bando PART-TIME
Bando per lavoro part time studenti attualmente iscritti ad un corso di Laurea Federico II
Expire: 2024-03-01
Candidati

HomePage

The screenshot shows a web application for managing calls for applications. At the top, there's a navigation bar with the university logo and links for Home, Call For Application, and Contatti.

The main content area displays three call entries:

- ERASMUS + For Traineeship**
Date of Expire: 2024-01-01
Avviso di selezione per l'assegnazione di 390 borse di mobilità Erasmus a fini di tirocinio 2023/24
Edit Delete
- Bando PART-TIME**
Date of Expire: 2024-03-01
Selezione per assegnazione di collaborazioni studentesche 23/24
Edit Delete
- STEM Intesa San Paolo**
Date of Expire: 2024-02-02
Concorso per l'assegnazione di n. 1 borsa di studio biennale STEM IMI CIB
Edit Delete

A large yellow hand icon points to the "Edit" button of the first call entry. A grey arrow points from this entry to a detailed view modal titled "CallForApplication 8".

CallForApplication 8

Title: Bando PART-TIME

Expire Date: 01/03/2024

Doc Url: <https://www.unina.it/documents/11958/42822072/PT-2>

Description: Selezione per assegnazione di collaborazioni studentesche 23/24

Submit Call For Application

Vista di un **Supervisor**:
-Accesso ai Bandi da lui creati
-Modifica/Eliminazione e Creazione dei Bandi

Participation number: 7

Issued Date: 2023-12-14

Review State: In Review

Status: *Applied*



Review

Participation ID: 7

Name: **Antonio** Surname: **Mare**

Matricola: M63001374

Student Contact:

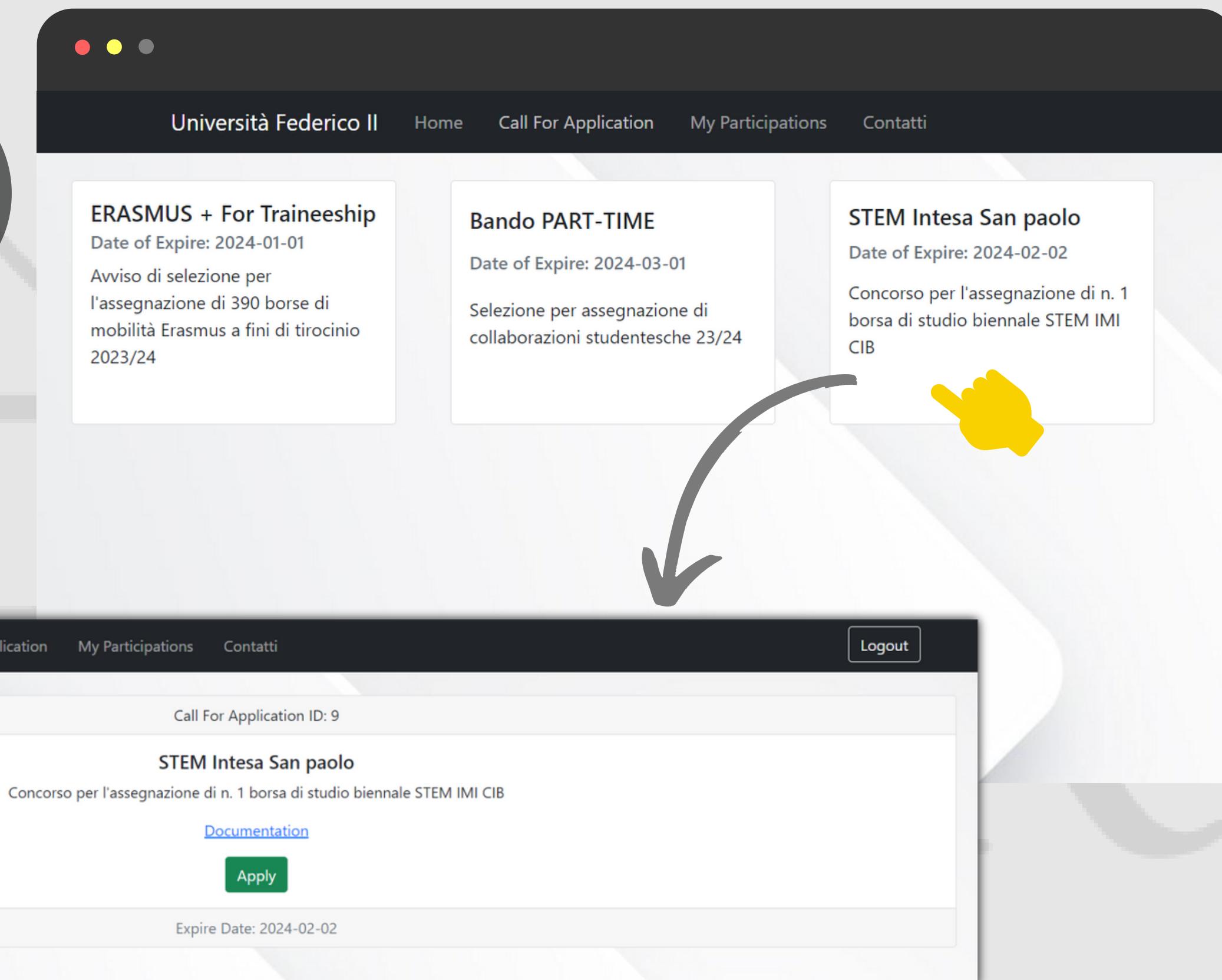
Matricola	Email
M63001374	antonio.mare@live.it

Approve **Decline**

Vista di un **Supervisor**:

- Accesso alle participations relative ad un Bando
- Review con Approvazione/Rifiuto di una participation

Vista di uno **Studente**:
-Accesso ai Bandi aperti
-Vista dei **dettagli** del
Bando con possibilità di fare
application



The screenshot shows the Università Federico II application portal interface. At the top, there is a navigation bar with the university's name and links to Home, Call For Application, My Participations, and Contatti. Below the navigation bar, three call cards are displayed:

- ERASMUS + For Traineeship**
Date of Expire: 2024-01-01
Avviso di selezione per l'assegnazione di 390 borse di mobilità Erasmus a fini di tirocinio 2023/24
- Bando PART-TIME**
Date of Expire: 2024-03-01
Selezione per assegnazione di collaborazioni studentesche 23/24
- STEM Intesa San paolo**
Date of Expire: 2024-02-02
Concorso per l'assegnazione di n. 1 borsa di studio biennale STEM IMI CIB

A large yellow hand icon is positioned over the third call card, pointing towards it. A curved arrow originates from the bottom right of the third call card and points down to a detailed view of the "STEM Intesa San paolo" call for application.

Call For Application ID: 9

STEM Intesa San paolo
Concorso per l'assegnazione di n. 1 borsa di studio biennale STEM IMI CIB

[Documentation](#)

Apply

Expire Date: 2024-02-02



Participation number: 3

Issued Date: 2023-12-13

Review Status: *Reviewed*

Status: **Declined**

Applied for: [ERASMUS + For Traineeship](#)

Participation number: 4

Issued Date: 2023-12-14

Review Status: *To Be Reviewed*

Status: **Applied**

Applied for: [Bando PART-TIME](#)

Participation number: 7

Issued Date: 2023-12-14

Review Status: *In Review*

Status: **Approved**

Applied for: [STEM Intesa San paolo](#)

Vista di uno **Studente**:

- Accesso alle participation sottomesse
- Monitoring dello stato di lavorazione/esito

4.Tecnologie Utilizzate



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II





- **Keycloak** è un sistema open-source per la gestione delle **identità** e degli **accessi**.
- È stato progettato per offrire servizi di **autenticazione**, **autorizzazione** e gestione delle **sessioni** per applicazioni e servizi.
- Keycloak fornisce funzionalità di sicurezza avanzate, inclusa la **gestione degli utenti**, la federazione delle **identità**, il **single sign-on** (SSO) e la gestione centralizzata degli accessi.

All'interno della nostra applicazione è stata utilizzata la versione **15.0.2** come provider **IAM**



Configurazione

- Keycloak è organizzato in **Realm** (un set di utenti, credenziali, ruoli e gruppi) e **Client**.
- Per prima cosa, per configurare correttamente Keycloak, è stato creato un Realm denominato “**SSD_REALM**” all’interno del quale è stato poi creato un client: **“Application-rest-api”**

The screenshot shows the Keycloak administration interface. The top navigation bar has the Keycloak logo and the text "KEYCLOAK". Below it, a dropdown menu shows "SSD_REALM". The main sidebar on the left has sections "Configure" and "Manage". Under "Configure", there are links for "Realm Settings", "Clients", "Client Scopes", "Roles", "Identity Providers", "User Federation", and "Authentication". Under "Manage", there are links for "Groups", "Users", "Sessions", "Events", "Import", and "Export". The right panel is titled "Clients" and contains a table with the following data:

Client ID	Enabled
account	True
account-console	True
admin-cli	True
application-rest-api	True
broker	True
realm-management	True
security-admin-console	True



RBAC

Keycloak ci ha consentito di realizzare un Controllo Accessi basato su Ruoli (**RBAC**) per l'accesso alle varie risorse.

Al fine di assegnare a ciascun utente degli specifici permessi sono stati realizzati 3 ruoli distinti:

- **STUDENTE**
- **SUPERVISOR**
- **ADMIN**

Roles

Realm Roles Default Roles

Search... View all roles

Role Name	Composite
ROLE_ADMIN	True
ROLE_STUDENTE	False
ROLE_SUPERVISOR	False
default-roles-ssd_realm	True
offline_access	False
uma_authorization	False



RBAC

- L'unico **ruolo composito** è assegnato è quello di “**ADMIN**”
- La ragione alla base di questa scelta consiste nella possibilità di registrare utenti nella piattaforma assieme alla necessità dei permessi necessari all'utente “**ADMIN**” per **abilitare/disabilitare** i vari utenti.

ROLE_ADMIN trash

Details Attributes Users in Role

Role Name

Description

Composite Roles ON OFF

Save Cancel

Composite Roles

Realm Roles	Available Roles	Associated Roles
<input type="text" value="realm-management"/>	<input type="text" value="default-roles-ssd_realm"/> <input type="text" value="offline_access"/> <input type="text" value="ROLE_STUDENTE"/> <input type="text" value="ROLE_SUPERVISOR"/> <input type="text" value="uma_authorization"/>	<input type="text"/>
	Add selected >	< Remove selected
<input type="text" value="create-client"/> <input type="text" value="impersonation"/> <input type="text" value="manage-authorization"/> <input type="text" value="manage-clients"/> <input type="text" value="manage-events"/>	<input type="text"/>	<input type="text" value="manage-users"/> <input type="text" value="query-clients"/> <input type="text" value="query-realms"/> <input type="text" value="query-users"/> <input type="text" value="realm-admin"/>
	Add selected >	< Remove selected



Integrazione con Spring Boot

- Allo scopo di integrare Keycloak con il back-end sviluppato utilizzando il framework “**Spring Boot**” è necessario inserire le dipendenze richieste all’ interno del file “pom.xml”
- Mentre le informazioni necessarie e le proprietà richieste vengono inserite nel file denominato “application.properties”

```
<dependency>
    <groupId>org.keycloak</groupId>
    <artifactId>keycloak-spring-boot-2-adapter</artifactId>
    <version>13.0.1</version>
</dependency>
<dependency>
    <groupId>org.keycloak</groupId>
    <artifactId>keycloak-tomcat7-adapter-dist</artifactId>
    <version>13.0.1</version>
    <type>pom</type>
</dependency>
```

```
keycloak.realm = SSD_REALM
keycloak.auth-server-url = http://mykeycloak:8080/auth
keycloak.resource = ${keycloakResource}
keycloak.principal-attribute=preferred_username
keycloak.ssl-required=none
keycloak.use-resource-role-mappings = true
```



Integrazione con Spring Boot

Per far sì che le proprietà di Keycloak definite alla slide precedente vengano ricercate correttamente da Spring Boot è necessaria una classe di configurazione (chiamata “**ConfigResolver**”) evitando che venga realizzata la ricerca di default del file “keycloak.json”

```
@Configuration
public class CustomKeycloakSpringBootConfigResolver extends KeycloakSpringBootConfigResolver {
    private final KeycloakDeployment keycloakDeployment;

    public CustomKeycloakSpringBootConfigResolver(KeycloakSpringBootProperties properties) {
        keycloakDeployment = KeycloakDeploymentBuilder.build(properties);
    }

    @Override
    public KeycloakDeployment resolve(HttpFacade.Request facade) {
        return keycloakDeployment;
    }
}
```

In seguito, è stato essenziale definire una nuova classe denominata **SecurityConfig**. Questa classe estende la classe **KeycloakWebSecurityConfigurerAdapter**, consentendo la ridefinizione dei metodi di base di Keycloak per interporre la logica applicativa e facilitare le fasi di **autorizzazione**.

```
/**  
 * Registers the KeycloakAuthenticationProvider with the authentication manager.  
 */  
@Autowired  
public void configureGlobal(AuthenticationManagerBuilder auth) throws Exception {  
    KeycloakAuthenticationProvider keycloakAuthenticationProvider = keycloakAuthenticationProvider();  
    keycloakAuthenticationProvider.setGrantedAuthoritiesMapper(new SimpleAuthorityMapper());  
    auth.authenticationProvider(keycloakAuthenticationProvider);  
}
```

La presenza di questo metodo è fondamentale per registrare Keycloak come **Authentication Manager** al posto del modulo Spring Security, che di default è abilitato.

L'integrazione nelle applicazioni Spring Boot avviene mediante la sovrascrittura degli strumenti e metodi forniti da **Spring Security**, il meccanismo nativo di Spring.

Questa integrazione è implementata nel codice attraverso una classe denominata "**Security Config**", la quale facilita l'interposizione di Keycloak nel processo.

In particolare le policy di autorizzazione realizzate sono di tipo "**resource based**" (basate sui ruoli). Ciò viene realizzato con l'override del metodo **configure** di Spring Security.

```
@Override  
protected void configure(HttpSecurity http) throws Exception {  
    super.configure(http);  
    http  
        .csrf().disable()  
        .authorizeRequests()  
        .antMatchers(HttpMethod.POST, "/api/guest/register").permitAll()  
        .antMatchers("/api/admin/user/**").hasRole("ADMIN")  
        .antMatchers("/api/student/**").hasRole("STUDENTE")  
        .antMatchers("/api/callForApplications/guest/getLast").permitAll()  
        .antMatchers("/api/callForApplications/student/**").hasRole("STUDENTE")  
        .antMatchers("/api/participations/student/**").hasRole("STUDENTE")  
        .antMatchers("/api/callForApplications/supervisor/**").hasRole("SUPERVISOR")  
        .antMatchers("/api/participations/supervisor/**").hasRole("SUPERVISOR")  
    .anyRequest().authenticated();  
}
```

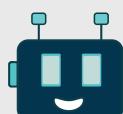


Registrazione degli Utenti

- Il form di Sign-Up consente agli utenti di effettuare la registrazione all'applicazione, specificando tra le informazioni anche il **ruolo** desiderato.
- Qualsiasi **tentativo** di registrazione privo delle informazioni necessarie verrà **rifiutato** dal server e segnalato opportunamente.

Registrazione Fallita 😞 !

Controlla che tutte le informazioni inserite siano corrette!



E' inoltre presente il servizio gratuito Google ReCaptcha v.2 per impedire vengano realizzati tentativi di registrazione automatici provenienti dai cosiddetti "**bot**"

Sign Up

UserName
Enter Username !
Insert the Username

Name
Enter Name !
Insert your Name

...

Enter Tel. Number

Password
Password !
Confirm Password
Password !

Non sono un robot reCAPTCHA
Privacy - Termini

[Create Account](#)

Already have an account?? [Sign In](#)



One Time Password

- A seguito della registrazione e dell'attivazione dell'account da parte dell'ADMIN a ciascuna tipologia di utente viene richiesto di configurare un dispositivo per l'implementazione dell'autenticazione a due fattori (2FA), oltre alla verifica della mail specificata in fase di registrazione.
- Nel nostro caso per generare gli OTP (One Time Password) è stato utilizzato Google Authenticator 

Mobile Authenticator Setup

A You need to set up Mobile Authenticator to activate your account.

1. Install one of the following applications on your mobile:
FreeOTP
Google Authenticator
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

Submit



Access Token

- Dopo aver completato con successo la procedura di login, l'utente acquisirà un **token di identità** e un **token di accesso**.
- Il token di identità comprende **informazioni relative all'utente**, quali il nome utente e l'indirizzo email.
- Il token di accesso è **digitalmente firmato dal realm** e contiene dettagli di accesso, come il ruolo dell'utente che l'applicazione può impiegare per stabilire le risorse per le quali sono concessi i permessi.

```
{  
  "exp": 1700666207,  
  "iat": 1700666147,  
  "auth_time": 1700666136,  
  "jti": "e14d410a-2eac-4516-8e52-37c5d9dff8ec",  
  "iss": "http://localhost:9000/auth/realms/SSD_REALM",  
  "aud": "account",  
  "sub": "93f1556e-f73e-4f27-807f-5d0ceec9097e",  
  "typ": "Bearer",  
  "azp": "application-rest-api",  
  "nonce": "8422035b-0169-4e6b-816e-7ee716aac159",  
  "session_state": "e720ab19-d0b1-453a-83cb-  
7eb353bd1701",  
  "acr": "0",  
  "allowed-origins": [  
    "*"  
,  
  "realm_access": {  
    "roles": [  
      "offline_access",  
      "uma_authorization",  
      "default-roles-ssd_realm",  
      "ROLE_SUPERVISOR"  
    ]  
  },  
  "resource_access": {  
    "application-rest-api": {  
      "roles": [  
        "ROLE_SUPERVISOR"  
      ]  
    },  
    "account": {  
      "roles": [  
        "manage-account",  
        "manage-account-links",  
        "view-profile"  
      ]  
    }  
  }  
}.
```



HashiCorp **Vault**

HashiCorp Vault è un sistema di gestione dei **segreti** identity-based utilizzato per **gestire e proteggere** l'accesso ai dati sensibili quali token, password, certificati o API keys...



Configurazione

Come descritto nel file di configurazione, si prevede:

- Il **salvataggio** dei segreti all'interno della cartella `./vault/data`
- L'ascolto per le richieste sul porto **8200** e mediante protocollo **HTTP**
- La possibilità di gestire Vault comodamente mediante una **GUI**

```
storage "file" {
    path      = "./vault/data"
}

listener "tcp" {
    address      = "0.0.0.0:8200"
    tls_disable = "true"
}

api_addr = "http://127.0.0.1:8200"
cluster_addr = "http://127.0.0.1:8201"
ui = true
```

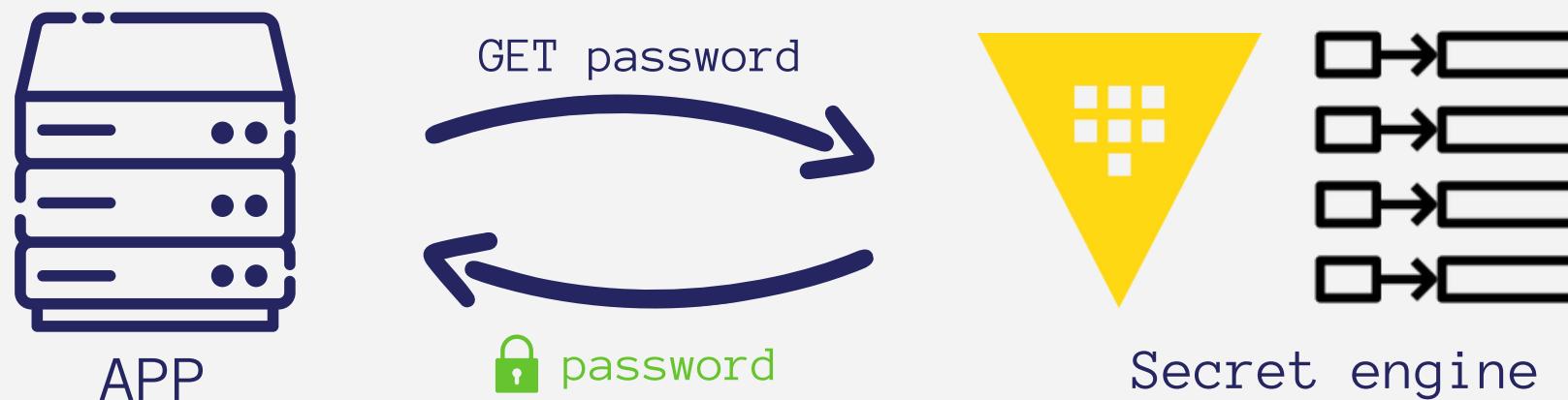


Secret engine

L'architettura di Vault è un'architettura a **plug-in**. Questi possono essere di tre tipi a seconda della funzionalità che implementano: **auth methods**, **secret engines** e **database plugins**.

Di nostro interesse è il *built-in secret engine* di Vault che ha il compito di **archiviare**, **generare** o **crittografare** dati di diverse tipologie. La più semplice è quella chiave/valore.

Il secret engine ci permetterà quindi di accedere a queste coppie chiave/valore in maniera protetta e **sicura** mediante apposite API.





Let's Encrypt è un'autorità di certificazione (**CA**) che offre certificati (**X.509**) **SSL/TLS** gratuiti per la crittografia del traffico web.

- L'obiettivo di Let's Encrypt e il protocollo **ACME** è quello di consentire di configurare un server HTTPS e di ottenere automaticamente un certificato di fiducia del browser, senza alcun intervento umano
- L'organizzazione fornisce strumenti software, come **Certbot**, che semplificano l'installazione e la gestione dei certificati SSL/TLS.
- Inoltre, i certificati Let's Encrypt sono validi per un breve periodo di tempo (**90 giorni**), incoraggiando l'uso delle pratiche di rinnovo automatico.

Certificazione



Al fine di acquisire un **certificato** per un determinato dominio, è necessario dimostrare il controllo di detto dominio. Questo processo richiede l'interazione col modulo software "**Agent**," ovvero l'agente di gestione dei certificati sul server web.

La comunicazione tra le due entità avviene mediante l'impiego del protocollo **ACME** (Automatic Certificate Management Environment).

Il protocollo ACME, è un protocollo di comunicazione sviluppato per agevolare l'interazione automatica tra l'Autorità di Certificazione e il Server Web. La sua specifica è chiaramente delineata nel **RFC 8555** (IETF).

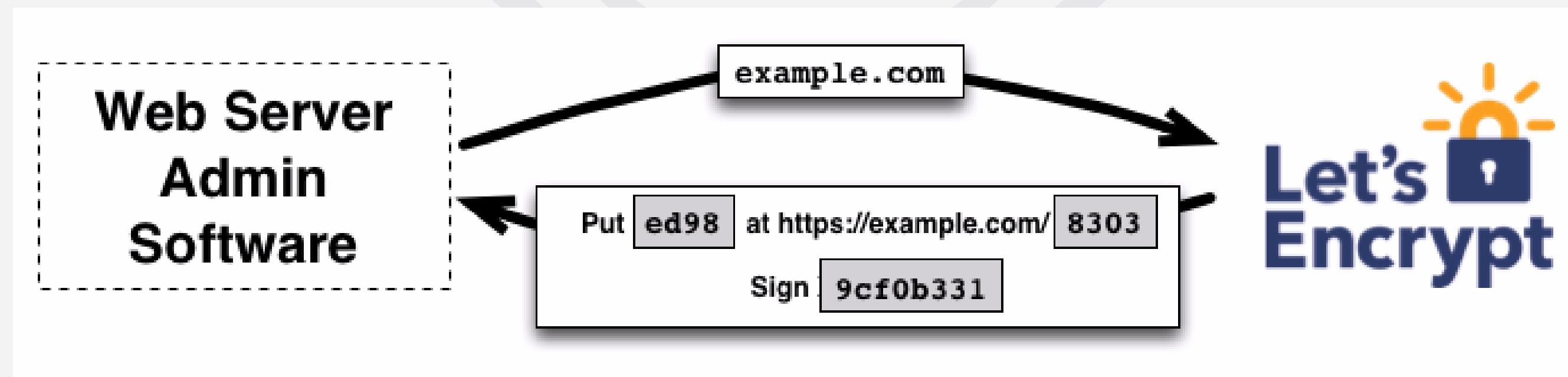
Ci sono **due** fasi per questo processo:

1. Prima di tutto l'agente dimostra alla CA che il server web controlla un dominio.
2. Poi, l'agente, può richiedere, rinnovare e revocare i certificati per quel dominio.

Validazione del dominio



Let's Encrypt identifica l'amministratore del server con la chiave pubblica. La prima volta che il client interagisce con Let's Encrypt, genera una **coppia di chiavi** e dimostra al Let's Encrypt CA che il server controlla uno o più domini.





La CA Let's Encrypt esaminerà il nome di dominio richiesto e emetterà una o più serie di **sfide**. Ci sono due modi che l'agente può utilizzare per dimostrare il **controllo** del dominio:

1.

Aggiungere un record DNS al dominio example.com

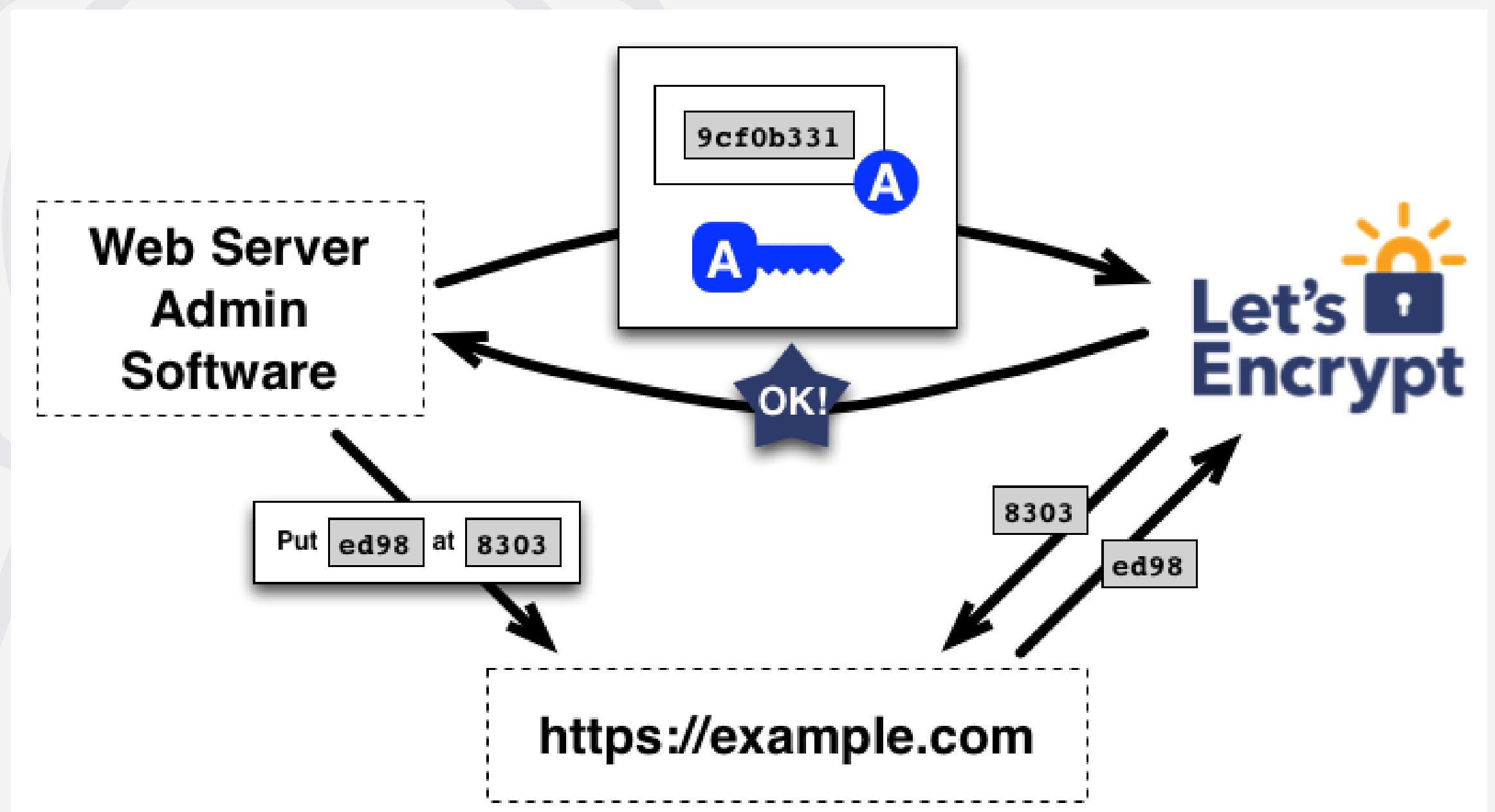
2.

Aggiungere una risorsa HTTP sotto un noto URI su <http://example.com/>

Insieme alle sfide, il Let's Encrypt CA fornisce anche una **nonce** che **l'agente** deve firmare con la sua coppia di chiavi per dimostrare che controlla la coppia stessa.

Una volta che il client ha completato questi passaggi, notifica alla CA che è pronto a completare la **convalida**. Poi è compito della CA verificare che le sfide siano state soddisfatte.

L'agente **identificato** dalla chiave pubblica è autorizzato alla gestione dei certificati.

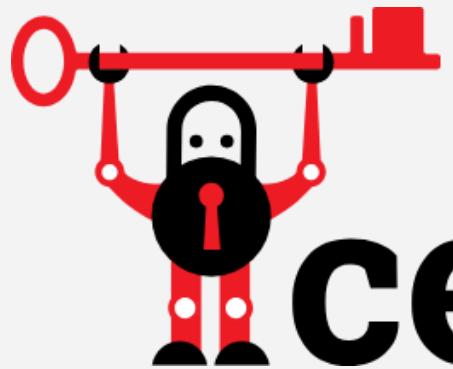


Una volta che l'agente ha una coppia di chiavi autorizzata, richiedere, rinnovare e revocare i certificati è semplice, basta inviare messaggi di gestione dei certificati e **firmarli** con la **coppia** di chiavi autorizzata.

Registrazione dominio “www.banduinina.it”

- La registrazione di un **dominio di rete**, necessaria affinchè la web app sia raggiungibile utilizzando un nome simbolico (in tal caso *banduinina.it*), è stata realizzata sul sito “Register.it”
- **Register.it** è un'azienda italiana che opera nel settore della fornitura di servizi di registrazione di domini, hosting, protezione del brand e pubblicità in rete. È stata la prima società italiana accreditata dall' **ICANN** e dal 2013 è stata riconosciuta ufficialmente dall'Agenzia per l'Italia digitale (AgID) come gestore certificato per la fornitura della Posta Elettronica Certificata.

The screenshot shows the main interface of the Register.it control panel. At the top, there's a navigation bar with links for Blog, Offerte, WebMail, Rivenditori, Rinnovi, Assistenza, and Logout. The main header displays the domain "banduinina.it". Below the header, there's a banner with the text "IL TUO SITO WEB È CONFORME?" and a green button labeled "SCOPRILO SUBITO!". A sidebar on the right shows account information: "Codice Cliente: DF26033-EURO" and "Gestione account, fatture e pagamenti ». The main content area is titled "PANNELLO DI CONTROLLO" and "banduinina.it". It features a grid of service icons under the heading "GESTISCI IL TUO DOMINIO E I TUOI PRODOTTI". The services include: DOMINIO & DNS, ASSOCIAZIONE DOMINIO, SMTP, EMAIL, PEC, WEB HOSTING, WORDPRESS HOSTING, HOSTING WINDOWS, MICRO SITE & COURTESY PAGE, SIMPLY SITE, ECOMMERCE, ADVERTISING, SITELOCK, and OFFICE 365. On the far right, a sidebar titled "I TUOI PRODOTTI" lists "PEC omaggio", "PEC omaggio", and "Dominio .online e .site in omaggio" all marked as "OMAGGIO". Another sidebar titled "ATTIVI" shows "Domini e prodotti" and "banduinina.it". At the bottom, there's an "Assistenza" section with a link to "Richiedi assistenza" and a note about finding answers or sending help requests.



certbot

- All'interno della nostra applicazione è stato utilizzato **CertBot** come software open-source per la gestione dei certificati e la comunicazione con Let's Encrypt.
- In particolare esso, è stato a sua volta deployato come **container Docker** all'interno della nostra architettura.

ssl-service:

```
image: certbot/certbot:v1.23.0
```

volumes:

```
- ./certbot/www/:/var/www/certbot/:rw  
- ./certbot/conf:/etc/letsencrypt/:rw
```

depends_on:

```
- front-end
```

command:

```
- renew  
#- certonly  
#- --webroot  
#- -w  
#- /var/www/certbot/  
#- --email=uninabandi@libero.it  
#- --agree-tos  
#- --no-eff-email  
#- -d  
#- bandiunina.it
```



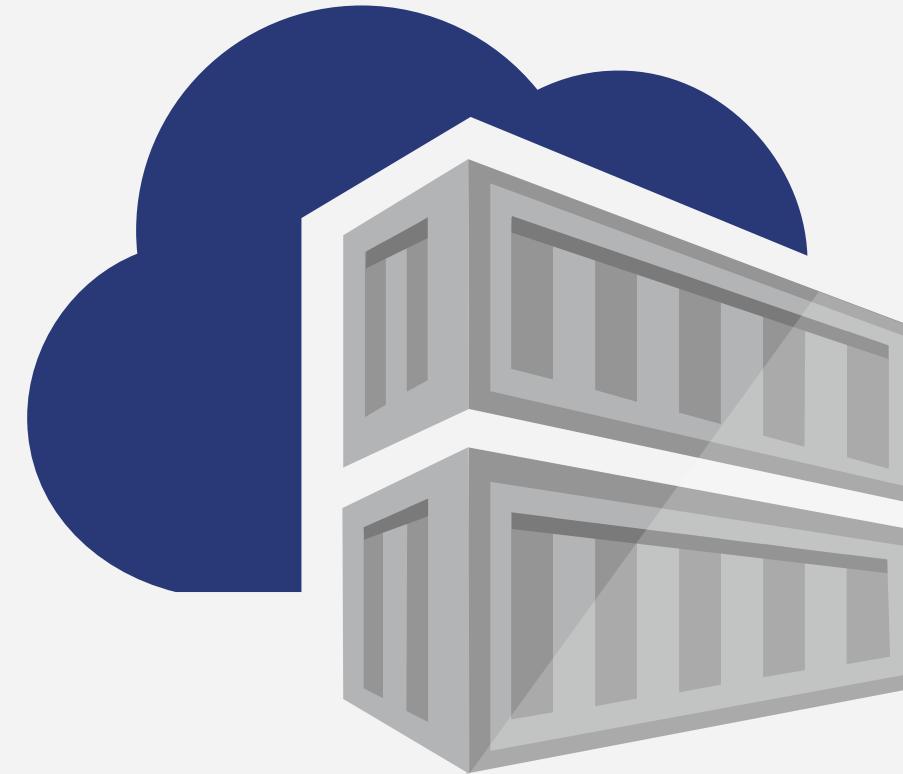
- **Docker** è una piattaforma open-source che facilita la creazione, distribuzione e gestione di applicazioni in “**container**”.
- I “contenitori” sono ambienti leggeri e portatili che includono tutto il **necessario** per eseguire un'applicazione, tra cui codice, runtime, librerie e dipendenze.
- Docker consente di **isolare** le applicazioni in contenitori, fornendo un'ambiente consistente e **riproducibile** su qualsiasi sistema in cui Docker è installato.
- Lo sviluppo di applicazioni basate su container consente di semplificare il **deployment** e i tempi di sviluppo, nonché di garantire facilmente attributi di **sicurezza** legati all'isolamento delle parti del sistema.



Ciascun container viene inizializzato e avviato con tutto il necessario mediante un file di configurazione tipicamente denominato “**Dockerfile**”

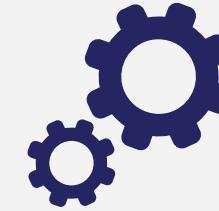
Come mostrato dall’architettura di riferimento è stato necessario realizzare ben **7** container distinti:

1. Spring Boot Java **Back-end**
2. Spring Boot Java **Admin-back-end**
3. **Nginx** con React **Front-end**
4. **CertBot**
5. **MySQL** per il database
6. **Vault**
7. **Keycloak**

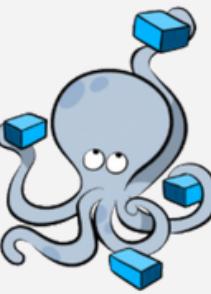




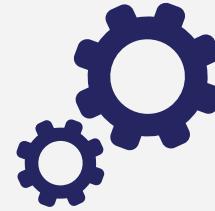
docker compose



- E' uno strumento che consente di definire e gestire applicazioni Docker **multi-container**.
- Con Docker Compose, è possibile definire un'applicazione composta da più servizi in un file chiamato **docker-compose.yml**, che contiene informazioni su quali immagini Docker utilizzare, come configurare i container, le **reti**, i volumi e altre opzioni di configurazione.
- Una volta definito il file docker-compose.yml, è possibile avviare l'intera applicazione eseguendo un **singolo comando** (`docker-compose up`).
- L'utilizzo di Docker Compose semplifica notevolmente la gestione di applicazioni complesse con più componenti, poiché consente di **orchestrare** facilmente l'avvio, l'arresto e la gestione di più container in modo coordinato.



docker compose



- Di seguito si riporta una parte del file di configurazione '**docker-compose.yml**' col quale vengono avviati e inizializzati tutti i container necessari all'avvio della nostra applicazione.
- Grazie all'impiego di docker compose viene realizzata di default una **rete virtuale** per la comunicazione dei container **interni**.
- Come è possibile osservare l'unico servizio che è possibile raggiungere dall'esterno è Nginx che espone i porti **80** e **443**

```
front-end:
  build:
    context: ./front-end
    dockerfile: Dockerfile
    restart: unless-stopped
    ports:
      - 80:80
      - 443:443
    depends_on:
      - back-end
    volumes:
      - ./nginx.conf:/etc/nginx/nginx.conf
  vault:
    hostname: vault
    container_name: vault
    restart: unless-stopped
    image: vault:1.13.3
    environment:
      VAULT_ADDR: "http://0.0.0.0:8200"
      VAULT_API_ADDR: "http://0.0.0.0:8200"
    volumes:
      - ./vault/config:/vault/config
      - ./vault/policies:/vault/policies
      - ./vault/data:/vault/data
      - ./vault/logs:/vault/logs
    cap_add:
      - IPC_LOCK
  entrypoint: vault server -config=/vault/config/config.hcl
```



Nginx è un web server open source che fa della **leggerezza** e delle **prestazioni** i suoi principali punti di forza.

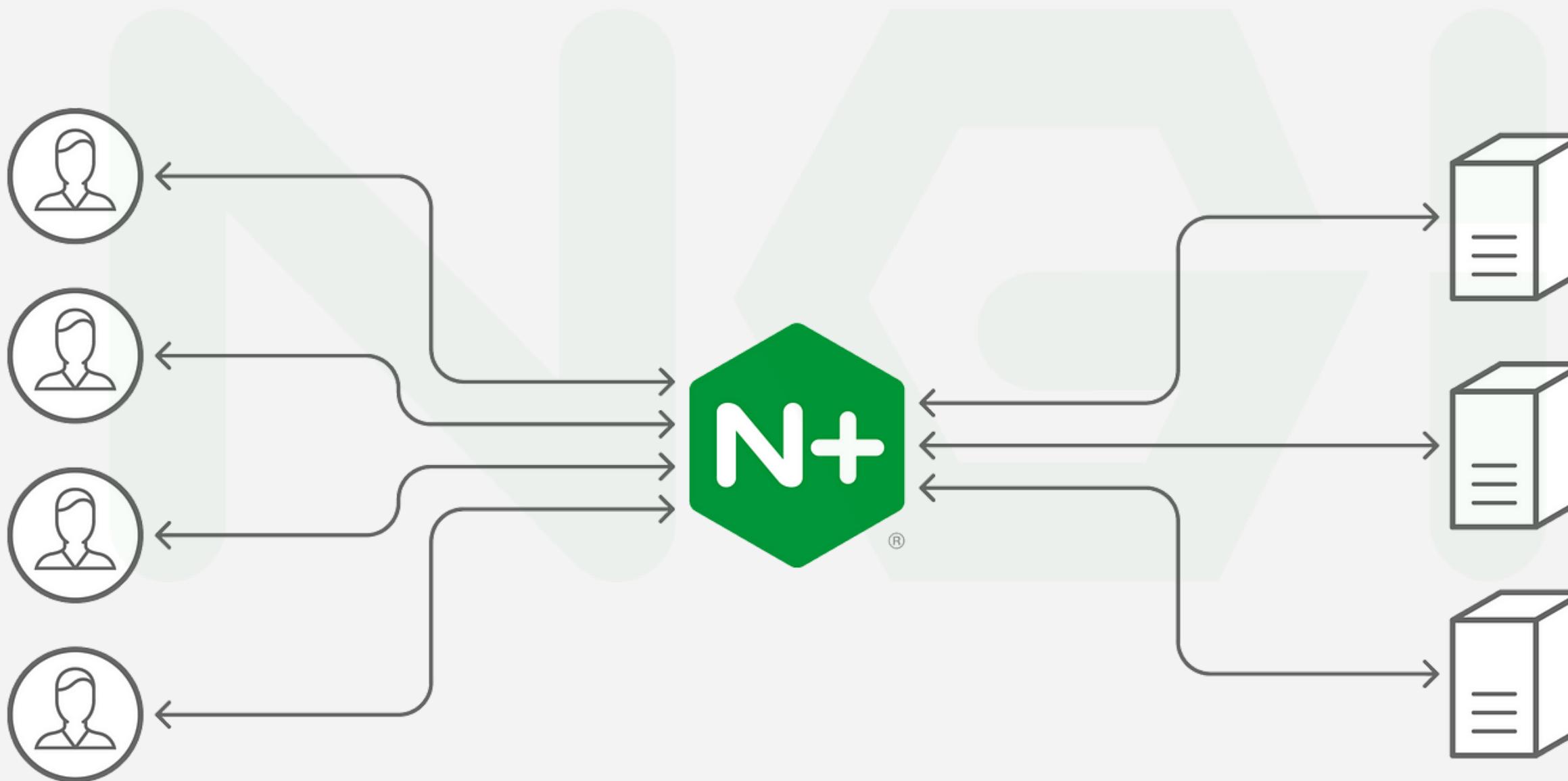
Esso può agire anche da **cache HTTP**, **load balancer** e **reverse-proxy**.

È proprio a queste ultime due funzionalità che nginx deve, ad oggi, la sua **diffusione su larga scala**.

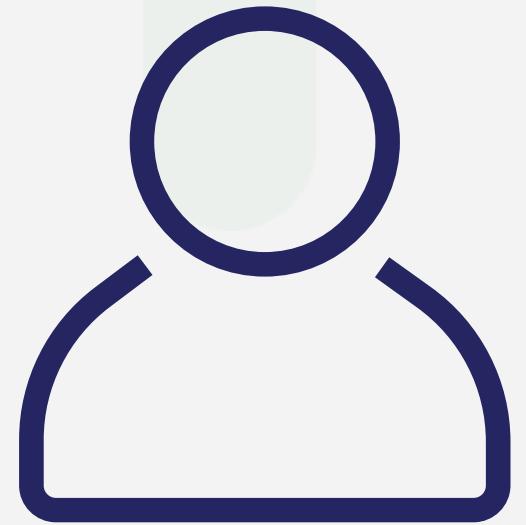
All'interno della nostra applicazione è stata
utilizzata la versione **1.24.0**

La funzionalità di nginx sfruttata per la nostra applicazione è quella di **reverse-proxy**.

Grazie a quest'ultima, infatti, nginx funge da **API Gateway** dell'applicazione permettendo così di instradare qualsiasi richiesta proveniente dai client all'appropriato servizio in esecuzione sul server.



Essendo l'unico punto di ingresso dell'applicazione, **nginx** dovrà essere configurato in modo da instaurare una **comunicazione sicura** con i client mediante il protocollo **HTTPS**.



HTTPS





- **DigitalOcean** è una piattaforma di cloud computing che fornisce servizi di infrastruttura come servizio (**IaaS**) per sviluppatori, aziende e team di programmati. La piattaforma offre una serie di servizi che consentono agli utenti di distribuire, gestire e scalare applicazioni su server virtuali (chiamati "droplets"), storage object-oriented, reti e altri servizi di cloud computing.

Tra le principali funzionalità ritroviamo:

1. **Droplets**: Si tratta di macchine virtuali configurabili dall'utente su cui è possibile eseguire applicazioni.
2. **Storage**: Servizi di storage basati su SSD
3. **Reti**: E' possibile configurare reti private virtuali, load balancer e altri servizi di rete
4. **Monitoring and Alert**: Strumenti per monitorare le prestazioni delle applicazioni e ricevere notifiche in caso di problemi

5. THREAT ANALYSIS AND ASSESSMENT



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II





1

Definizione obiettivo

Raggiungere un **livello di security low** [seguendo la **NIST SP 800-53 Rev. 5.1**] per l'applicazione categorizzata **low-impact** [NIST SP 800-37]



La modellazione è stata effettuata grazie al tool **Microsoft Threat Modeling Tool**

Modellazione del sistema



3

Identificazione dei threats

Microsoft TMT permette la generazione di un **report** di classificazione delle minacce



4

E' stata riportata per ogni minaccia individuata la **mitigazione** corrispondente

Mitigazione dei threats



5

Validazione delle mitigazioni

Per ogni mitigazione sono stati riportati i rispettivi **security controls** da implementare [seguendo lo standard NIST SP 800-53 Rev. 5.1]

Step 1 - risk based security categorization

Secondo il **NIST Security Management Framework** (“*NIST Special Publication 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems*”) bisogna anzitutto categorizzare le informazioni gestite dal sistema (ed il sistema informativo stesso) sulla base di una “analisi dell’impatto” (*impact analysis*) orientata relativamente alla perdita di una (o più) delle proprietà CIA.

Seguendo la pubblicazione “**FIPS Publication 199 - Standards for Security Categorization of Federal Information and Information Systems**” è stato assegnato un livello generale di impatto alle informazioni gestite dal sistema informativo (ed al sistema informativo stesso) pari alla categoria **Low-impact**.

Low-impact: *The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals*

nota: ogni tipo di informazione gestita dal sistema informativo è stata classificata low-impact e dunque il livello generale, pari al livello più alto categorizzato durante l’analisi, è pari proprio a low-impact.

Cos'è la Threat Analysis?

- • La threat analysis è un **processo** utilizzato per determinare quali sono i tipi di **minacce** ("threats") ai quali sono sottoposti i componenti di un sistema informatico che devono essere **protetti**, determinando il **rischio** ad essi associato.

• *Process of formally evaluating the degree of **threat** to an information system or enterprise and describing the nature of the threat [NIST glossary]*

Cos'è un threat?

- • I **threats** (che non includono esclusivamente attacchi mirati ma anche minacce ambientali, errori umani etc..) possono compromettere **confidentiality**, **integrity** o **availability** delle informazioni elaborate, archiviate o trasmesse.

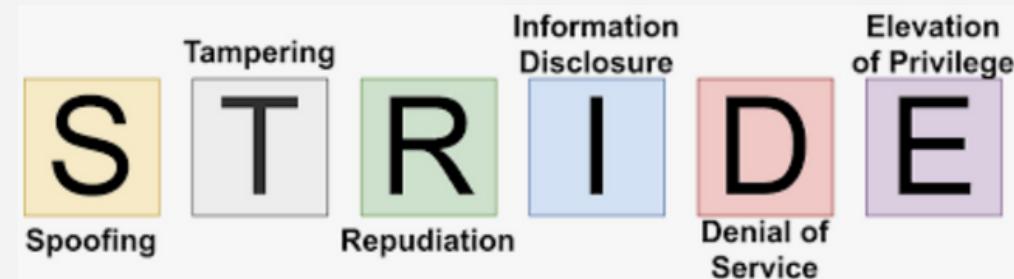
• *A threat is an event or situation that has the potential for causing undesirable consequences or impact [NIST glossary]*

Step 2/3 - threat modeling

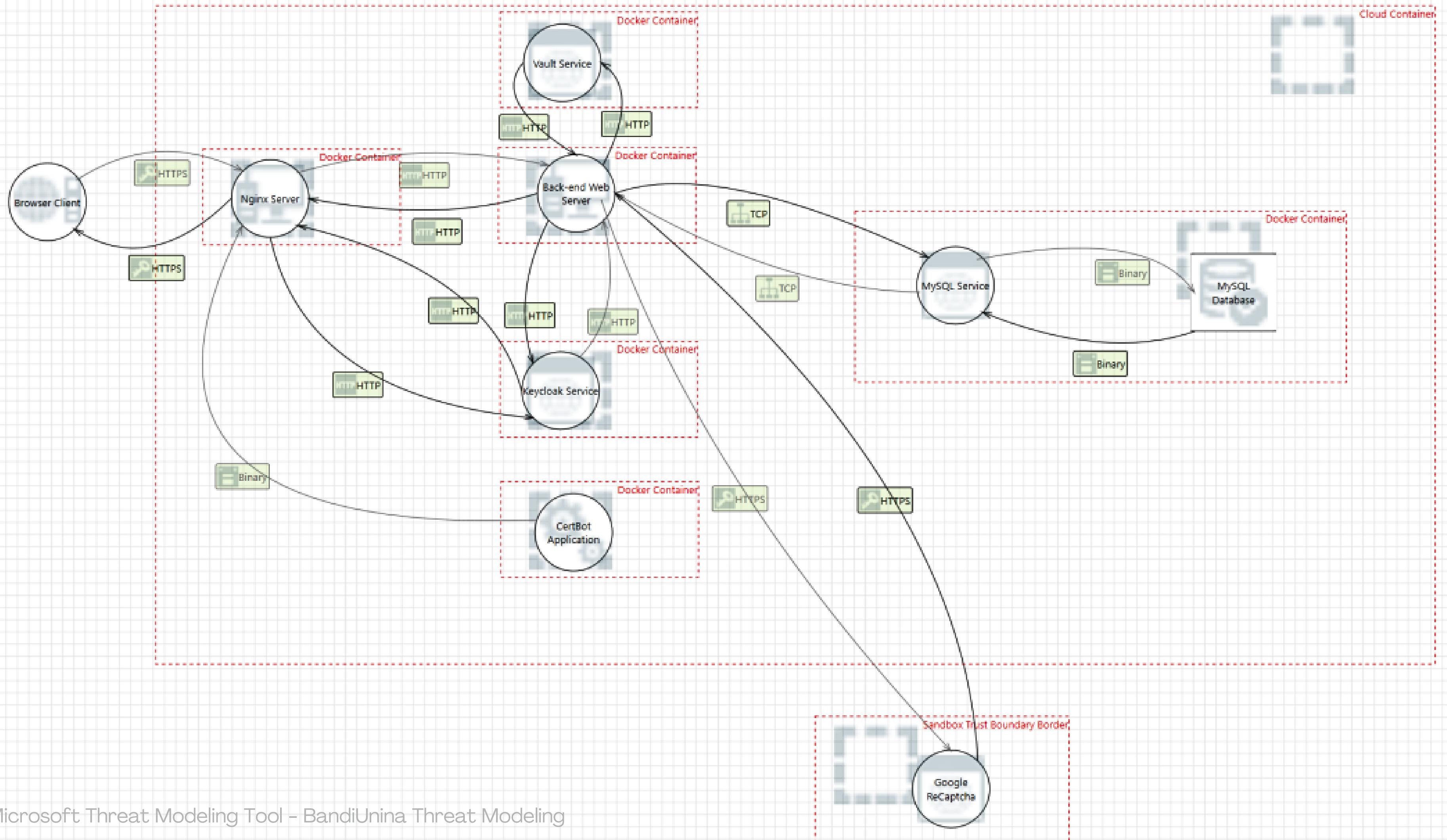
Il threat modeling è il processo che consente di **identificare** ed **enumerare** i threats al sistema informativo, e di conseguenza individuare le contromisure necessarie per **mitigarli**.

“A form of risk assessment that models aspects of the attack and defense sides of a logical entity, such as a piece of data, an application, a host, a system, or an environment” [NIST glossary]

Per modellare l'applicazione ed eseguire il processo di threat modeling, è stato utilizzato il tool gratuito **Microsoft Threat Modeling Tool** (centrale nel MSDL), basato sulla classificazione STRIDE:



Threat	Desired property	Threat Definition
Spoofing	Authenticity	Pretending to be something or someone other than yourself
Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere
Repudiation	Non-repudiability	Claiming that you didn't do something or were not responsible; can be honest or false
Information disclosure	Confidentiality	Providing information to someone not authorized to access it
Denial of service	Availability	Exhausting resources needed to provide service
Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do



Step 4 - threat analysis

- Successivamente alla modellazione della applicazione è stato possibile generare un **report sintetico** in formato **csv** di tutte le minacce STRIDE rivelate dal tool Microsoft Threat Modeling Tool (riportato nelle diapositive successive).
- Ad ogni minaccia è associato uno **stato** (**Mitigated**, Needs Investigation, Not Applicable) configurabile dall'analista, un titolo, una breve descrizione e la sua categoria STRIDE -> Nel report si è aggiunta ad ogni minaccia la relativa mitigazione da utilizzare in fase implementativa ed i relativi controlli di sicurezza che la garantiscono.
- La progettazione dei **security controls** è stata basata sullo standard **NIST SP 800-53** “Recommended Security Controls for Federal Information Systems and Organizations”, pubblicato dal **National Institute of Standards and Technology (NIST)** nel 2013, il quale descrive un elenco di security controls da implementare al fine di raggiungere un determinato **livello di sicurezza**: è stato scelto il livello di security “**low**” basandoci sulla **risk based security categorization** fatta nello step 1.
- Tale catalogo di security controls è organizzato in 18 famiglie: 17 specificate dalla pubblicazione **FIPS 200** “Minimum Security Requirements for Federal Information and Information Systems” del 2006 ed 1 aggiuntiva (Program Management)
- Per la FIPS-200 L'insieme minimo di security requirements ricopre 17 “**aree di sicurezza**” con l'obiettivo di proteggere *confidentiality, integrity and availability* (“CIA” triade) di sistemi informativi federali e delle informazioni da essi processate, memorizzate e trasmesse.

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	MA Maintenance	PM	Program Management

Step 5 – Assessment

In base alle mitigazioni individuate ed i rispettivi security controls da implementare (durante la fase di analysis), le famiglie da considerare tra quelle specificate dalla pubblicazione FIPS-200 sono le seguenti:

- Per mitigazione threats di **Information Disclosure** e **Spoofing** – Access Control (**AC**)
- Per mitigazione di **Repudiation**, **Elevation of Privilege** e **Information Disclosure** – “Identification and Authentication” (**IA**)
- Per mitigazione **Denial of Service**, **Tampering**, **Information Disclosure** e **Spoofing** – “System and Communications Protection” (**SC**)
- Per mitigazione **Repudiation** – “Audit And Accountability” (**AU**)

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
Data Flow HTTPS Is Potentially Interrupted	Denial Of Service	HTTPS	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.	SC-7 (3), SC-5, SC-7, SC-7(8)	Nginx, unico punto di accesso alle funzionalità della web-app, implementa meccanismi di gestione del flusso in ingresso mitigando DoS volumetrici (meccanismi opportunamente configurati tramite il file ".config").
Potential Process Crash or Stop for Keycloak Service	Denial Of Service	HTTP	High	Mitigated	Keycloak Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5	Il deploy dei componenti della web-app (API Gateway e front-end, secrets manager, Back-end, DBMS...) avviene in ambiente containerizzato gestito da docker-compose ed ogni container è configurato per essere eseguito
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.	SC-7 (3), SC-5, SC-7, SC-7(8)	Nginx unico punto di accesso alle funzionalità della web-app che implementa meccanismi di gestione del flusso in ingresso mitigando DoS volumetrici. Inoltre l'orchestrazione di container tramite Docker Compose permette di eseguire la web-app in una network locale non accessibile dall'esterno (Se non attraverso l'API Gateway).
Potential Process Crash or Stop for Back-end Web Server	Denial Of Service	HTTP	High	Mitigated	Back-end Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5	Il deploy dei componenti della web-app (API Gateway e front-end, secrets manager, Back-end, DBMS...) avviene in containers organizzati rete privata gestita da docker-compose ed ogni container è configurato per essere eseguito nuovamente in caso di crash. Inoltre tale ambiente containerizzato è eseguito su piattaforma cloud Digital Ocean, la quale è progettata per garantire alta availability oltre che alta scalabilità, flessibilità e connessioni low-latency.
Potential Process Crash or Stop for Vault Service	Denial Of Service	HTTP	High	Mitigated	Vault Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5	Il deploy dei componenti della web-app (API Gateway e front-end, secrets manager, Back-end, DBMS...) avviene in containers organizzati rete privata gestita da docker-compose ed ogni container è configurato per essere eseguito nuovamente in caso di crash. Inoltre tale ambiente containerizzato è eseguito su piattaforma cloud Digital Ocean, la quale è progettata per garantire alta availability oltre che alta scalabilità, flessibilità e connessioni low-latency.
Potential Process Crash or Stop for Nginx Server	Denial Of Service	HTTP	High	Mitigated	Nginx Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5	Il deploy dei componenti della web-app (API Gateway e front-end, secrets manager, Back-end, DBMS...) avviene in containers organizzati rete privata gestita da docker-compose ed ogni container è configurato per essere eseguito nuovamente in caso di crash. Inoltre tale ambiente containerizzato è eseguito su piattaforma cloud Digital Ocean, la quale è progettata per garantire alta availability oltre che alta scalabilità, flessibilità e connessioni low-latency.
Potential Process Crash or Stop for MySQL Service	Denial Of Service	TCP	High	Mitigated	MySQL Service crashes, halts, stops or runs slowly; in all cases violating an availability metric.	SC-5	Il deploy dei componenti della web-app (API Gateway e front-end, secrets manager, Back-end, DBMS...) avviene in containers organizzati rete privata gestita da docker-compose ed ogni container è configurato per essere eseguito nuovamente in caso di crash. Inoltre tale ambiente containerizzato è eseguito su piattaforma cloud Digital Ocean, la quale è progettata per garantire alta availability oltre che alta scalabilità, flessibilità e connessioni low-latency.
Elevation Using Impersonation	Elevation Of Privilege	HTTPS	High	Mitigated	Browser Client may be able to impersonate the context of Nginx Server in order to gain additional privilege.	AC-4, SC-23, SC-39	La comunicazione tra client e front-end (gestito dall'API-Gateway Nginx) avviene su HTTPS, il quale si basa su protocollo TLS che utilizza certificati digitali per autenticare la comunicazione, quindi un client malevolo non può impersonificare Nginx verso l'esterno. Inoltre il deploy in rete dockerizzata dei componenti della applicazione garantisce comunicazioni interne private e dunque previene la impersonificazione da parte di nodi esterni nei confronti
Elevation by Changing the Execution Flow in Back-end Web Server	Elevation Of Privilege	HTTP	High	Mitigated	An attacker may pass data into Back-end Web Server in order to change the flow of program execution within Back-end Web Server to the attacker's choosing.	SI-10	Il back-end implementa meccanismi di input validation al fine di proteggersi da attacchi che sfruttano vulnerabilità di tipo EOP.

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
Elevation by Changing the Execution Flow in Back-end Web Server	Elevation Of Privilege	HTTP	High	Mitigated	An attacker may pass data into Back-end Web Server in order to change the flow of program execution within Back-end Web Server to the attacker's choosing.	SI-10	Il back-end implementa meccanismi di input validation al fine di proteggersi da attacchi che sfruttano vulnerabilità di tipo EOP.
Weak Access Control for a Resource	Information Disclosure	Binary	High	Mitigated	Improper data protection of MySQL Database can allow an attacker to read information not intended for disclosure. Review authorization settings.	AC-4, IA-2	Per l'accesso al database che mantiene la persistenza delle entità di dominio del sistema informatico è necessaria AUTENTICAZIONE tramite una coppia username-password. Tale coppia di segreti è opportunamente gestita dal componente secrets manager Vault, ed il back-end la ottiene comunicando con tale servizio in una rete privata dockerizzata sicura con deploy su infrastruttura
Data Flow Sniffing	Information Disclosure	TCP	High	Mitigated	Data flowing across TCP 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 system or simply be a disclosure of information leading to compliance violations. Consider encrypting the data flow.	SC-7, SC-8, SC-7(8)	La rete privata di containers gestita da docker-compose è accessibile solo tramite l'API Gateway (Nginx), dunque non è possibile fare "sniffing" delle comunicazioni TCP interne (dall'esterno della rete). Inoltre la comunicazione tra l'API-Gateway ed i client avviene su canale sicuro basato su protocollo applicativo HTTPS che si basa sul protocollo sicuro a livello trasporto TLS .
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance	SC-7, SC-8, SC-7(8)	La rete privata di containers gestita da docker-compose è accessibile solo tramite l'API Gateway (Nginx), dunque non è possibile fare "sniffing" delle comunicazioni HTTP interne (dall'esterno della rete). Inoltre la comunicazione tra l'API-Gateway ed i client avviene su canale sicuro basato su protocollo
Potential Data Repudiation by Nginx Server	Repudiation	HTTPS	High	Mitigated	Nginx Server 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 summary of	AU-2	L'API-Gateway Nginx è stato appositamente configurato (tramite il file ".config") per fare logging di tutte le richieste e risposte.
Potential Data Repudiation by Browser Client	Repudiation	HTTPS	High	Mitigated	Browser Client 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 summary of	AU-2	L'API-Gateway Nginx è stato appositamente configurato (tramite il file ".config") per fare logging di tutte le richieste e risposte.
Spoofing the Nginx Server Process	Spoofing	HTTP	High	Mitigated	Nginx Server may be spoofed by an attacker and this may lead to unauthorized access to Keycloak Service. Consider using a standard authentication mechanism to identify	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Keycloak Service Process	Spoofing	HTTP	High	Mitigated	Keycloak Service may be spoofed by an attacker and this may lead to information disclosure by Nginx Server. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Back-end Web Server Process	Spoofing	HTTP	High	Mitigated	Back-end Web Server may be spoofed by an attacker and this may lead to unauthorized access to Nginx Server. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Nginx Server Process	Spoofing	HTTP	High	Mitigated	Nginx Server may be spoofed by an attacker and this may lead to information disclosure by Back-end Web Server. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Nginx Server Process	Spoofing	HTTP	High	Mitigated	Nginx Server may be spoofed by an attacker and this may lead to information disclosure by Keycloak Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Back-end Web Server Process	Spoofing	HTTP	High	Mitigated	Back-end Web Server may be spoofed by an attacker and this may lead to information disclosure by Vault Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Vault Service Process	Spoofing	HTTP	High	Mitigated	Vault Service may be spoofed by an attacker and this may lead to information disclosure by Back-end Web Server. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
Spoofing the Back-end Web Server Process	Spoofing	HTTP	High	Mitigated	Back-end Web Server may be spoofed by an attacker and this may lead to unauthorized access to Vault Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Back-end Web Server Process	Spoofing	HTTP	High	Mitigated	Back-end Web Server may be spoofed by an attacker and this may lead to unauthorized access to Keycloak Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Keycloak Service Process	Spoofing	HTTP	High	Mitigated	Keycloak Service may be spoofed by an attacker and this may lead to information disclosure by Back-end Web Server. Consider using a standard authentication	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Nginx Server Process	Spoofing	HTTPS	High	Mitigated	Nginx Server may be spoofed by an attacker and this may lead to unauthorized access to Browser Client. Consider using a standard authentication mechanism to identify	AC-4, SC-12, SC-13, SC-17, SC-23	L'API-Gateway Nginx e il browser client comunicano su canale sicuro HTTPS.
Spoofing of Source Data Store MySQL Database	Spoofing	Binary	High	Mitigated	MySQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to MySQL Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Back-end Web Server Process	Spoofing	TCP	High	Mitigated	Back-end Web Server may be spoofed by an attacker and this may lead to unauthorized access to MySQL Service. Consider using a standard authentication mechanism to	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the MySQL Service Process	Spoofing	TCP	High	Mitigated	MySQL Service may be spoofed by an attacker and this may lead to information disclosure by Back-end Web Server. Consider using a standard authentication	SC-7, SC-7 (8)	La rete privata di docker containers in esecuzione su piattaforma cloud è raggiungibile da nodi esterni solo tramite l'API Gateway Nginx.
Spoofing the Google ReCaptcha Process	Spoofing	HTTPS	High	Mitigated	Google ReCaptcha may be spoofed by an attacker and this may lead to unauthorized access to Back-end Web Server. Consider using a standard authentication	SC-12, SC-13, SC-17, SC-23	Il Back-end comunica con il server che offre il servizio google ReCaptcha (https://www.google.com/recaptcha/api/siteverify) tramite HTTPS e quindi usa certificato TLS
Potential Lack of Input Validation for Back-end Web Server	Tampering	HTTP	High	Mitigated	Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Back-end Web Server or an elevation of privilege attack against Back-end Web Server or an information disclosure by Back-end Web Server. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the	SI-10	Il back-end implementa meccanismi di input validation per proteggersi da attacchi dovuti a tampering di flusso.
Back-end Web Server Process Memory Tampered	Tampering	HTTP	High	Mitigated	If Back-end Web Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Keycloak Service executes (for example, passing back a function pointer.), then Back-end Web Server can tamper with Keycloak Service. Consider if the function could work with less access to memory, such as	SC-39	Utilizzando una rete di container gestita da docker-compose, ogni macro-componente dell'applicazione esegue in un dominio d'esecuzione a sé stante (process isolation) e comunicherà con gli altri processi soltanto mediante interfacce da noi definite e controllate.

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
Potential Lack of Input Validation for MySQL Service	Tampering	TCP	High	Mitigated	Data flowing across TCP may be tampered with by an attacker. This may lead to a denial of service attack against MySQL Service or an elevation of privilege attack against MySQL Service or an information disclosure by MySQL Service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	SI-10	Il back-end, unico componente che comunica con il MySQL server nella rete privata dockerizzata, implementa meccanismi di input validation per proteggersi da attacchi dovuti a tampering di flusso e dunque anche il flusso TCP tra di essi è robusto a tampering. Inoltre Hibernate, un framework di persistenza per applicazioni Java, contribuisce alla sicurezza attraverso l'utilizzo di statement preparati e parametrizzati, riducendo il rischio di SQL injection. Il mapping automatico dei tipi di dati Java al database aiuta a prevenire errori di conversione e manipolazione dei dati. Il supporto a transazioni ACID garantisce l'integrità dei dati, evitando situazioni inconsistenti. L'Object-Relational Mapping semplifica la gestione dei dati, mentre la configurazione sicura delle connessioni al database offre opzioni di connessione sicura. La gestione delle relazioni e la validazione dei dati contribuiscono a garantire l'integrità e la coerenza delle informazioni. Tuttavia, la sicurezza complessiva richiede anche l'implementazione di best practice a livello di applicazione e infrastruttura.
Nginx Server Process Memory Tampered	Tampering	HTTPS	High	Mitigated	If Nginx Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Browser Client executes (for example, passing back a function pointer.), then Nginx Server can tamper with Browser Client. Consider if the function could work with	SC-39	Utilizzando una rete di container gestita da docker-compose, ogni macro-componente dell'applicazione esegue in un dominio d'esecuzione a sé stante (process isolation) e comunicherà con gli altri processi soltanto mediante interfacce da noi definite e controllate.
Nginx Server Process Memory Tampered	Tampering	HTTP	High	Mitigated	If Nginx Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Keycloak Service executes (for example, passing back a function pointer.), then Nginx Server can tamper with Keycloak Service. Consider if the function could work with	SC-39	Utilizzando una rete di container gestita da docker-compose, ogni macro-componente dell'applicazione esegue in un dominio d'esecuzione a sé stante (process isolation) e comunicherà con gli altri processi soltanto mediante interfacce da noi definite e controllate.
Cross Site Scripting	Tampering	HTTP	High	Mitigated	The web server 'Nginx Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	SI-10, SI-10(5)	L'utilizzo del framework React come tecnologia di sviluppo delle risorse web front-end consente di beneficiare di funzionalità di input validation e sanitization implementate nativamente. Inoltre Ngnix è appositamente configurato per difendersi da XSS attacks (configurazione presente in file ".config") grazie all'aggiunta di appositi header (tra cui quello relativo alla Content Security Policy).
Back-end Web Server Process Memory Tampered	Tampering	HTTP	High	Mitigated	If Back-end Web Server is given access to memory, such as shared memory or pointers, or is given the ability to control what Vault Service executes (for example, passing back a function pointer.), then Back-end Web Server can tamper with Vault Service. Consider if the function could work with less access to memory, such as passing data	SC-39	Utilizzando una rete di container gestita da docker-compose, ogni macro-componente dell'applicazione esegue in un dominio d'esecuzione a sé stante (process isolation) e comunicherà con gli altri processi soltanto mediante interfacce da noi definite e controllate.
Back-end Web Server Process Memory Tampered	Tampering	TCP	High	Mitigated	If Back-end Web Server is given access to memory, such as shared memory or pointers, or is given the ability to control what MySQL Service executes (for example, passing back a function pointer.), then Back-end Web Server can tamper with MySQL Service. Consider if the function could work with less access to memory, such as	SC-39	Utilizzando una rete di container gestita da docker-compose, ogni macro-componente dell'applicazione esegue in un dominio d'esecuzione a sé stante (process isolation) e comunicherà con gli altri processi soltanto mediante interfacce da noi definite e controllate.

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
MITIGAZIONE UGUALE A ID: 31							
Potential Data Repudiation by Nginx Server	Repudiation	HTTP	High	Mitigated	Nginx Server 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 summary of		
MITIGAZIONE UGUALE A ID=23							
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow HTTP Is Potentially Interrupted	Denial Of Service	HTTP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow TCP Is Potentially Interrupted	Denial Of Service	TCP	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
Data Flow HTTPS Is Potentially Interrupted	Denial Of Service	HTTPS	High	Mitigated	An external agent interrupts data flowing across a trust boundary in either direction.		
MITIGAZIONE UGUALE A ID=21							
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance		
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance		
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance		
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance		
Data Flow Sniffing	Information Disclosure	HTTP	High	Mitigated	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 system or simply be a disclosure of information leading to compliance		

Threat title	Category	Interaction	Priority	State	Threat description	Security controls	Mitigation description
MITIGATED "BY DEFAULT"							
Browser Client May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTPS	High	Mitigated	Nginx Server may be able to remotely execute code for Browser Client.	//	La versione di Ngnix utilizzata (v:1.24.0) non presenta vulnerabilità di RCE note.
Elevation by Changing the Execution Flow in Keycloak Service	Elevation Of Privilege	HTTP	High	Mitigated	An attacker may pass data into Keycloak Service in order to change the flow of program execution within Keycloak Service to the attacker's choosing.	//	La versione di Keycloak utilizzata (v:15.0.2) non presenta vulnerabilità di EOP note.
Elevation by Changing the Execution Flow in Vault Service	Elevation Of Privilege	HTTP	High	Mitigated	An attacker may pass data into Vault Service in order to change the flow of program execution within Vault	//	La versione di Vault utilizzata (v:1.13.3) non presenta vulnerabilità di EOP note.
Elevation by Changing the Execution Flow in Nginx Server	Elevation Of Privilege	HTTP	High	Mitigated	An attacker may pass data into Nginx Server in order to change the flow of program execution within Nginx Server	//	La versione di Ngnix utilizzata (v:1.24.0) non presenta vulnerabilità di EOP note.
Potential Lack of Input Validation for Nginx Server	Tampering	HTTP	High	Mitigated	Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Nginx Server or an elevation of privilege attack against Nginx Server or an information disclosure by Nginx Server. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify	//	La versione di Ngnix utilizzata (v:1.24.0) di per sè fornisce robustezza a minacce di tipologia denial-of-service, EOP ed information disclosure. Inoltre l'utilizzo del framework React come tecnologia di sviluppo delle risorse web front-end consente di beneficiare di funzionalità di input validation e sanitization implementate nativamente.
NOT APPLICABLE							
Potential Data+B70:G95 Repudiation by Back-end Web Server	Repudiation	HTTP	High	Not Applicable	Back-end Web Server 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		
Potential Data Repudiation by Vault Service	Repudiation	HTTP	High	Not Applicable	Vault Service 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 summary of		
Potential Data Repudiation by MySQL Service	Repudiation	TCP	High	Not Applicable	MySQL Service 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 summary of		
Potential Data Repudiation by Back-end Web Server	Repudiation	HTTPS	High	Not Applicable	Back-end Web Server 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		
Potential Data Repudiation by Keycloak Service	Repudiation	HTTP	High	Not Applicable	Keycloak Service 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 summary of		
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Keycloak Service may be able to impersonate the context of Nginx Server in order to gain additional privilege.		
Keycloak Service May be Subject to Elevation of Privilege Using Remote Code	Elevation Of Privilege	HTTP	High	Not Applicable	Nginx Server may be able to remotely execute code for Keycloak Service.		
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Nginx Server may be able to impersonate the context of Back-end Web Server in order to gain additional		
Nginx Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Back-end Web Server may be able to remotely execute code for Nginx Server.		

Threat title	Category	Interaction	Priority	State	Threat description		Security controls	Mitigation description
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Nginx Server may be able to impersonate the context of Back-end Web Server in order to gain additional privilege.			
Nginx Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Back-end Web Server may be able to remotely execute code for Nginx Server.			
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Back-end Web Server may be able to impersonate the context of Vault Service in order to gain additional privilege.			
Back-end Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Vault Service may be able to remotely execute code for Back-end Web Server.			
Vault Service May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Back-end Web Server may be able to remotely execute code for Vault Service.			
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Vault Service may be able to impersonate the context of Back-end Web Server in order to gain additional privilege.			
Nginx Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Keycloak Service may be able to remotely execute code for Nginx Server.			
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Nginx Server may be able to impersonate the context of Keycloak Service in order to gain additional privilege.			
Elevation Using Impersonation	Elevation Of Privilege	HTTP	High	Not Applicable	Keycloak Service may be able to impersonate the context of Back-end Web Server in order to gain additional privilege.			
Keycloak Service May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTP	High	Not Applicable	Back-end Web Server may be able to remotely execute code for Keycloak Service.			
Elevation Using Impersonation	Elevation Of Privilege	TCP	High	Not Applicable	MySQL Service may be able to impersonate the context of Back-end Web Server in order to gain additional privilege.			
MySQL Service May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	TCP	High	Not Applicable	Back-end Web Server may be able to remotely execute code for MySQL Service.			
Elevation by Changing the Execution Flow in MySQL Service	Elevation Of Privilege	TCP	High	Not Applicable	An attacker may pass data into MySQL Service in order to change the flow of program execution within MySQL Service to the attacker's			
Elevation Using Impersonation	Elevation Of Privilege	HTTPS	High	Not Applicable	Back-end Web Server may be able to impersonate the context of Google ReCaptcha in order to gain additional privilege.			
Back-end Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Elevation Of Privilege	HTTPS	High	Not Applicable	Google ReCaptcha may be able to remotely execute code for Back-end Web Server.			
Weak Authentication Scheme	Information Disclosure	HTTP	High	Not Applicable	Custom authentication schemes are susceptible to common weaknesses such as weak credential change management, credential equivalence, easily guessable credentials, null credentials, downgrade authentication or a weak credential change management system.			
Weak Authentication Scheme	Information Disclosure	HTTP	High	Not Applicable	Consider the impact and potential mitigations for your custom authentication scheme.			
Cross Site Scripting	Tampering	HTTPS	High	Not Applicable	The web server 'Back-end Web Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.			
Potential Lack of Input Validation for Keycloak Service	Tampering	HTTP	High	Not Applicable	Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Keycloak Service or an elevation of privilege attack against Keycloak Service or an information disclosure by Keycloak Service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.			
Potential Lack of Input Validation for Keycloak Service	Tampering	HTTP	High	Not Applicable	Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Keycloak Service or an elevation of privilege attack against Keycloak Service or an information disclosure by Keycloak Service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.			
Potential Lack of Input Validation for Vault Service	Tampering	HTTP	High	Not Applicable	Data flowing across HTTP may be tampered with by an attacker. This may lead to a denial of service attack against Vault Service or an elevation of privilege attack against Vault Service or an information disclosure by Vault Service. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.			



6. “Access Control” Control Family

NIST Risk Management Framework SP 800-53 Rev. 5.1

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	Policy and Procedures	X	X	X	X
AC-2	Account Management		X	X	X
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			X	X
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			X	X
AC-2(3)	DISABLE ACCOUNTS			X	X
AC-2(4)	AUTOMATED AUDIT ACTIONS			X	X
AC-2(5)	INACTIVITY LOGOUT			X	X
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE		W: Incorporated into AC-2k.		
AC-2(11)	USAGE CONDITIONS				X
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				X
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS			X	X
AC-3	Access Enforcement		X	X	X
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS		W: Incorporated into AC-6.		
AC-3(2)	DUAL AUTHORIZATION				
AC-3(3)	MANDATORY ACCESS CONTROL				
AC-3(4)	DISCRETIONARY ACCESS CONTROL				
AC-3(5)	SECURITY-RELEVANT INFORMATION				
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION		W: Incorporated into MP-4 and SC-28.		
AC-3(7)	ROLE-BASED ACCESS CONTROL				
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS				
AC-3(9)	CONTROLLED RELEASE				
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS				
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES				
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS				
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL				
AC-3(14)	INDIVIDUAL ACCESS	X			
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL				
AC-4	Information Flow Enforcement			X	X
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-4(2)	PROCESSING DOMAINS				
AC-4(3)	DYNAMIC INFORMATION FLOW CONTROL				
AC-4(4)	FLOW CONTROL OF ENCRYPTED INFORMATION				X
AC-4(5)	EMBEDDED DATA TYPES				
AC-4(6)	METADATA				
AC-4(7)	ONE-WAY FLOW MECHANISMS				
AC-4(8)	SECURITY AND PRIVACY POLICY FILTERS				
AC-4(9)	HUMAN REVIEWS				
AC-4(10)	ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS				
AC-4(11)	CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS				
AC-4(12)	DATA TYPE IDENTIFIERS				
AC-4(13)	DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS				
AC-4(14)	SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS				
AC-4(15)	DETECTION OF UNSANCTIONED INFORMATION				
AC-4(16)	INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS		W: Incorporated into AC-4.		
AC-4(17)	DOMAIN AUTHENTICATION				
AC-4(18)	SECURITY ATTRIBUTE BINDING		W: Incorporated into AC-16.		
AC-4(19)	VALIDATION OF METADATA				
AC-4(20)	APPROVED SOLUTIONS				
AC-4(21)	PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS				
AC-4(22)	ACCESS ONLY				
AC-4(23)	MODIFY NON-RELEASEABLE INFORMATION				
AC-4(24)	INTERNAL NORMALIZED FORMAT				
AC-4(25)	DATA SANITIZATION				
AC-4(26)	AUDIT FILTERING ACTIONS				
AC-4(27)	REDUNDANT/INDEPENDENT FILTERING MECHANISMS				
AC-4(28)	LINEAR FILTER PIPELINES				
AC-4(29)	FILTER ORCHESTRATION ENGINES				
AC-4(30)	FILTER MECHANISMS USING MULTIPLE PROCESSES				
AC-4(31)	FAILED CONTENT TRANSFER PREVENTION				
AC-4(32)	PROCESS REQUIREMENTS FOR INFORMATION TRANSFER				
AC-5	Separation of Duties			X	X
AC-6	Least Privilege			X	X
AC-6(1)	AUTHORIZE ACCESS TO SECURITY FUNCTIONS			X	X
AC-6(2)	NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS			X	X
AC-6(3)	NETWORK ACCESS TO PRIVILEGED COMMANDS				X
AC-6(4)	SEPARATE PROCESSING DOMAINS				
AC-6(5)	PRIVILEGED ACCOUNTS			X	X
AC-6(6)	PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS				
AC-6(7)	REVIEW OF USER PRIVILEGES			X	X
AC-6(8)	PRIVILEGE LEVELS FOR CODE EXECUTION				
AC-6(9)	LOG USE OF PRIVILEGED FUNCTIONS			X	X

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-6(10)	PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS			X	X
AC-7	Unsuccessful Logon Attempts		X	X	X
AC-7(1)	AUTOMATIC ACCOUNT LOCK	W: Incorporated into AC-7.			
AC-7(2)	PURGE OR WIPE MOBILE DEVICE				
AC-7(3)	BIOMETRIC ATTEMPT LIMITING				
AC-7(4)	USE OF ALTERNATE AUTHENTICATION FACTOR				
AC-8	System Use Notification		X	X	X
AC-9	Previous Logon Notification				
AC-9(1)	UNSUCCESSFUL LOGONS				
AC-9(2)	SUCCESSFUL AND UNSUCCESSFUL LOGONS				
AC-9(3)	NOTIFICATION OF ACCOUNT CHANGES				
AC-9(4)	ADDITIONAL LOGON INFORMATION				
AC-10	Concurrent Session Control				X
AC-11	Device Lock			X	X
AC-11(1)	PATTERN-HIDING DISPLAYS			X	X
AC-12	Session Termination			X	X
AC-12(1)	USER-INITIATED LOGOUTS				
AC-12(2)	TERMINATION MESSAGE				
AC-12(3)	TIMEOUT WARNING MESSAGE				
AC-13	Supervision and Review-Access Control	W: Incorporated into AC-2 and AU-6.			
AC-14	Permitted Actions without Identification or Authentication		X	X	X
AC-14(1)	NECESSARY USES	W: Incorporated into AC-14.			
AC-15	Automated Marking	W: Incorporated into MP-3.			
AC-16	Security and Privacy Attributes				
AC-16(1)	DYNAMIC ATTRIBUTE ASSOCIATION				
AC-16(2)	ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS				
AC-16(3)	MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM				
AC-16(4)	ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS				
AC-16(5)	ATTRIBUTE DISPLAYS ON OBJECTS TO BE OUTPUT				
AC-16(6)	MAINTENANCE OF ATTRIBUTE ASSOCIATION				
AC-16(7)	CONSISTENT ATTRIBUTE INTERPRETATION				
AC-16(8)	ASSOCIATION TECHNIQUES AND TECHNOLOGIES				
AC-16(9)	ATTRIBUTE REASSIGNMENT – REGRADING MECHANISMS				
AC-16(10)	ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS				
AC-17	Remote Access		X	X	X
AC-17(1)	MONITORING AND CONTROL			X	X
AC-17(2)	PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION			X	X
AC-17(3)	MANAGED ACCESS CONTROL POINTS			X	X
AC-17(4)	PRIVILEGED COMMANDS AND ACCESS			X	X
AC-17(5)	MONITORING FOR UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-17(6)	PROTECTION OF MECHANISM INFORMATION				
AC-17(7)	ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS	W: Incorporated into AC-3(10).			

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-17(8)	DISABLE NONSECURE NETWORK PROTOCOLS	W: Incorporated into CM-7.			
AC-17(9)	DISCONNECT OR DISABLE ACCESS				
AC-17(10)	AUTHENTICATE REMOTE COMMANDS				
AC-18	Wireless Access		X	X	X
AC-18(1)	AUTHENTICATION AND ENCRYPTION			X	X
AC-18(2)	MONITORING UNAUTHORIZED CONNECTIONS	W: Incorporated into SI-4.			
AC-18(3)	DISABLE WIRELESS NETWORKING			X	X
AC-18(4)	RESTRICT CONFIGURATIONS BY USERS				X
AC-18(5)	ANTENNAS AND TRANSMISSION POWER LEVELS				X
AC-19	Access Control for Mobile Devices		X	X	X
AC-19(1)	USE OF WRITABLE AND PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(2)	USE OF PERSONALLY OWNED PORTABLE STORAGE DEVICES	W: Incorporated into MP-7.			
AC-19(3)	USE OF PORTABLE STORAGE DEVICES WITH NO IDENTIFIABLE OWNER	W: Incorporated into MP-7.			
AC-19(4)	RESTRICTIONS FOR CLASSIFIED INFORMATION				
AC-19(5)	FULL DEVICE OR CONTAINER-BASED ENCRYPTION			X	X
AC-20	Use of External Systems		X	X	X
AC-20(1)	LIMITS ON AUTHORIZED USE			X	X
AC-20(2)	PORTABLE STORAGE DEVICES — RESTRICTED USE			X	X
AC-20(3)	NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE				
AC-20(4)	NETWORK ACCESSIBLE STORAGE DEVICES — PROHIBITED USE				
AC-20(5)	PORTABLE STORAGE DEVICES — PROHIBITED USE				
AC-21	Information Sharing			X	X
AC-21(1)	AUTOMATED DECISION SUPPORT				
AC-21(2)	INFORMATION SEARCH AND RETRIEVAL				
AC-22	Publicly Accessible Content		X	X	X
AC-23	Data Mining Protection				
AC-24	Access Control Decisions				
AC-24(1)	TRANSMIT ACCESS AUTHORIZATION INFORMATION				
AC-24(2)	NO USER OR PROCESS IDENTITY				
AC-25	Reference Monitor				

AC-2: Account Management



- a) Specificare i tipi di account permessi (individuali, condivisi, di sistema, anonimi, ...).
 - b) Assegnare un manager degli account.
 - c) Richiedere prerequisiti per determinati ruoli.
 - d) Specificare i ruoli e i privilegi d'accesso per ogni tipo di account.
 - e) Avere la possibilità di creare, attivare, modificare, rimuovere account.
 - f) Monitorare l'utilizzo degli account.
 - g) Autorizzare l'accesso al sistema su: (1) un accesso valido; 2) altri attributi dell'organizzazione>.
-

Tramite **keycloak**, è stato possibile specificare due ruoli: **Student** e **Supervisor** ed i permessi ad essi associati.

E' stato poi creato un utente aggiuntivo denominato **Admin** il quale è l'unico che ha i permessi (grazie ai ruoli assegnatogli) per abilitare/disabilitare ed eliminare i vari account.

L' **auditing** è abilitato in keycloak per quanto riguarda gli accessi effettuati e le operazioni realizzate sia per gli utenti non privilegiati che per quelli privilegiati.

AC-2(1): AUTOMATED SYSTEM ACCOUNT MANAGEMENT

Automatizzazione del meccanismo di gestione degli account

L'account Admin ha la possibilità grazie ai ruoli assegnatogli di abilitare/disabilitare ed eliminare i vari account. Assieme all' IAM keycloak viene realizzata la gestione **automatica** degli account.

List Of Users

Users	Informations	Enable/Disable
admin		<input checked="" type="checkbox"/>
cesposito	ciro esposito	<input checked="" type="checkbox"/>
mconti	matteo conti	<input checked="" type="checkbox"/>
vcasola	Valentina Casola	<input checked="" type="checkbox"/>
viasio	vittorio de jasio	<input checked="" type="checkbox"/>

Assigned Roles ⓘ

- [manage-users](#)
- [query-users](#)
- [view-users](#)

[« Remove selected](#)

Name: **Valentina** Surname: **Casola**

Badge Number: **9632587**

Supervisor Contact:

Email	Telefono	BirthDay
v.casola@unina.it	36985258	1970-10-10

[Back](#) [Delete User](#)

*Da notare che all'utente Admin sono stati assegnati solo i ruoli di **realm-management** strettamente necessari a svolgere le sue funzioni.

AC-2(3): DISABLE ACCOUNTS

Disabilitare gli account quando:

- a) Sono scaduti
- b) Non sono più associati a utenti o individui
- c) Violano le policy dell'organizzazione
- d) Sono rimasti inattivi per un certo periodo di tempo

L'utilizzo in congiunzione dell'IAM **Keycloak** e dell'account di **Admin** consente di rispettare il punto **b) c) e d)** procedendo alla disabilitazione degli account corrispondenti

The image shows two screenshots of the Keycloak Admin UI. The top screenshot is a table of active sessions. A session from IP 127.0.0.1, started on Nov 27, 2023 at 4:33:37 PM, is highlighted with a yellow circle around its 'Last Access' timestamp. The bottom screenshot shows the 'Edit User' form for a user named 'Mare'. The 'User Enabled' switch is set to 'ON' (highlighted with a yellow arrow). The 'User Temporarily Locked' and 'Email Verified' switches are both set to 'OFF'.

IP Address	Started	Last Access	Clients	Action
127.0.0.1	Nov 27, 2023 4:33:37 PM	Nov 27, 2023 4:33:37 PM	application-rest-api	Logout

Log out all sessions

Last Name: Mare

User Enabled: ON

User Temporarily Locked: OFF

Email Verified: ON

AC-2(4): AUTOMATED AUDIT ACTIONS

Auditing automatico relativo alla creazione, modifica e cancellazione degli account

Il sistema assieme a Keycloak implementa un meccanismo di **auditing** della gestione degli account tale per cui ciascuna operazione di registrazione, modifica o cancellazione di un account viene **memorizzata**.



Time	Operation Type	Resource Type	Resource Path	Details
11/27/23 4:41:37 PM	DELETE	USER	users/fd64bb7a-84d9-4fb1-af8f-828b05b7c607	<button>Auth</button>
11/27/23 4:41:30 PM	UPDATE	USER	users/5e522376-4a36-4393-97f8-1621ca4b2dfd	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	CLIENT_ROLE_MAPPING	users/5e522376-4a36-4393-97f8-1621ca4b2dfd/role-mappings/clients/7c440cc9-006d-42e0-8080-80a536295332	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	REALM_ROLE_MAPPING	users/5e522376-4a36-4393-97f8-1621ca4b2dfd/role-mappings/realm	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	USER	users/5e522376-4a36-4393-97f8-1621ca4b2dfd	<button>Auth</button>

AC-2(5): INACTIVITY LOGOUT

Logout automatico degli utenti inattivi

Tramite Keycloak è possibile settare il tempo massimo di **"idle"** dopo il quale una sessione viene considerata **expired** invalidando la sessione del browser e i relativi token



SSO Session Idle Minutes

Sia **Keycloak** che l'API Gateway **NGINX** sono stati configurati opportunamente per effettuare anche l'auditing delle varie connessioni così come l'esecuzione di funzionalità privilegiate.

Events Config

Event Listeners

Login Events Settings

Save Events

Saved Types

- SEND_RESET_PASSWORD
- UPDATE_CONSENT_ERROR
- GRANT_CONSENT
- VERIFY_PROFILE_ERROR
- REMOVE_TOTP
- REVOKE_GRANT
- UPDATE_TOTP
- LOGIN_ERROR
- CLIENT_LOGIN
- RESET_PASSWORD_ERROR
- IMPERSONATE_ERROR
- CODE_TO_TOKEN_ERROR
- CUSTOM_REQUIRED_ACTION
- OAUTH2_DEVICE_CODE_TO_TOKEN_ERROR
- RESTART_AUTHENTICATION
- IMPERSONATE
- UPDATE_PROFILE_ERROR
- LOGIN
- OAUTH2_DEVICE_VERIFY_USER_CODE
- UPDATE_PASSWORD_ERROR
- CLIENT_INITIATED_ACCOUNT_LINKING
- TOKEN_EXCHANGE
- AUTHREQID_TO_TOKEN
- LOGOUT
- REGISTER
- DELETE_ACCOUNT_ERROR
- CLIENT_REGISTER
- IDENTITY_PROVIDER_LINK_ACCOUNT
- DELETE_ACCOUNT
- UPDATE_PASSWORD
- CLIENT_DELETE
- FEDERATED_IDENTITY_LINK_ERROR
- IDENTITY_PROVIDER_FIRST_LOGIN
- CLIENT_DELETE_ERROR
- VERIFY_EMAIL
- CLIENT_LOGIN_ERROR
- RESTART_AUTHENTICATION_ERROR
- EXECUTE_ACTIONS

```
access_log /var/log/nginx/all.log combined;
location / {
root /data/www;
if ( $uri = '/index.html' ) {
add_header Cache-Control no-store always;
}
try_files $uri $uri/ /index.html;
}

location /auth {
access_log /var/log/nginx/auth.log combined;
proxy_pass http://mykeycloak:8080;
}

location /api {
access_log /var/log/nginx/backend.log combined;
proxy_pass http://back-end:8081;
proxy_buffers 4 256k;
}

location /admin {
access_log /var/log/nginx/admin-backend.log combined;
proxy_pass http://Admin-back-end:8082;
proxy_buffers 4 256k;
}
```

AC-2(13): DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS

Disabilitare gli utenti entro un certo periodo di tempo quando si presenta un rischio significativo per l'organizzazione

Ancora una volta grazie all'utente **Admin** è possibile immediatamente disabilitare gli account che possono rappresentare un rischio per la sicurezza dell'organizzazione.



List Of Users		
Users	Informations	Enable/Disable
admin		<input checked="" type="checkbox"/>
cesposito	ciro esposito	<input checked="" type="checkbox"/>
mconti	matteo conti	<input checked="" type="checkbox"/>
vcasola	Valentina Casola	<input checked="" type="checkbox"/>
viasio	vittorio de iasio	<input type="checkbox"/>

AC-3: ENFORCEMENT DEGLI ACCESSI

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

Le policy di controllo accessi regolano l'accesso tra le entità o soggetti attivi (utenti, processi) ed oggetti passivi. Allo scopo è stato impiegato **l'IAM Keycloak** integrandolo opportunamente con **Spring Boot** lato back-end per consentire l'accesso alle **API** definite solo agli utenti con uno specifico **ruolo**.

AC-3(5): INFORMAZIONI RILEVANTI PER LA SICUREZZA

Prevenire l'accesso alle informazioni rilevanti per la sicurezza ad eccezioni degli stati sicuri e di non operatività del sistema.

L'applicazione impiega servizi volti a garantire la **protezione** dei dati privati attraverso l'uso di crittografia a livello trasporto per tutte le comunicazioni esterne al perimetro di sicurezza. Inoltre, si avvale di un servizio di Identity and Access Management per assicurare che solo entità **autorizzate** possano accedere alle risorse del sistema.

AC-3(7): ROLE-BASED ACCESS CONTROL

Imporre un criterio di controllo degli accessi basato sui ruoli

L'applicazione impiega il sistema Identity and Access Management Keycloak per implementare il meccanismo di Role-Based Access Control (**RBAC**), una politica di controllo degli accessi che regola l'accesso agli oggetti e alle funzioni del sistema in base al ruolo definito dell'entità interessata. I ruoli attivi nel sistema sono tre, ovvero **Supervisor**, **Student** e **Admin** per accedere a risorse e funzionalità distinte.

The screenshot shows the 'Roles' management screen in Keycloak. At the top, there are tabs for 'Realm Roles' and 'Default Roles', with 'Realm Roles' being selected. Below the tabs is a search bar labeled 'Search...' with a magnifying glass icon, and a 'View all roles' button. A table lists three roles:

Role Name	Composite
ROLE_ADMIN	True
ROLE_STUDENTE	False
ROLE_SUPERVISOR	False

AC-4: ENFORCEMENT DEL FLUSSO DI INFORMAZIONI

Impiegare meccanismi di autorizzazione per proteggere il flusso di informazioni all'interno del sistema e tra sistemi diversi connessi.

Il flusso di dati proveniente dal client verso il Back-end dell'applicazione viene protetto utilizzando il protocollo **TLS** ottenendo confidenzialità e autenticità alle richieste verso le varie **API**.

In particolare i tentativi di connessione non sicura usando **HTTP** vengono reindirizzati dall'Entry Point dell'applicazione **Nginx** verso la porta **443** per impiegare il protocollo **HTTPS**.

```
server {  
  
    include /etc/nginx/mime.types;  
    listen      443 ssl;  
    server_name bandiunina.it;  
  
    ssl_certificate      /etc/letsencrypt/live/bandiunina.it/fullchain.pem;  
    ssl_certificate_key  /etc/letsencrypt/live/bandiunina.it/privkey.pem;  
  
    add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;  
    #add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src * data:;";  
    add_header X-XSS-Protection: "1; mode=block";  
  
    proxy_set_header X-Forwarded-For $proxy_protocol_addr;  
    proxy_set_header X-Forwarded-Proto $scheme;  
    proxy_set_header Host $host;
```

AC-5: SEPARAZIONE DEI COMPITI

Definire meccanismi per supportare la separazione dei compiti tra diversi utenti o ruoli

Come accennato nell'introduzione, il Sistema prevede la definizione di due classi di utenti distinte, identificate rispettivamente nel ruolo di **Supervisor** e di **Studente**.

L'insieme delle funzionalità a cui i ruoli hanno accesso sono completamente **disgiunti**.

L'obiettivo è affrontare il potenziale abuso dei privilegi e ridurre il rischio di attività malevola. Inoltre le funzionalità associate all'utente **Admin** sono state implementate in un back-end **separato** anch'esso dockerizzato.

Ad esempio un Supervisor può creare un nuovo Bando, vedere le “applications” per i Bandi da lui creati, accettare o rifiutare queste ultime; mentre uno studente può visualizzare i Bandi aperti, fare application e visionare lo stato di quest'ultima.

Roles	
Realm Roles	Default Roles
<input type="text" value="Search..."/>	<input type="button" value="View all roles"/>
Role Name	Composite
ROLE_ADMIN	True
ROLE_STUDENTE	False
ROLE_SUPERVISOR	False

```
.antMatchers("/api/callForApplications/student/**").hasRole("STUDENTE")
.antMatchers("/api/participations/student/**").hasRole("STUDENTE")

.antMatchers("/api/callForApplications/supervisor/**").hasRole("SUPERVISOR")
.antMatchers("/api/participations/supervisor/**").hasRole("SUPERVISOR")
```

AC-6: PRIVILEGIO MINIMO

Ciascun utente deve poter svolgere solo le azioni necessarie per i compiti organizzativi assegnati.

L'intera applicazione è stata sviluppata seguendo questo **requisito** facendo sì che agli utenti con uno specifico **ruolo** siano consentite solo le operazioni e l'accesso alle API desiderate. In particolare il principio del **minimo privilegio** viene applicato anche ai processi di sistema, assicurando che essi operino a livelli di privilegio non superiori a quelli necessari per compiere le missioni organizzative o funzioni aziendali.

AC-6(1): ACCESSO AUTORIZZATO A FUNZIONI DI SICUREZZA

Autorizzare l'accesso alle funzioni di sicurezza(hardware, software, firmware) e alle informazioni rilevanti alla sicurezza.

Le funzioni di sicurezza gestiscono account e autorizzazioni, monitorano eventi e definiscono parametri di rilevamento. Le informazioni di sicurezza comprendono regole di filtraggio, configurazioni dei servizi, gestione chiavi e elenchi di controllo. Tali funzioni ed informazioni sono accessibili e manipolabili solo agli **sviluppatori** e tramite la console offerta da **Keycloak**, dunque inaccessibili agli utenti generici.

AC-6:(2): ACCESSO NON PRIVILEGIATO A FUNZIONALITA' NON CRITICHE

Richiedere che gli utenti di sistema utilizzino account o ruoli non privilegiati, quando accedono a funzioni non di sicurezza.

Chiaramente ad un utente generico potrà essere assegnato solo il ruolo di **Studente** o **Supervisore** per l'accesso alle funzionalità loro richieste (**non critiche**) ma non a quelle privilegiate.

AC-6(5): ACCOUNT PRIVILEGIATI

Restringere gli account privilegiati a personale o utenti esclusivi.

Solo l'utente **Admin** con l'omonimo ruolo ha accesso alla funzione privilegiata di **rimozione** e **abilitazione/disabilitazione** degli account di sistema.

AC-6(7): REVISIONE DEI PRIVILEGI DEGLI UTENTI

Restringere gli account privilegiati a personale o utenti esclusivi.

In fase di specifica dei requisiti e di progettazione del sistema è stata effettuata un'attenta **valutazione** dei privilegi associati a ciascun ruolo e delle relative funzionalità. E' ad ogni modo possibile **riassegnare** o **rimuovere** i privilegi, se necessario, per riflettere correttamente la missione organizzativa e le esigenze aziendali.

AC-6:(9): LOGGARE L'USO DI FUNZIONI PRIVILEGIATE

Le operazioni considerate privilegiate come la creazione di nuovi utenti del sistema vengono opportunamente **registerate** mediante l'abilitazione di un meccanismo **automatico** da parte di **Keycloak**.



Time	Operation Type	Resource Type	Resource Path	Details
11/27/23 4:41:37 PM	DELETE	USER	users/fd64bb7a-84d9-4fb1-af8f-828b05b7c607	<button>Auth</button>
11/27/23 4:41:30 PM	UPDATE	USER	users/5e522376-4a36-4393-97f8-1621ca4b2dfd	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	CLIENT_ROLE_MAPPING	users/5e522376-4a36-4393-97f8-1621ca4b2dfd/role-mappings/clients/7c440cc9-006d-42e0-8080-80a536295332	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	REALM_ROLE_MAPPING	users/5e522376-4a36-4393-97f8-1621ca4b2dfd/role-mappings/realm	<button>Auth</button>
11/27/23 4:41:19 PM	CREATE	USER	users/5e522376-4a36-4393-97f8-1621ca4b2dfd	<button>Auth</button>

AC-6:(10): VIETARE AD UTENTI NON PRIVILEGIATI L'ESECUZIONE DI FUNZIONI PRIVILEGIATE

Solo all'utente Admin al quale è stato assegnato il ruolo di **Admin** è possibile accedere alle API associate all'esecuzione di funzioni **privilegiate**. Il tentativo di accesso a tali API dagli utenti non appartenenti al ruolo specificato verrà bloccato e segnalato con un errore "**403 Forbidden**" direttamente da Keycloak.



```
.antMatchers("/api/admin/user/**").hasRole("ADMIN")
.antMatchers("/api/student/delete/**").hasRole("ADMIN")
.antMatchers("/api/supervisor/delete/**").hasRole("ADMIN")
```

AC-7: TENTATIVI DI ACCESSO FALLITI

- a) Imporre un limite definito di tentativi di login falliti da parte di un utente avvenuti in un certo periodo di tempo
- b) Effettuare, automaticamente, il blocco dell'account per un tempo definito e notificare l'amministratore di sistema

E' possibile configurare **Keycloak** per imporre un **limite** massimo al numero di tentativi di login **falliti**.

In particolare nel nostro caso è stato imposto un limite di **5 tentativi**, dopo il quale l'account viene bloccato per almeno **5 minuti** fino ad un massimo di **1 ora**.

Inoltre al trascorrere di **24 ore** il contatore relativo al numero di tentativi di login fallimentari viene azzerato. E' possibile impostare anche una soglia temporale per implementare una forma di protezione contro tentativi di login automatici "**Quick**" nel nostro caso pari a **500 millisecondi** che triggerà un'attesa di **5 minuti**.

Enabled	<input checked="" type="checkbox"/>
Permanent Lockout	<input type="checkbox"/> OFF
Max Login Failures	5
Wait Increment	5 Minutes
Quick Login Check Milli Seconds	500
Minimum Quick Login Wait	5 Minutes
Max Wait	15 Minutes
Failure Reset Time	12 Hours
<input type="button"/> Save <input type="button"/> Cancel	

AC-7: TENTATIVI DI ACCESSO FALLITI

Riportiamo di seguito il log offerto da Keycloak a seguito dell'abilitazione del meccanismo appena descritto effettuando vari tentativi di login falliti.



17:28:51,687 **WARN** [org.keycloak.services] (Brute Force Protector) KC-SERVICES0053: **login failure** for user 93f1556e-f73e-4f27-807f-5d0ceec9097e from ip X.X.X.X



17:28:51,690 **WARN** [org.keycloak.events] (default task-5) type=**LOGIN_ERROR**, realmId=SSD_REALM, clientId=application-rest-api, userId=93f1556e-f73e-4f27-807f-5d0ceec9097e, **error=invalid_user_credentials**, auth_method=openid-connect, auth_type=code, code_id=617fe08c-5d46-4684-80b5-c79eb2d5811c, username=vcasola,



17:29:00,681 **WARN** [org.keycloak.events] (default task-5) type=**LOGIN_ERROR**, realmId=SSD_REALM, clientId=application-rest-api, userId=93f1556e-f73e-4f27-807f-5d0ceec9097e,, **error=user_temporarily_disabled**, auth_method=openid-connect, auth_type=code, , code_id=617fe08c-5d46-4684-80b5-c79eb2d5811c, username=vcasola,

AC-8: NOTIFICHE SULL'UTILIZZO DEL SISTEMA

a) Mostrate un *banner* o messaggio di notifica agli utenti prima di garantire loro accesso al sistema che fornisca avvisi sulla privacy e sulla sicurezza in conformità con le leggi applicabili, gli ordini esecutivi, le direttive, i regolamenti, le politiche, gli standard e le linee guida.

Informare inoltre che l'utilizzo del sistema può essere monitorato, registrato e soggetto a revisione.

b) Mantenere il messaggio di notifica o il banner sullo schermo fino a quando gli utenti non riconoscono e accettano le condizioni di utilizzo

The screenshot shows a Terms and Conditions page with a light gray background. At the top right, the title "Terms and Conditions" is displayed in bold black font. Below it, a welcome message reads: "Welcome to our Terms and Conditions. Please read carefully the following rules governing your use of our service." A note indicates the last update date: "Last updated: December 12, 2022". A instruction for users follows: "Please read these terms and conditions carefully before using Our Service." On the right side, there is a section titled "Interpretation and Definitions". Under this, the "Interpretation" heading is defined as: "The words of which the initial letter is capitalized have meanings defined under the following conditions. The following definitions shall have the same meaning regardless of whether they appear in singular or in plural." The "Definitions" section lists several terms with their meanings:

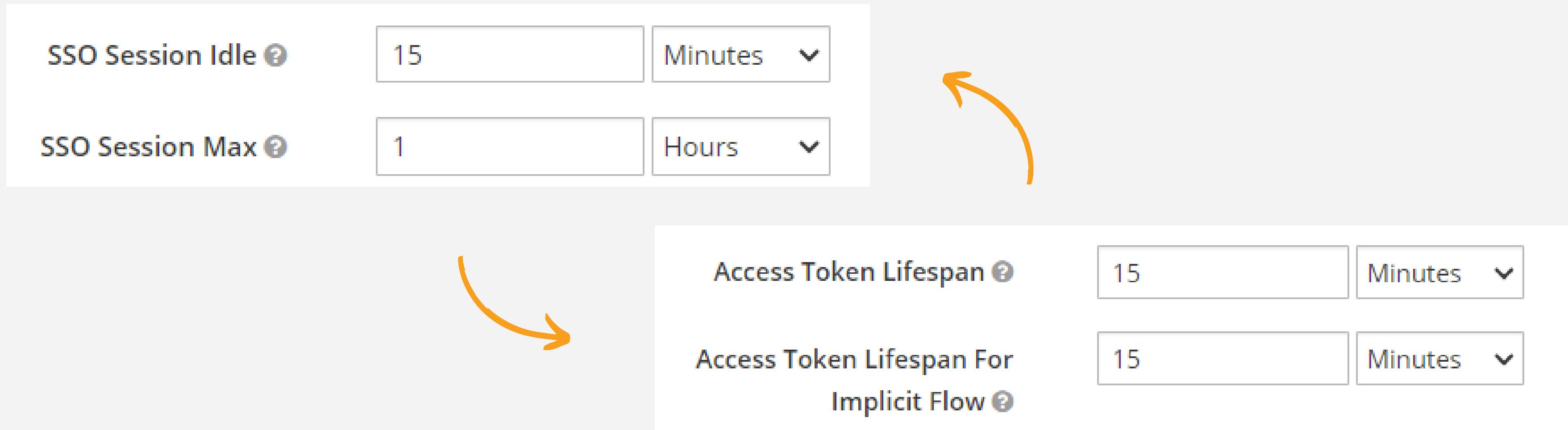
- Affiliate**: means an entity that controls, is controlled by or is under common control with a party, where "control" means ownership of 50% or more of the shares, equity interest or other securities entitled to vote for election of directors or other managing authority.
- Country**: refers to: Italy
- Company**: (referred to as either "the Company", "We", "Us" or "Our" in this Agreement) refers to UninaBandi Online, Piazzale Tecchio Napoli.
- Device**: means any device that can access the Service such as a computer, a cellphone or a digital tablet.
- Service**: refers to the Website.

Ciascun utente, a seguito della registrazione e all'atto del primo **Log-in** all'interno dell'applicazione è obbligato a prendere **visione** e ad **accettare i termini e le condizioni d'uso**.

AC-12: TERMINAZIONE DELLA SESSIONE UTENTE

Terminare automaticamente una sessione utente dopo condizioni definite dall'organizzazione o eventi che richiedono una disconnessione

Tramite Keycloak è possibile impostare un durata massima di **15 minuti** per una sessione, al trascorrere dei quali l'IAM **invalida** la sessione applicativa. Quest'ultima, può, in ogni caso, rimanere attiva per un massimo di **1 ora**.



AC-12(1): LOGOUT INIZIATI DALL'UTENTE

Fornire una capacità di disconnessione per le sessioni di comunicazione avviate dall'utente



Ovviamente l'applicazione fornisce la funzione
di **logout** a seguito di un'autenticazione
avvenuta con successo tramite l'apposito

bottone inserito nella **Navbar** di ciascun utente.

In particolare viene effettuata un richiesta
esplicita a Keycloak per la disconnessione che
risulta, in seguito al **button-click**, invalidata.



AC-14: AZIONI PERMESSE SENZA IDENTIFICAZIONE O AUTENTICAZIONE

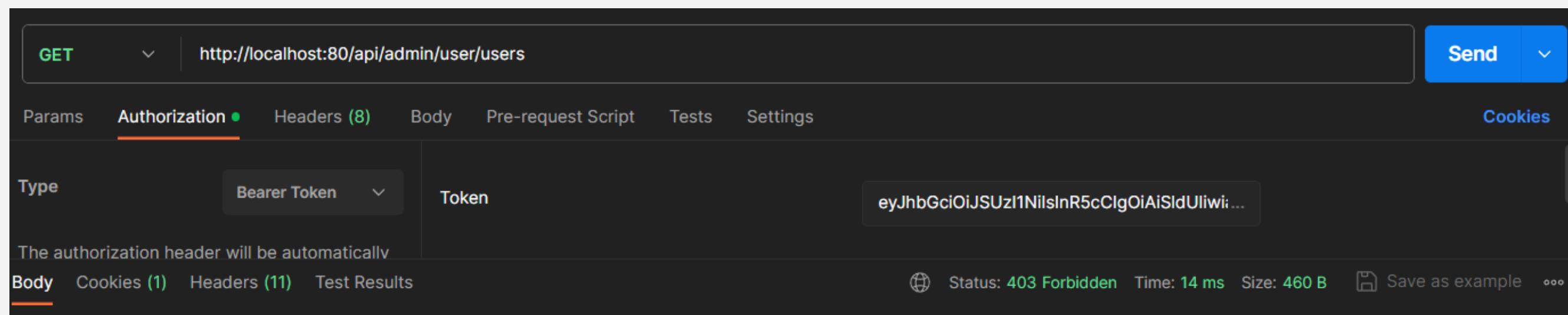
Identificazione e documentazione delle user action che possono essere effettuate sul sistema senza identificazione o autenticazione

Tutte le funzionalità effettive offerte dal sistema necessitano di autenticazione.

Un utente privo di **autenticazione** ed **identificazione** è solo in grado di visualizzare la pagina di **Home** che mostra gli ultimi due bandi di partecipazione pubblicati, mentre in termini di funzionalità dell'applicazione, l'unica offerta a tale categoria di utenti è quella di **Login** e **Registrazione**.

Qualsiasi altro tentativo di accesso alle API esposte senza un opportuno token di autenticazione sarà rifiutata con un messaggio di tipo **“403 Forbidden”**.

```
.authorizeRequests()  
.antMatchers(HttpMethod.POST, "/api/guest/register/*").permitAll()
```

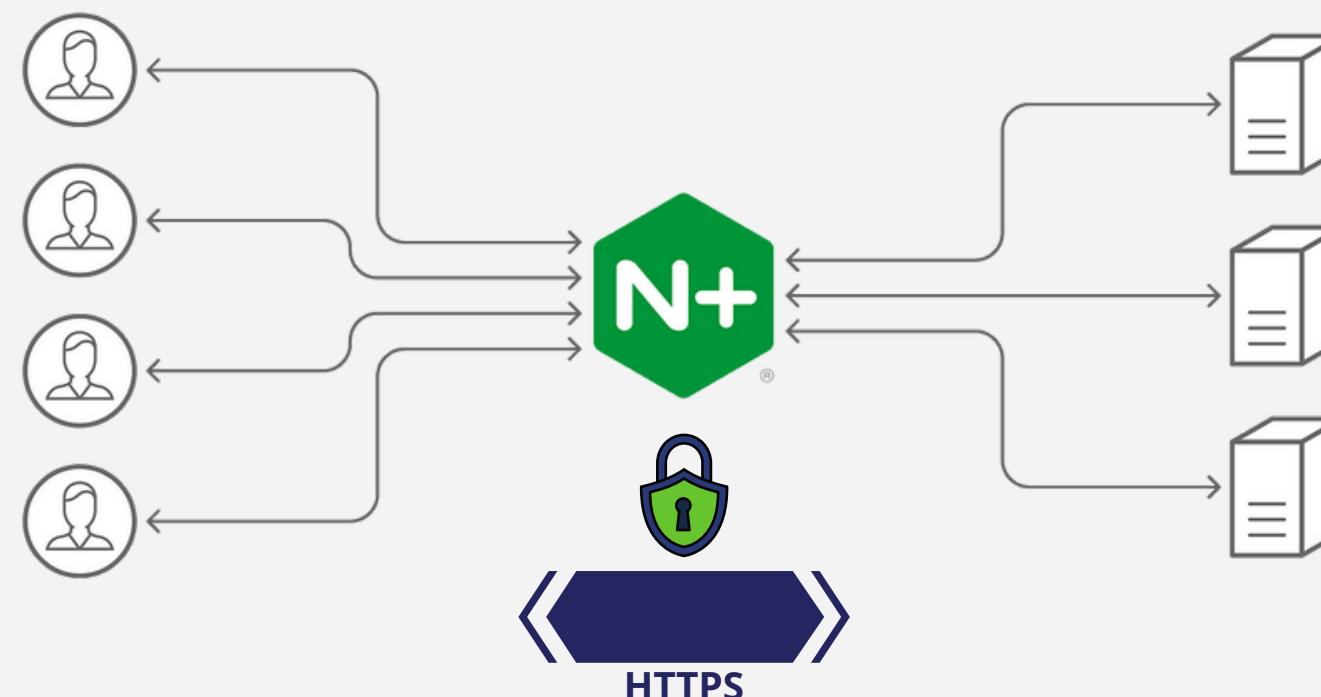


AC-17: ACCESSO DA REMOTO

- a) Stabilire le restrizioni d'uso e i requisiti di connessione per ogni tipo di accesso remoto consentito
 - b) Autorizzare ogni tipo di accesso remoto al sistema prima di consentire tali connessioni.
-

L'integrità e la confidenzialità delle interazioni degli utenti esterni con il sistema sono garantite attraverso l'implementazione di un tunnel crittografico **TLS**. Tutte le connessioni HTTP vengono reindirizzate verso connessioni **HTTPS** al fine di prevenire interazioni non sicure col sistema.

L'accesso alle risorse fornite dal sistema avviene esclusivamente attraverso l'**API Gateway**, che rappresenta il solo punto autorizzato per l'interfacciamento tra il client e il sistema. Quest'ultimo è responsabile anche della registrazione di tutte le richieste effettuate. Inoltre, le API REST associate ai servizi forniti dal backend sono vincolate a percorsi **protetti** in base al ruolo dell'utente che effettua la richiesta.



AC-17(1): MONITORAGGIO E CONTROLLO

Impiegare meccanismi automatizzati per monitorare e controllare i metodi di accesso remoto.

Tutte le attività di **accesso remoto** ai servizi della logica di business e a Keycloak sono registrati dai rispettivi componenti di **logging**.



AC-17(2): ACCOUNT PRIVILEGIATI

Implementare meccanismi crittografici per proteggere la confidenzialità e l'integrità delle sessioni di accesso remoto

Per garantire la **confidenzialità** e **l'integrità** delle comunicazioni con l'esterno viene utilizzato il protocollo **TLS** (Transport Layer Security).

AC-17(3): MANAGED ACCESS CONTROL POINTS

Instrandare gli accessi remoti attraverso i punti di controllo degli accessi di rete autorizzati e gestiti.

Come già ribadito in precedenza l'API Gateway rappresenta l'**unico punto di accesso** per le richieste verso il backend dell'applicazione **dirottando** opportunamente le connessioni non sicure verso connessioni TLS.

AC-17(4): ACCESSI E COMANDI PRIVILEGIATI

- (a) Autorizzare l'esecuzione di comandi privilegiati e l'accesso alle informazioni rilevanti per la sicurezza tramite accesso remoto solo in un formato che fornisca prove verificabili e per le seguenti esigenze: [esigenze definite dall'organizzazione];
 - (b) Documentare le motivazioni dell'accesso remoto nel piano di sicurezza del sistema.
-

Le attività di accesso ed esecuzione remota di comandi privilegiati in termini di sicurezza sono state tracciate e registrate opportunamente dai componenti di logging come descritto nella famiglia di controlli **AU**.

Overview e ulteriori Controlli

“Access Control” controls family

NIST Risk Management Framework SP 800-53 Rev. 5.1

I controlli applicati seguendo le linee guida definite dal NIST consentono di raggiungere una protezione del sistema complessivo fino ad un livello moderate, eccezion fatta per :

Controlli non realizzati:

- **AC-2(2)** : Gestione automatica degli account temporanei e di emergenza

Controlli non implementabili:

- **AC-11**: Blocco del dispositivo
- **AC-19**: Controllo Accessi per dispositivi mobili
- **AC-18**: Accesso Wireless
- **AC-20**: Utilizzo di sistemi esterni
- **AC-21**: Condivisione di informazioni
- **AC-22**: Contenuti accessibili pubblicamente

8. “Identification and Authentication” Control Family

NIST Risk Management Framework SP 800-53 Rev. 5.1

- I controlli di sicurezza della famiglia “identification and authentication” implementati per **Bandiunina** permettono di raggiungere il **livello low** nell’ambito della sicurezza delle operazioni di identificazione e autenticazione nel sistema informatico.
-

La famiglia di controlli IA è stata selezionata per mitigare le **minacce** di:

- **Repudiation** - *A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions* [Open Worldwide Application Security Project]
- **Elevation of Privilege** - *Privilege escalation occurs when a user gets access to more resources or functionality than they are normally allowed, and such elevation or changes should have been prevented by the application* [Open Worldwide Application Security Project]
- **Information Disclosure** - *The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information* [MITRE CWE]

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
IA-5(2)	PUBLIC KEY-BASED AUTHENTICATION			X	X
IA-5(3)	IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION		W: Incorporated into IA-12(4).		
IA-5(4)	AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION		W: Incorporated into IA-5(1).		
IA-5(5)	CHANGE AUTHENTICATORS PRIOR TO DELIVERY				
IA-5(6)	PROTECTION OF AUTHENTICATORS			X	X
IA-5(7)	NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS				
IA-5(8)	MULTIPLE SYSTEM ACCOUNTS				
IA-5(9)	FEDERATED CREDENTIAL MANAGEMENT				
IA-5(10)	DYNAMIC CREDENTIAL BINDING				
IA-5(11)	HARDWARE TOKEN-BASED AUTHENTICATION		W: Incorporated into IA-2(1) and IA-2(2).		
IA-5(12)	BIOMETRIC AUTHENTICATION PERFORMANCE				
IA-5(13)	EXPIRATION OF CACHED AUTHENTICATORS				
IA-5(14)	MANAGING CONTENT OF PKI TRUST STORES				
IA-5(15)	GSA-APPROVED PRODUCTS AND SERVICES				
IA-5(16)	IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE				
IA-5(17)	PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS				
IA-5(18)	PASSWORD MANAGERS				
IA-6	Authentication Feedback		X	X	X
IA-7	Cryptographic Module Authentication		X	X	X
IA-8	Identification and Authentication (Non-Organizational Users)		X	X	X
IA-8(1)	ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES		X	X	X
IA-8(2)	ACCEPTANCE OF EXTERNAL AUTHENTICATORS		X	X	X
IA-8(3)	USE OF FICAM-APPROVED PRODUCTS		W: Incorporated into IA-8(2).		
IA-8(4)	USE OF DEFINED PROFILES		X	X	X
IA-8(5)	ACCEPTANCE OF PIV-I CREDENTIALS				
IA-8(6)	DISASSOCIABILITY				
IA-9	Service Identification and Authentication				
IA-9(1)	INFORMATION EXCHANGE		W: Incorporated into IA-9.		
IA-9(2)	TRANSMISSION OF DECISIONS		W: Incorporated into IA-9.		
IA-10	Adaptive Authentication				
IA-11	Re-authentication		X	X	X
IA-12	Identity Proofing			X	X
IA-12(1)	SUPERVISOR AUTHORIZATION				
IA-12(2)	IDENTITY EVIDENCE			X	X
IA-12(3)	IDENTITY EVIDENCE VALIDATION AND VERIFICATION			X	X
IA-12(4)	IN-PERSON VALIDATION AND VERIFICATION				X
IA-12(5)	ADDRESS CONFIRMATION			X	X
IA-12(6)	ACCEPT EXTERNALLY-PROOFED IDENTITIES				

IA-2 Identification and Authentication (Organizational Users)

- **IA-2: Le organizzazioni devono utilizzare password, autenticatori fisici o biometrici per autenticare le identità degli utenti o, nel caso di autenticazione a più fattori, combinazioni tra essi.**

Gli utenti, tramite Keycloak, effettuano il login utilizzando la coppia **username** e **password** che li identifica univocamente. Il web client riceve (in risposta ad una richiesta di log-in andata a buon fine) un token di autenticazione da presentare al web server.

The screenshot shows a 'Sign Up' form with the following fields:

- User Name: A text input field with placeholder text "Enter Username".
- ... (Ellipsis indicating more fields)
- Password: A text input field with placeholder text "Password".
- Confirm Password: A text input field with placeholder text "Password".
- Non sono un robot: A checkbox labeled "Non sono un robot".
- reCAPTCHA: A reCAPTCHA interface with a checkbox and the text "Privacy - Termini".
- Create Account: A blue button labeled "Create Account".
- Already have an account?? [Sign In](#): Text at the bottom of the form.

```
{
  "exp": 1700666207,
  "iat": 1700666147,
  "auth_time": 1700666136,
  "jti": "e14d410a-2eac-4516-8e52-37c5d9dff8ec",
  "iss": "http://localhost:9000/auth/realms/SSD_REALM",
  "aud": "account",
  "sub": "93f1556e-f73e-4f27-807f-5d0ceec9097e",
  "typ": "Bearer",
  "azp": "application-rest-api",
  "nonce": "8422035b-0169-4e6b-816e-7ee716aac159",
  "session_state": "e720ab19-d0b1-453a-83cb-7eb353bd1701",
  "acr": "0",
  "allowed_origins": [
    "*"
  ],
  "realm_access": {
    "roles": [
      "offline_access",
      "uma_authorization",
      "default-roles-ssd_realm",
      "ROLE_SUPERVISOR"
    ]
  },
  "resource_access": {
    "application-rest-api": {
      "roles": [
        "ROLE_SUPERVISOR"
      ]
    }
  },
  "account": {
    "roles": [
      "manage-account",
      "manage-account-links",
      "view-profile"
    ]
  }
}.
```

- IA-2 (1): Implementare un meccanismo di autenticazione multi-fattore di account privilegiati
- IA-2 (2): Implementare un meccanismo di autenticazione multi-fattore di account non privilegiati

L'autenticazione multi-fattore è obbligatoria per tutti gli utenti dell'applicazione: è richiesta l'immissione della coppia username-password e di una **one-time password** generata dalla app **Google Authenticator**. L'associazione di un dispositivo per la generazione di OTPs è effettuata al primo login dell'utente, dopo la quale sarà possibile generare una OTP per ogni login (utilizzando il dispositivo associato).

Authentication

Flows Bindings Required Actions Password Policy

OTP Policy WebAuthn Policy

WebAuthn Passwordless Policy CIBA Policy

Required Action	Enabled	Default Action
Configure OTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Register

La OTP è un codice pseudo-casuale generato utilizzando un algoritmo sicuro. Le effettive caratteristiche possono essere configurate direttamente in keycloak



Authentication

Flows Bindings Required Actions Password Policy

OTP Policy WebAuthn Policy

WebAuthn Passwordless Policy CIBA Policy

OTP Type Time Based

OTP Hash Algorithm SHA1

Number of Digits 6

Look Ahead Window 1

OTP Token Period 30

Supported Applications FreeOTP, Google Authenticator

1. Associazione Dispositivo

Dopo la **registrazione**, al primo tentativo di log-in, l'utente dovrà effettuare il **set-up** di un dispositivo per la generazione di OTPs (scansionando, tramite Google Authenticator, un **QR-code** con il dispositivo da associare all'account ed assegnandogli un "*device name*")

Mobile Authenticator Setup

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

1. Install one of the following applications on your mobile:
FreeOTP
Google Authenticator
2. Open the application and scan the barcode:



Unable to scan?

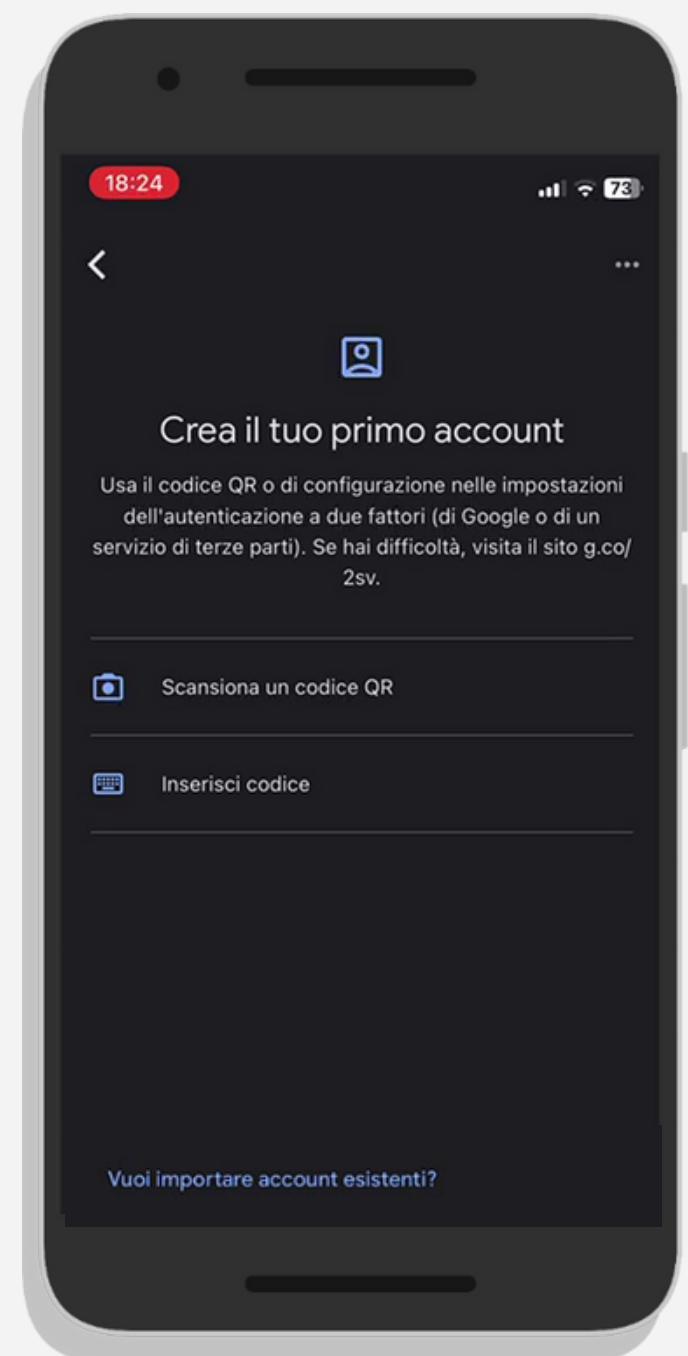
3. Enter the one-time code provided by the application and click Submit to finish the setup.

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

One-time code *

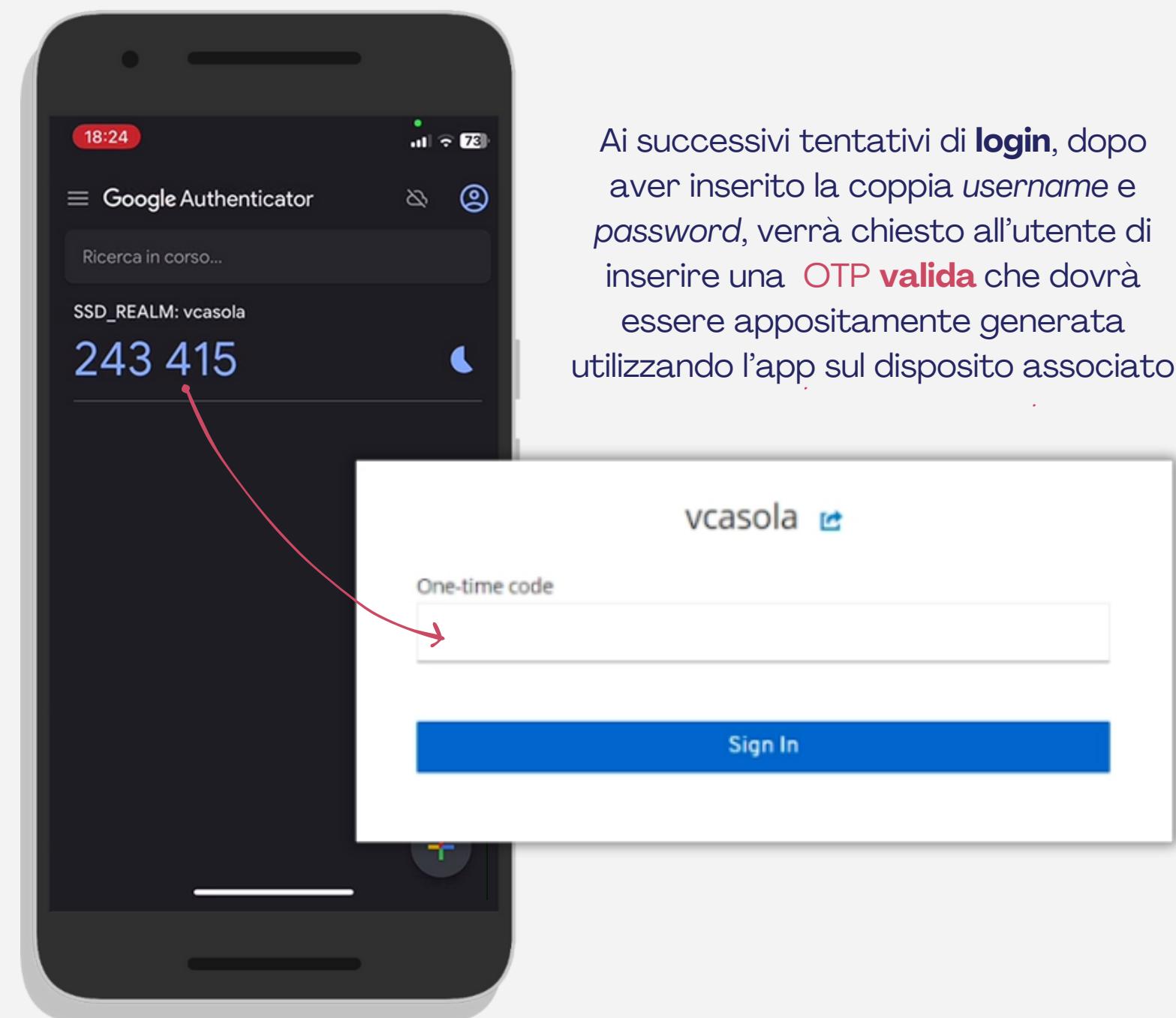
Device Name

Submit



2. Generazione ed inserimento OTP

L'utente, dopo aver associato un dispositivo, dovrà generare una **OTP** tramite la app (dal dispositivo precedentemente associato) per potersi **autenticare** nel sistema informatico, inserendo la OTP generata nel form di set-up del **Mobile Authenticator**



Ai successivi tentativi di **login**, dopo aver inserito la coppia *username* e *password*, verrà chiesto all'utente di inserire una **OTP valida** che dovrà essere appositamente generata utilizzando l'app sul dispositivo associato

Azioni necessarie alla registrazione...

Oltre alla **configurazione della OTP**, l'utente all'atto della registrazione dovrà anche **Accettare termini e condizioni** dell'utilizzo del servizio e verificare il possesso dell'indirizzo di **posta elettronica** inserito (tramite conferma via e-mail)

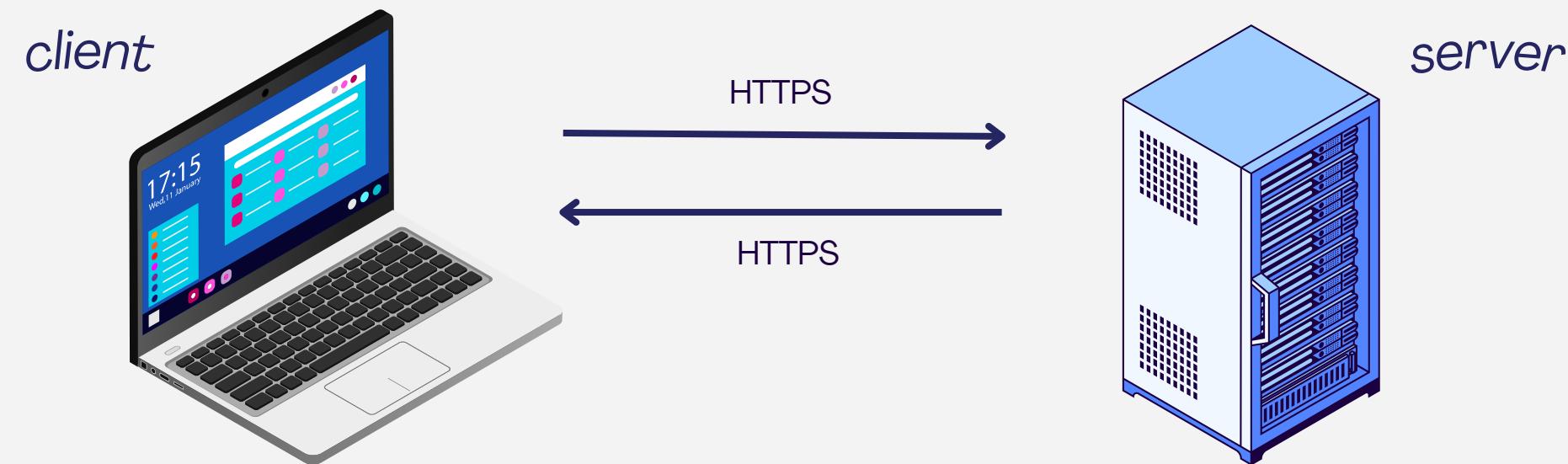
Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy ⓘ WebAuthn Passwordless Policy ⓘ CIBA Policy

Required Action	Enabled	Default Action ⓘ	Register
Configure OTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Terms and Conditions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Update Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Update Profile	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Verify Email	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Delete Account	<input type="checkbox"/>	<input type="checkbox"/>	
Update User Locale	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

- IA-2 (8): Implementare meccanismi di autenticazione resistenti al replay (reply-resistant) per l'accesso ad account privilegiati e non privilegiati.
-

Il traffico da e verso la web-app è incapsulato in pacchetti **HTTPS**, i quali si basano sul protocollo di livello trasporto **TLS** (Transport Layer Security). Alla creazione di un canale di comunicazione gli end-point si scambiano un *nonce* che impedisce il replay di pacchetti in una sessione differente.



Inoltre il processo di autorizzazione dello standard **OpenID Connect (OIDC)** impiega lo scambio di un *nonce* (valido dunque una solo una volta) per la richiesta a Keycloak del rilascio del **session token** e dell'**access token**.



IA-3 Device Identification and Authentication

- IA-3: Identificare e autenticare in modo univoco i dispositivi e/o tipi di dispositivi definiti prima di stabilire una connessione.

Il meccanismo di autenticazione, implementato tramite keycloak, associa univocamente ai token di accesso (access token) l'**indirizzo IP** del dispositivo da cui è effettuata l'autenticazione (impedendo tentativi di autenticazione da un indirizzo IP distinto da quello associato al token)

The screenshot shows the Keycloak application interface for the 'Application-rest-api' client. The top navigation bar includes links for Settings, Keys, Roles, Client Scopes, Mappers, Scope, Revocation, Sessions (which is currently selected), Offline Access, and Installation. Below the navigation bar, a section titled 'Active Sessions' displays a count of 2. A table lists two active sessions:

User	From IP	Session Start
rcanonico	192.168.192.8	Dec 15, 2023 10:00:44 AM
antoniomare	192.168.192.8	Dec 15, 2023 10:02:54 AM

A 'Show Sessions' button is located in the bottom right corner of the session table.

IA-4 Identifier Management

- **IA-4: Assegnare un identificativo univoco ad ogni account associandolo all'individuo che lo utilizza. Prevenire il riuso di identificativi.**
-

Alla registrazione di un utente al sistema informatico, a quest'ultimo viene chiesto di inserire un nome utente (o **username**) univoco. Dunque, nel caso in cui lo username inserito fosse già identificativo di un altro utente, la registrazione non andrà a buon fine e l'individuo dovrà reinserire un nuovo username (finché non risulterà disponibile).

Inoltre anche ulteriori caratteristiche degli utenti (non admin) sono considerate univoche nel sistema informatico: l'**indirizzo di posta elettronica**, il **numero telefonico** e la **matricola** (nel caso dello studente, mentre nel caso di un supervisore si tratta del **numero di badge**).

Il controllo della univocità dello username, della e-mail e del numero di telefono è effettuato dall'IAM **Keycloak**, mentre il controllo sulla matricola (ma in effetti anche sugli altri campi univoci) è effettuato dal **DBMS** del database MySQL (i campi corrispondenti nel db sono settati appositamente ad univoci)

IA-4(4): Gestire l'identità degli individui identificandoli univocamente attraverso il loro status all'interno dell'organizzazione, dunque come: studente, supervisore o admin.

Gli utenti sono identificati univocamente all'interno del sistema informatico a partire dal proprio **ruolo** all'interno dell'organizzazione (ovvero, in tal caso, dell'*Università di Napoli Federico II*). In particolare: uno **“studente”** è un individuo correttamente iscritto ad uno dei corsi di laurea dell'ateneo, un **“supervisore”** è un individuo avente il ruolo di dipendente all'interno dell'ateneo e che è incaricato della gestione dei bandi di concorso offerti dall'ateneo, ed infine un **“amministratore”** è un individuo dipendente dell'ateneo che ha il compito di gestire svariati aspetti (precedentemente descritti) del sistema informatico.



IA-5 Authenticator management

IA-5: Gestire l'autenticatore in modo tale da:

- 1. Verificare, come parte della distribuzione iniziale dell'autenticatore, l'identità dell'individuo, del gruppo, del ruolo, del servizio o del dispositivo che riceve l'autenticatore;**
- 2. Stabilire il contenuto iniziale dell'autenticatore per tutti gli autenticatori emessi dall'organizzazione;**
- 3. Assicurarsi che gli autenticatori abbiano una sufficiente robustezza del meccanismo per il loro uso previsto;**
- 4. Stabilire ed implementare procedure amministrative per la distribuzione iniziale dell'autenticatore, per autenticatori persi, compromessi o danneggiati, e per revocare autenticatori;**
- 5. Cambiare gli autenticatori predefiniti prima del primo utilizzo;**
- 6. Cambiare o rinnovare gli autenticatori quando vengono smarriti;**
- 7. Proteggere il contenuto dell'autenticatore da divulgazioni e modifiche non autorizzate;**
- 8. Richiedere agli individui di adottare, e far implementare ai dispositivi, controlli specifici per proteggere gli autenticatori;**
- 9. Cambiare gli autenticatori per gli account di gruppo o di ruolo quando cambia l'appartenenza a tali account.**

La autenticazione per **Bandiunina** è realizzata attraverso l'utilizzo di password (una password utente ed una OTP, come detto in precedenza). La gestione dell'autenticatore è effettuata interamente dall'IAM scelto, ovvero keycloak.

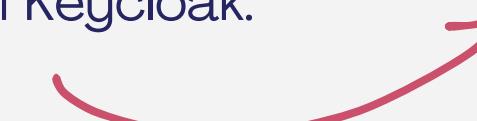
1. La **verifica** dell'individuo al momento della assegnazione dell'autenticatore è effettuata grazie alla verifica tramite indirizzo di posta elettronica
2. Il contenuto iniziale dell'autenticatore è stabilito dall'utente in fase di registrazione
3. La **robustezza** degli autenticatori è gestita da keycloak ed è configurabile dall'admin dell'IAM. Difatti è possibile specificare in keycloak delle **policy** di validazione di una nuova password che devono essere verificate (policy come lunghezza minima, caratteri speciali etc..)
4. La **distribuzione** iniziale degli autenticatori, e la **gestione** in caso di autenticatore perso/dimenticato è a carico dell'IAM.
5. Non sono presenti autenticatori predefiniti
6. E' possibile ottenere una nuova password (tramite posta elettronica) se la precedente viene dimenticata
7. La **protezione** degli autenticatori da modifiche non autorizzate e divulgazioni è garantita dalle caratteristiche di sicurezza della web-app e dell'IAM stesso. Anzitutto la comunicazione verso la web-app avviene su **TLS**. Inoltre le password non vengono memorizzate in chiaro: prima della memorizzazione o della convalida, Keycloak codifica le password utilizzando un **algoritmo di hash** "salted" standard: **PBKDF2** è l'unico algoritmo integrato e predefinito disponibile [Keycloak Administration Guide]
8. Gli individui utilizzano dispositivi personali per l'autenticazione a doppio fattore.
9. Nel caso in cui fosse necessario un **cambio di ruolo** sarà necessario eliminare l'account relativo e di conseguenza anche l'autenticatore (a carico dell'amministratore dell'IAM). Tuttavia non è prevista per l'applicazione in questione la possibilità di cambio di ruolo degli utenti.

IA-5(1): Per autenticazione basata su password

IA-5 (1): Per l'autenticazione basata su password: Le password scelte dagli utenti non devono far parte di dizionari di password vulnerabili. Le password devono essere trasportate su canali protetti crittograficamente. La memorizzazione delle password deve essere gestita in maniera sicura. Bisogna definire regole di complessità delle password.

Innanzitutto il client browser viene redirezionato dal front-end della web-app verso la pagina di registrazione/login offerta da keycloak, dunque le password viaggiano dall'end-point client all'end-point server su canale protetto crittograficamente (in un canale **TLS**). Inoltre la memorizzazione delle password (comprese le OTP) è effettuata hashando con l'algoritmo **PasswordBased Key Derivation Function 2** (che produce una key che può essere usata o come encryption key o come hash value) e salvate in un database, quindi non sono visibili agli amministratori di Keycloak in chiaro.

- Le credenziali d'accesso dovranno risultare sufficientemente complesse e la password avrà diversi vincoli, tutti settati dall'interfaccia grafica di Keycloak.



Authentication

Flows Bindings Required Actions Password Policy OTP Policy WebAuthn Policy WebAuthn Passwordless Policy CIBA Policy

Policy Type	Policy Value	Actions
Minimum Length	8	Delete
Not Email		Delete
Special Characters	1	Delete
Lowercase Characters	3	Delete
Uppercase Characters	1	Delete
Not Recently Used	3	Delete
Digits	1	Delete
Not Username		Delete
Maximum Length	64	Delete

Save Cancel

Add policy...

IA-5 (6): Protezione degli autenticatori. Proteggere gli autenticatori in maniera adeguata in relazione al livello di segretezza delle informazioni accessibili tramite uso dell'autenticatore.

Ciò viene assicurato tramite l'impiego di Keycloak come autenticatore, visto che fornisce un supporto alla memorizzazione delle credenziali (email, password, codici OTP) **sicuro** ed **affidabile**, memorizzandole in un **database** creato ad hoc e gestito da keycloak.

Difatti è necessaria una adeguata protezione delle credenziali di accesso in quanto il sistema informativo deve gestire importanti **dati ed operazioni istituzionali**, e dunque il livello di segretezza di esse è abbastanza elevato.

Keycloak memorizza le password come digest dell'algoritmo PBKDF2 che applica **iterativamente** una funzione **pseudorandomica** (HMAC-SHA-1 di default) all'input, utilizzando anche un salt-value.

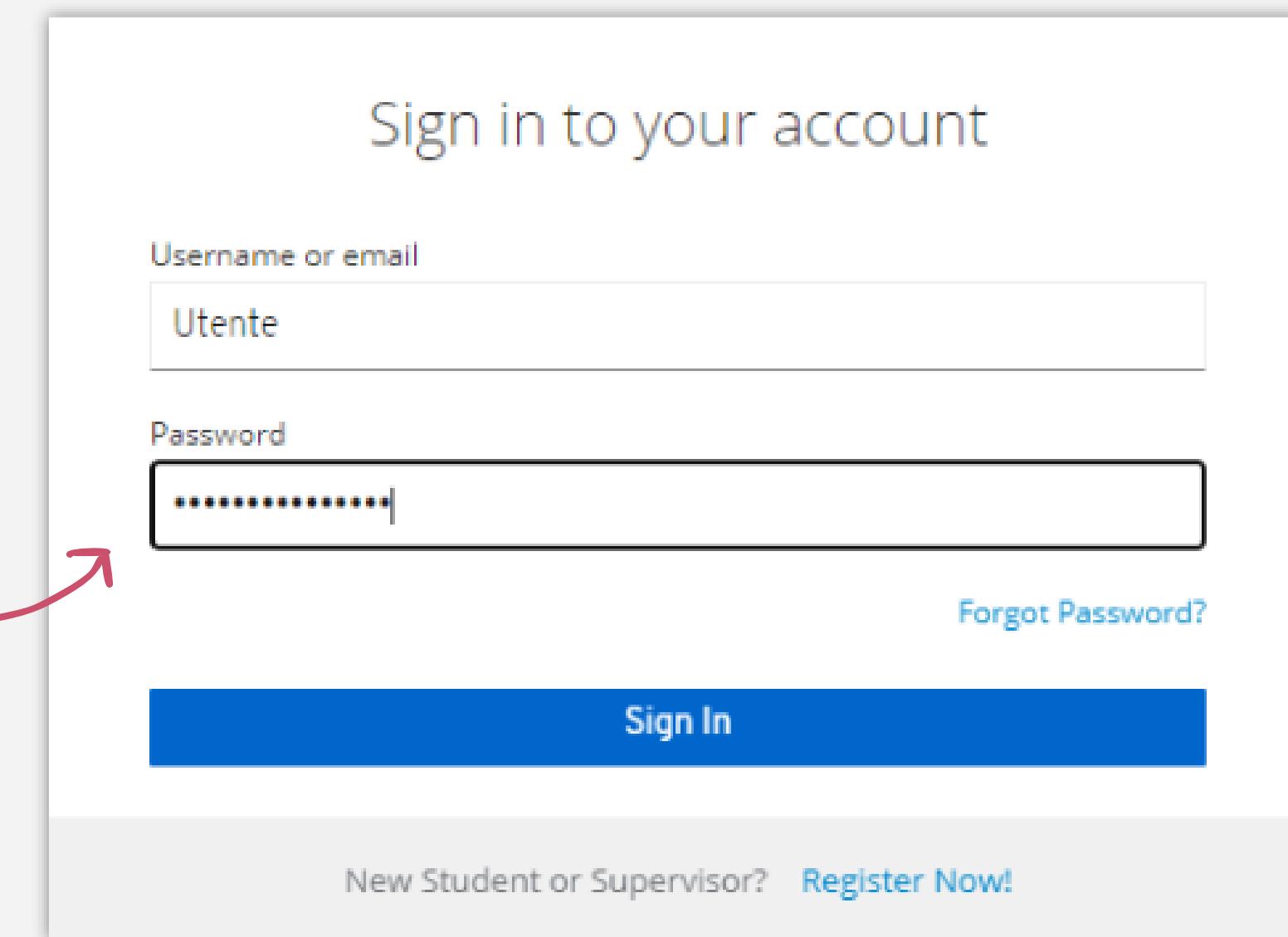
Derived Key = PBKDF2(Password, Salt, P-R Function, Iterations_num, DKLlen)

L'algoritmo è appositamente progettato per aumentare di molto la sua complessità computazionale per numeri di iterazioni molto grandi e può quindi essere molto robusto a **Brute Force Attacks**. Inoltre Aggiungere un salt-value riduce la vulnerabilità a **Rainbow Table Attacks** (quindi all'utilizzo di hash pre-calcolati).

IA-6 Authentication Feedback

IA-6: Oscurare il feedback di informazioni di autenticazione durante il processo di autenticazione per proteggere l'informazione da possibili exploit e utilizzo da individui non autorizzati.

- Tutti i caratteri digitati all'interno di form di autenticazione (quindi sia login che registrazione) sono protetti da tecniche di **oscuramento**.



Sign in to your account

Username or email

Utente

Password

.....

Forgot Password?

Sign In

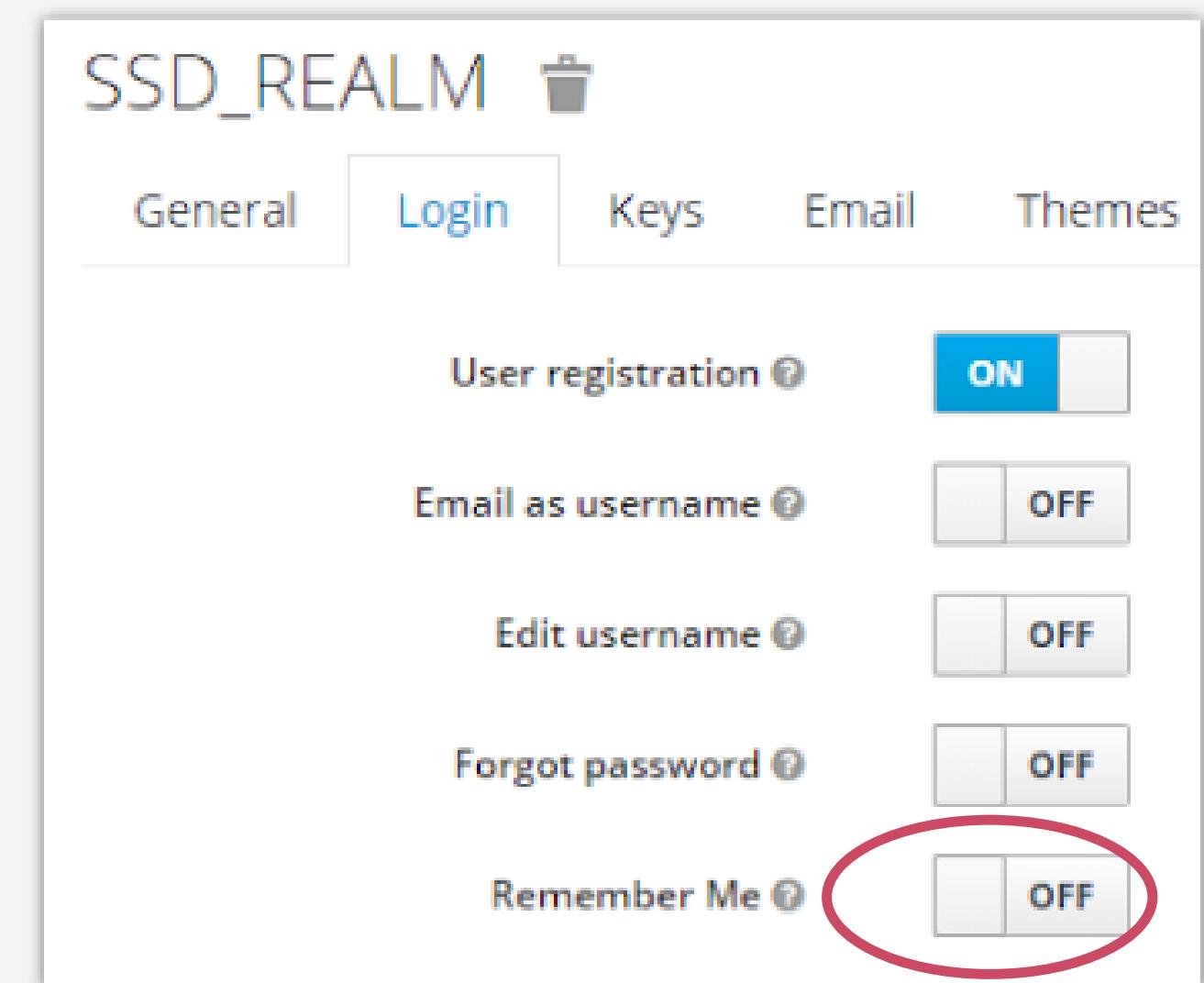
New Student or Supervisor? [Register Now!](#)

IA-11 Re-authentication

IA-11: L'organizzazione può richiedere una nuova autenticazione agli individui in determinate situazioni, come quando avviene un cambiamento del ruolo, degli autenticatori o delle credenziali, quando cambiano le policy di sicurezza, dopo un tempo fissato operiodicamente.

È richiesta una **nuova autenticazione** quando:

- Viene effettuato il **logout** dall'applicazione (Vedi AC-12)
- Allo **scadere** della sessione (Vedi AC-12)
- Alla chiusura e riapertura del Browser (Remember me OFF)



Security Controls non applicabili...

IA-2 (12): Accettazione di Personal Identity Verification (PIV)

L'applicazione non fa impiego di autenticatori fisici o logici sottoposti da agenzie federali

IA-7: Autenticazione al modulo crittografico

gli utenti dell'applicazione non hanno accesso ad alcun modulo crittografico.

IA-8: Identificazione e Autenticazione di utenti non-organizzativi.

L'applicazione non prevede l'identificazione, autenticazione e dunque accesso al servizio da parte di utenti che non fanno parte dell'organizzazione *Università di Napoli Federico II*.



9. “System and communication protection” Control Family

NIST Risk Management Framework SP 800-53 Rev. 5.1

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-1	Policy and Procedures		X	X	X
SC-2	Separation of System and User Functionality			X	X
SC-2(1)	INTERFACES FOR NON-PRIVILEGED USERS				
SC-2(2)	DISASSOCIABILITY				
SC-3	Security Function Isolation				X
SC-3(1)	HARDWARE SEPARATION				
SC-3(2)	ACCESS AND FLOW CONTROL FUNCTIONS				
SC-3(3)	MINIMIZE NONSECURITY FUNCTIONALITY				
SC-3(4)	MODULE COUPLING AND COHESIVENESS				
SC-3(5)	LAYERED STRUCTURES				
SC-4	Information in Shared System Resources			X	X
SC-4(1)	SECURITY LEVELS	W: Incorporated into SC-4.			
SC-4(2)	MULTILEVEL OR PERIODS PROCESSING				
SC-5	Denial-of-Service Protection		X	X	X
SC-5(1)	RESTRICT ABILITY TO ATTACK OTHER SYSTEMS				
SC-5(2)	CAPACITY, BANDWIDTH, AND REDUNDANCY				
SC-5(3)	DETECTION AND MONITORING				
SC-6	Resource Availability				
SC-7	Boundary Protection		X	X	X
SC-7(1)	PHYSICALLY SEPARATED SUBNETWORKS	W: Incorporated into SC-7.			
SC-7(2)	PUBLIC ACCESS	W: Incorporated into SC-7.			
SC-7(3)	ACCESS POINTS			X	X
SC-7(4)	EXTERNAL TELECOMMUNICATIONS SERVICES			X	X
SC-7(5)	DENY BY DEFAULT — ALLOW BY EXCEPTION			X	X
SC-7(6)	RESPONSE TO RECOGNIZED FAILURES	W: Incorporated into SC-7(18).			
SC-7(7)	SPLIT TUNNELING FOR REMOTE DEVICES			X	X
SC-7(8)	ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS			X	X
SC-7(9)	RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC				
SC-7(10)	PREVENT EXFILTRATION				
SC-7(11)	RESTRICT INCOMING COMMUNICATIONS TRAFFIC				
SC-7(12)	HOST-BASED PROTECTION				
SC-7(13)	ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS				

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-15(3)	DISABLING AND REMOVAL IN SECURE WORK AREAS				
SC-15(4)	EXPLICITLY INDICATE CURRENT PARTICIPANTS				
SC-16	Transmission of Security and Privacy Attributes				
SC-16(1)	INTEGRITY VERIFICATION				
SC-16(2)	ANTI-SPOOFING MECHANISMS				
SC-16(3)	CRYPTOGRAPHIC BINDING				
SC-17	Public Key Infrastructure Certificates			X	X
SC-18	Mobile Code			X	X
SC-18(1)	IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS				
SC-18(2)	ACQUISITION, DEVELOPMENT, AND USE				
SC-18(3)	PREVENT DOWNLOADING AND EXECUTION				
SC-18(4)	PREVENT AUTOMATIC EXECUTION				
SC-18(5)	ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS				
SC-19	Voice over Internet Protocol		W: Technology-specific; addressed as any other technology or protocol.		
SC-20	Secure Name/Address Resolution Service (Authoritative Source)		X	X	X
SC-20(1)	CHILD SUBSPACES		W: Incorporated into SC-20.		
SC-20(2)	DATA ORIGIN AND INTEGRITY				
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		X	X	X
SC-21(1)	DATA ORIGIN AND INTEGRITY		W: Incorporated into SC-21.		
SC-22	Architecture and Provisioning for Name/Address Resolution Service		X	X	X
SC-23	Session Authenticity			X	X
SC-23(1)	INVALIDATE SESSION IDENTIFIERS AT LOGOUT				
SC-23(2)	USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS		W: Incorporated into AC-12(1).		
SC-23(3)	UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS				
SC-23(4)	UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION		W: Incorporated into SC-23(3).		
SC-23(5)	ALLOWED CERTIFICATE AUTHORITIES				
SC-24	Fail in Known State				X
SC-25	Thin Nodes				
SC-26	Decoys				
SC-26(1)	DETECTION OF MALICIOUS CODE		W: Incorporated into SC-35.		
SC-27	Platform-Independent Applications				
SC-28	Protection of Information at Rest			X	X
SC-28(1)	CRYPTOGRAPHIC PROTECTION			X	X
SC-28(2)	OFFLINE STORAGE				
SC-28(3)	CRYPTOGRAPHIC KEYS				
SC-29	Heterogeneity				
SC-29(1)	VIRTUALIZATION TECHNIQUES				
SC-30	Concealment and Misdirection				
SC-30(1)	VIRTUALIZATION TECHNIQUES		W: Incorporated into SC-29(1).		

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
SC-30(2)	RANDOMNESS				
SC-30(3)	CHANGE PROCESSING AND STORAGE LOCATIONS				
SC-30(4)	MISLEADING INFORMATION				
SC-30(5)	CONCEALMENT OF SYSTEM COMPONENTS				
SC-31	Covert Channel Analysis				
SC-31(1)	TEST COVERT CHANNELS FOR EXPLOITABILITY				
SC-31(2)	MAXIMUM BANDWIDTH				
SC-31(3)	MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS				
SC-32	System Partitioning				
SC-32(1)	SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS				
SC-33	Transmission Preparation Integrity		W: Incorporated into SC-8.		
SC-34	Non-Modifiable Executable Programs				
SC-34(1)	NO WRITABLE STORAGE				
SC-34(2)	INTEGRITY PROTECTION AND READ-ONLY MEDIA				
SC-34(3)	HARDWARE-BASED PROTECTION		W: Moved to SC-51.		
SC-35	External Malicious Code Identification				
SC-36	Distributed Processing and Storage				
SC-36(1)	POLLING TECHNIQUES				
SC-36(2)	SYNCHRONIZATION				
SC-37	Out-of-Band Channels				
SC-37(1)	ENSURE DELIVERY AND TRANSMISSION				
SC-38	Operations Security				
SC-39	Process Isolation			X	X
SC-39(1)	HARDWARE SEPARATION				
SC-39(2)	SEPARATE EXECUTION DOMAIN PER THREAD				
SC-40	Wireless Link Protection				
SC-40(1)	ELECTROMAGNETIC INTERFERENCE				
SC-40(2)	REDUCE DETECTION POTENTIAL				
SC-40(3)	IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION				
SC-40(4)	SIGNAL PARAMETER IDENTIFICATION				
SC-41	Port and I/O Device Access				
SC-42	Sensor Capability and Data				
SC-42(1)	REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES				
SC-42(2)	AUTHORIZED USE				
SC-42(3)	PROHIBIT USE OF DEVICES		W: Incorporated into SC-42.		
SC-42(4)	NOTICE OF COLLECTION				
SC-42(5)	COLLECTION MINIMIZATION				
SC-43	Usage Restrictions				
SC-44	Detonation Chambers				
SC-45	System Time Synchronization				
SC-45(1)	SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE				
SC-45(2)	SECONDARY AUTHORITATIVE TIME SOURCE				

SC-2: Separation of System and User Functionality

Separare le funzionalità utente, inclusi i servizi dell'interfaccia utente, dalle funzionalità di gestione del sistema.

La **separazione** delle funzionalità utente da quelle di sistema avviene innanzitutto a livello **fisico** in quanto il deploy dei diversi componenti dell'applicazione in diversi container **Docker** garantisce un controllo maggiore sulle funzionalità che questi ultimi possono esporre.

Inoltre, a livello **logico** sono state realizzate **due interfacce grafiche** (studente/supervisor e admin) **distinte** che racchiudono, rispettivamente, le funzionalità utente e le funzionalità di sistema e ne regolamentano l'utilizzo.

SC-4: Information in Shared System Resources

Prevenire il trasferimento di informazioni non autorizzato ed involontario tramite risorse di sistema condivise.

L'accesso alle risorse di sistema condivise è regolamentato ed autorizzato dal sistema di **controllo degli accessi** implementato da **Keycloak**. Grazie a quest'ultimo, un utente potrà accedere solo ed esclusivamente alle informazioni alle quali ha il **permesso** di accedere. Nella nostra applicazione il controllo degli accessi è **Role Based**.

SC-5: Denial-Of-Service protection

Limitare o proteggersi dagli effetti indesiderati causati da attacchi DoS impiegando adeguate contromisure.

L'utilizzo dell'API Gateway Nginx come **unico punto di accesso** per l'applicazione, ci ha permesso di configurare quest'ultimo in modo da limitare il numero di richieste in un determinato lasso di tempo effettuabili da un singolo utente. In questo modo si **mitiga il rischio** di attacchi di tipo **DoS**.

Inoltre, per **limitare** gli effetti indesiderati causati da attacchi DoS, i container Docker sono stati configurati in maniera tale da riavviarsi in caso di crash.

```
http {  
    include      mime.types;  
    default_type application/octet-stream;  
  
    limit_req_zone $binary_remote_addr zone=limitreqsbyaddr:20m rate=10r/s;
```

```
services:  
  back-end:  
    build:  
      context: ./back-end  
      dockerfile: Dockerfile  
    ports:  
      - 8081:8081  
    restart: on-failure  
    environment:  
      DB_URL: jdbc:mysql://mysql:ssd_db  
      DB_USERNAME: ${MYSQL_USER}  
      DB_PASSWORD: ${MYSQL_PASSWORD}  
    depends_on:
```

SC-7: Boundary protection

Il sistema deve:

- Monitorare e controllare sia le comunicazioni in arrivo sulle interfacce esterne del sistema e sia le comunicazioni in arrivo sulle interfacce chiave interne al sistema
- Implementare sottoreti per componenti pubblicamente accessibili che sono fisicamente/logicamente separate dalle reti interne all'organizzazione
- Connettersi a reti o sistemi esterni soltanto mediante interfacce gestite che consistono in dispositivi di protezione perimetrale configurati secondo un'architettura di sicurezza organizzativa

I diversi container **Docker** sui quali sono istanziati i componenti dell'applicazione comunicano tra di loro utilizzando una **rete privata virtuale** non accessibile dall'esterno. In più, le comunicazioni da e verso l'esterno sono controllate da stringenti regole di **firewalling**.

SC-7 (3): Access points

Limitare il numero di connessioni al sistema dall'esterno.

L'utilizzo di **Nginx** come unico punto di accesso all'applicazione ci consente di **limitare**, attraverso un'opportuna configurazione, il numero massimo di **connessioni simultanee** provenienti dall'esterno.

```
http {
    include      mime.types;
    default_type application/octet-stream;

    limit_req_zone $binary_remote_addr zone=limitreqsbyaddr:20m rate=10r/s;

    proxy_read_timeout 300;
    proxy_connect_timeout 300;
    proxy_send_timeout 300;
```

SC-7 (5): Deny by default - Allow exception

Impedire di default qualsiasi tentativo di comunicazione e consenti il traffico mediante la definizione di eccezioni (whitelisting).

La piattaforma **DigitalOcean** permette di configurare in pochi click un semplice firewall per il controllo del traffico di rete da e verso la macchina sulla quale viene eseguito il deploy dell'applicazione. Grazie al **firewall** sarà possibile **impedire** qualsiasi tentativo di comunicazione con la macchina che non rispetti le **regole** da noi definite.

Firewall configuration



Inbound Rules

Set the Firewall rules for incoming traffic. Only the specified ports will accept inbound connections. All other traffic will be dropped.

Type	Protocol	Port Range	Sources	
SSH	TCP	22	All IPv4 All IPv6	Delete
HTTPS	TCP	443	All IPv4 All IPv6	Delete
HTTP	TCP	80	All IPv4 All IPv6	Delete
ICMP	ICMP		All IPv4 All IPv6	Delete
New rule				

Le sole ed uniche connessioni in **ingresso** che vengono **accettate** nel sistema sono le connessioni **SSH** (accesso remoto alla macchina), **HTTPS** e **HTTP** (per l'accesso alla web application) e **ICMP** per questioni di monitoring.

Firewall configuration



Outbound Rules

Set the Firewall rules for outbound traffic. Outbound traffic will only be allowed to the specified ports. All other traffic will be blocked.

Type	Protocol	Port Range	Destinations	
ICMP	ICMP		All IPv4 All IPv6	More ▾
All TCP	TCP	All ports	All IPv4 All IPv6	More ▾
All UDP	UDP	All ports	All IPv4 All IPv6	More ▾
New rule ▾				

Le sole ed uniche connessioni in **uscita** che vengono **permesse** sono le connessioni **ICMP** e tutte le connessioni **TCP** o **UDP**.

SC-7 (8) : Route traffic to authenticated proxy servers

Instradare il traffico dall'interno all'esterno, e viceversa, mediante l'utilizzo di proxy server autenticati posti in corrispondenza delle interfacce.

Il compito di **Nginx** è proprio quello di agire da **reverse-proxy** ponendosi così da **intermediario** tra i client e il server. In questo modo i client faranno richieste ad un unico punto che poi si occuperà di instradarle verso l'opportuno servizio.

```
front-end:  
  build:  
    context: ./front-end  
    dockerfile: Dockerfile  
  restart: on-failure  
  ports:  
    - 80:80  
    - 443:443  
  depends_on:  
    - back-end  
  volumes:  
    - ./nginx.conf:/etc/nginx/nginx.conf
```

SC-8: Transmission Confidentiality and Integrity

Proteggere la confidenzialità e l'integrità delle comunicazioni

Come suggerisce l'enhancement 1, al fine di garantire la confidenzialità e l'integrità delle comunicazioni, ci si serve dei meccanismi di **crittografia**. L'utilizzo di **TLS**, in tal senso, garantisce la crezione di un **tunnel crittografico** tra client e server che assicura la **confidenzialità** del traffico.

```
include /etc/nginx/mime.types;
listen      443 ssl;
server_name bandiunina.it;

ssl_certificate      /etc/letsencrypt/live/bandiunina.it/fullchain.pem;
ssl_certificate_key  /etc/letsencrypt/live/bandiunina.it/privkey.pem;

add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
#add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'";
add_header X-XSS-Protection: "1; mode=block";

proxy_set_header X-Forwarded-For $proxy_protocol_addr;
proxy_set_header X-Forwarded-Proto $scheme;
proxy_set_header Host $host;
```

SC-10: Network Disconnect

Terminare la connessione di rete associata ad una sessione di comunicazioni al termine della sessione o successivamente ad un periodo di inattività

I framework **SpringBoot** utilizzato per il backend si occupa in automatico di **terminare** le connessioni di rete al termine delle sessioni ad esse associate. In più l'API Gateway **Nginx** è stato configurato in modo da **chiudere** le connessioni attive allo scadere di un certo tempo di **timeout**.

```
proxy_read_timeout 300;  
proxy_connect_timeout 300;  
proxy_send_timeout 300;
```

SC-12: Cryptographic Key Establishment and Management

Stabilire e gestire le chiavi crittografiche, nel caso in cui venga impiegata la crittografia all'interno del sistema, in accordo con i requisiti di gestione delle chiavi definiti dall'organizzazione riguardanti generazione, distribuzione, conservazione, accesso e distruzione delle chiavi.

Le chiavi ed i certificati, necessari per il funzionamento di TLS, vengono gestiti e protetti dal modulo software **certbot**. L'**accesso** a questi ultimi da parte di Nginx viene realizzato **condividendo** un'area di **memoria** tra i container Docker in cui sono in esecuzione rispettivamente Nginx e certbot.

```
ssl-service:  
  image: certbot/certbot:v1.23.0  
  volumes:  
    - ./certbot/www/:/var/www/certbot/:rw  
    - ./certbot/conf:/etc/letsencrypt/:rw  
  depends_on:  
    - front-end  
  command:  
    - renew  
    #- certonly  
    #- --webroot  
    #- -W  
    #- /var/www/certbot/  
    #- --email=uninabandi@libero.it  
    #- --agree-tos  
    #- --no-eff-email  
    #- -d  
    #- bandiunina.it
```

SC-13: Cryptographic Protection

Determinare gli ambiti di impiego della crittografia e specificare, per ogni utilizzo, i tipi di crittografia.

Le connessioni tra client e server avvengono mediante il protocollo **TLS 1.3** e sono, quindi, cifrate grazie all'algoritmo di crittografia **AES-128**. Le restanti connessioni di rete avvengono tra i container docker all'interno di una **rete privata**. Pertanto, per queste ultime si è deciso di non utilizzare la crittografia.



SC-17: Public Key Infrastructure Certificates

- Emettere certificati a chiave pubblica *in base a politiche definite dall'organizzazione oppure ottenere certificati a chiave pubblica da un fornitore approvato*
 - *Includere solo trust anchor approvate nei trust store o archivi di certificati gestiti dall'organizzazione*
-

I certificato a chiave pubblica da noi utilizzato viene emesso dalla **Certification Authority Let's Encrypt**. Quest'ultima, oltre a curarsi dell'emissione, si occupa anche della verifica e del rinnovo dei certificati. Le **richieste** di emissione, verifica e rinnovo vengono effettuate in automatico dal gestore di certificati **certbot** utilizzando il protocollo specifico **ACME**.



SC-18: Mobile Code



- *Definire il codice mobile accettabile e non e le tecnologie utilizzate*
- *Autorizzare, monitorare e controllare l'uso di codice mobile all'interno del sistema*

L'applicazione da noi implementata **non fa uso** in alcun modo **di codice mobile** e non ne consente in alcun modo l'esecuzione. Inoltre l'utilizzo di **React** lato frontend consente di **mitigare** il rischio di attacchi **XSS** grazie al **parsing** ed all'**escaping** automatico del codice HTML che compone le pagine.

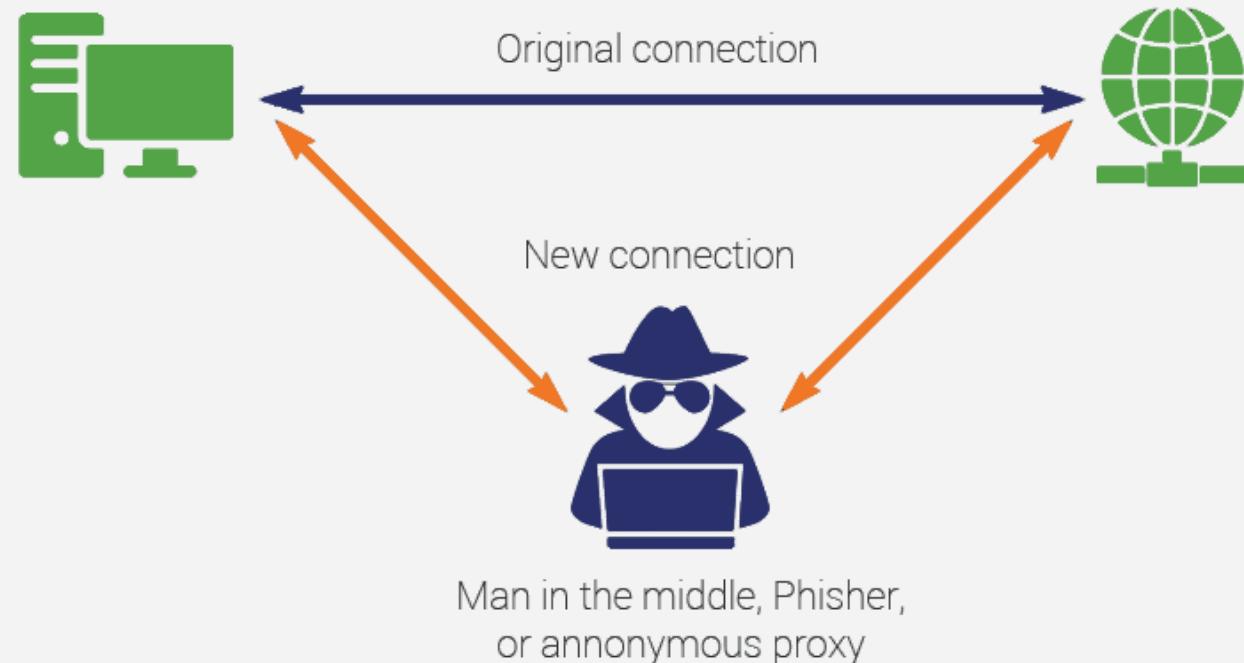
```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header Content-Security-Policy "default-src 'self'; frame-ancestors 'self'; script-src 'self' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; img-src 'self' 'unsafe-inline'";
add_header X-XSS-Protection: "1; mode=block";
```

Inoltre l'aggiunta tramite il Server Nginx del **XSS protection header** e del **CSP** header impedisce l'esecuzione di codice proveniente da fonti “non affidabili”.

SC-23: Session Authenticity

Proteggere l'autenticità delle sessioni di comunicazione

L'utilizzo di **TLS**, e quindi dei **certificati** a chiave pubblica, garantisce l'autenticazione del server e **previene** gli attacchi di tipo **man-in-the-middle**. Inoltre i **token di accesso** associati ad una sessione sono **gestiti** e **validati** in automatico da **Keycloak**. Ciò **mitiga** il rischio di attacchi di **session-hijacking**.



SC-28: Protection of Information at Rest

Proteggere la confidenzialità e l'integrità delle informazioni nello stato di riposo definite dall'organizzazione

Le informazioni da proteggere nello stato di riposo sono:

- **Credenziali degli utenti:** conservate e protette da Keycloak
- **Credenziali di accesso al database:** conservate in forma crittografata (**SC-28(1)**) e protette da Vault
- **Dati funzionali all'applicazione:** conservati e protetti dal database MySQL

SC-39: Process Isolation

Mantenere un dominio d'esecuzione diverso per ogni processo che esegue all'interno del sistema.

I diversi processi in esecuzione all'interno del sistema sono istanziati su **container Docker** distinti. In questo modo, ogni processo esegue in un dominio d'esecuzione a sé stante e comunicherà con gli altri processi soltanto mediante **interfacce** da noi definite e controllate.

Overview e ulteriori Controlli

“System and Communications Protection” controls family

NIST Risk Management Framework SP 800-53 Rev. 5.1

I controlli applicati seguendo le linee guida definite dal NIST consentono di raggiungere una protezione del sistema complessivo fino ad un livello **moderate**, eccezion fatta per :

Controlli non realizzati:

- **SC-21:** Secure name/address resolution service (recursive or caching resolver)

Controlli non implementabili:

- **SC-7(4) :** External telecommunications services
- **SC-20:** Secure name/address resolution service (authoritative source)
- **SC-22:** Architecture and provisioning for name/address resolution service



7. “Audit And Accountability” Control Family

NIST Risk Management Framework SP 800-53 Rev. 5.1

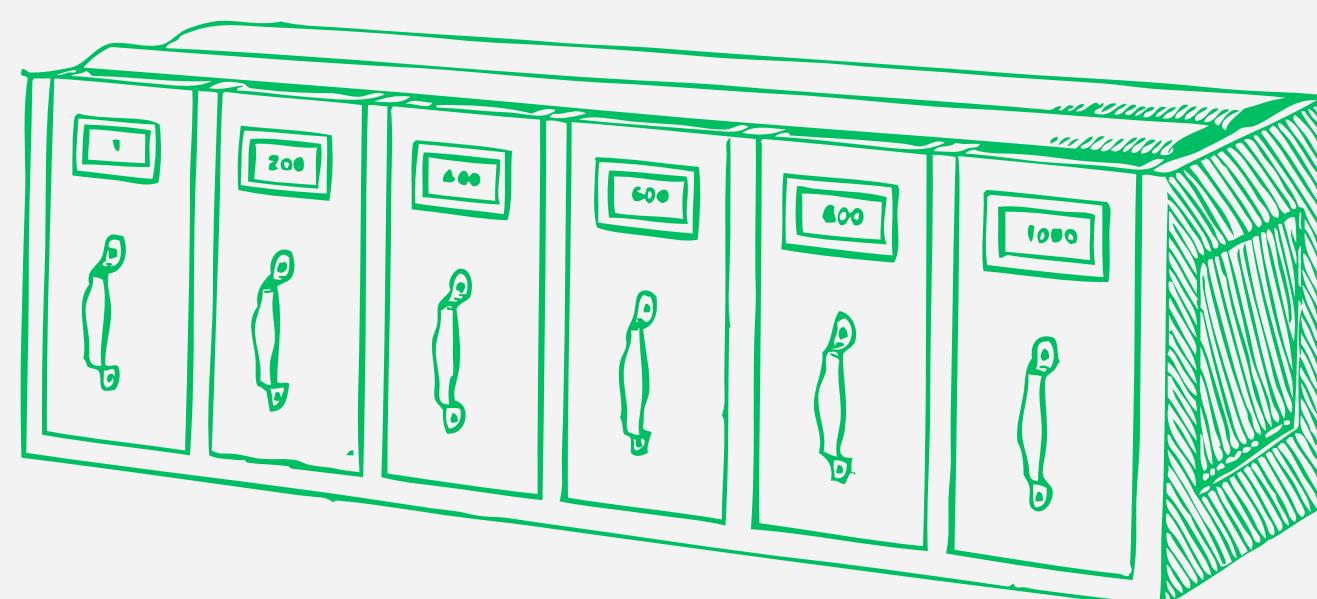
Control Number	Control Name Control Enhancement Name	Privacy Control Baseline	Security Control Baselines			Control Number	Control Name Control Enhancement Name	Privacy Control Baseline	Security Control Baselines		
			Low	Mod	High				Low	Mod	High
AU-1	Policy and Procedures	X	X	X	X	AU-8(1)	Synchronization with Authoritative Time Source		W: Moved to SC-45(1).		
AU-2	Event Logging	X	X	X	X	AU-8(2)	Secondary Authoritative Time Source		W: Moved to SC-45(2).		
AU-2(1)	Compilation of Audit Records from Multiple Sources		W: Incorporated into AU-12.			AU-9	Protection of Audit Information		X	X	X
AU-2(2)	Selection of Audit Events by Component		W: Incorporated into AU-12.			AU-9(1)	Hardware Write-once Media				
AU-2(3)	Reviews and Updates		W: Incorporated into AU-2.			AU-9(2)	Store on Separate Physical Systems or Components				X
AU-2(4)	Privileged Functions		W: Incorporated into AC-6(9).			AU-9(3)	Cryptographic Protection				X
AU-3	Content of Audit Records		X	X	X	AU-9(4)	Access by Subset of Privileged Users			X	X
AU-3(1)	Additional Audit Information			X	X	AU-9(5)	Dual Authorization				
AU-3(2)	Centralized Management of Planned Audit Record Content		W: Incorporated into PL-9.			AU-9(6)	Read-only Access				
AU-3(3)	Limit Personally Identifiable Information Elements	X				AU-9(7)	Store on Component with Different Operating System				
AU-4	Audit Log Storage Capacity		X	X	X	AU-10	Non-repudiation				X
AU-4(1)	Transfer to Alternate Storage					AU-10(1)	Association of Identities				
AU-5	Response to Audit Logging Process Failures		X	X	X	AU-10(2)	Validate Binding of Information Producer Identity				
AU-5(1)	Storage Capacity Warning				X	AU-10(3)	Chain of Custody				
AU-5(2)	Real-time Alerts				X	AU-10(4)	Validate Binding of Information Reviewer Identity				
AU-5(3)	Configurable Traffic Volume Thresholds					AU-10(5)	Digital Signatures		W: Incorporated into SI-7.		
AU-5(4)	Shutdown on Failure					AU-11	Audit Record Retention	X	X	X	X
AU-5(5)	Alternate Audit Logging Capability					AU-11(1)	Long-term Retrieval Capability				
AU-6	Audit Record Review, Analysis, and Reporting		X	X	X	AU-12	Audit Record Generation		X	X	X
AU-6(1)	Automated Process Integration			X	X	AU-12(1)	System-wide and Time-correlated Audit Trail				X
AU-6(2)	Automated Security Alerts		W: Incorporated into SI-4.			AU-12(2)	Standardized Formats				
AU-6(3)	Correlate Audit Record Repositories			X	X	AU-12(3)	Changes by Authorized Individuals				X
AU-6(4)	Central Review and Analysis					AU-12(4)	Query Parameter Audits of Personally Identifiable Information				
AU-6(5)	Integrated Analysis of Audit Records				X	AU-13	Monitoring for Information Disclosure				
AU-6(6)	Correlation with Physical Monitoring				X	AU-13(1)	Use of Automated Tools				
AU-6(7)	Permitted Actions					AU-13(2)	Review of Monitored Sites				
AU-6(8)	Full Text Analysis of Privileged Commands					AU-13(3)	Unauthorized Replication of Information				
AU-6(9)	Correlation with Information from NonTechnical Sources					AU-14	Session Audit				
AU-6(10)	Audit Level Adjustment		W: Incorporated into AU-6.			AU-14(1)	System Start-up				
AU-7	Audit Record Reduction and Report Generation			X	X	AU-14(2)	Capture and Record Content		W: Incorporated into AU-14.		
AU-7(1)	Automatic Processing			X	X	AU-14(3)	Remote Viewing and Listening				
AU-7(2)	Automatic Sort and Search		W: Incorporated into AU-7(1).			AU-15	Alternate Audit Logging Capability		W: Moved to AU-5(5).		
AU-8	Time Stamps		X	X	X	AU-16	Cross-Organizational Audit Logging				
						AU-16(1)	Identity Preservation				
						AU-16(2)	Sharing of Audit Information				
						AU-16(3)	Disassociability				

AU-1: Policy e Procedure

La famiglia di controlli **AU** del **NIST** rappresenta un pilastro essenziale nella gestione della sicurezza dell'informazione, concentrando la sua attenzione sulla registrazione, l'analisi e la responsabilizzazione delle attività legate alla sicurezza dei sistemi informativi.

La sua importanza risiede nella capacità di offrire un quadro robusto e dettagliato per garantire la **trasparenza** e la **tracciabilità** delle azioni all'interno di un ambiente IT.

Attraverso questi controlli, le organizzazioni possono non solo **identificare** e **rispondere** tempestivamente agli eventi di **sicurezza**, ma anche **imparare** dalle attività **passate** per migliorare proattivamente la loro postura di sicurezza.



AU-2: Event Logging

- a) Identificare i tipi di eventi che il sistema è in grado di registrare a supporto della funzione di audit;
 - b) Coordinare la funzione di registrazione degli eventi con altre entità organizzative che richiedono informazioni relative all'audit per guidare i criteri di selezione degli eventi da registrare;
 - c) Specificare i seguenti tipi di eventi da registrare nel sistema: [Assegnazione: tipi di eventi definiti dall'organizzazione (sottoinsieme dei tipi di eventi definiti in AU-2a.) insieme alla frequenza di registrazione (o alla situazione che richiede) per ciascun tipo di evento identificato];
 - d) Fornire una motivazione per cui i tipi di eventi selezionati per la registrazione sono ritenuti adeguati a supportare le indagini a posteriori sugli incidenti;
 - e) Rivedere e aggiornare i tipi di eventi selezionati per il logging [Assegnazione: frequenza definita dall'organizzazione].
-

AU-2: Event Logging

Compilation of audit records from multiple sources

- **Keycloak:** L'IAM consente di tener traccia di tutti i **login** (di successo o fallimentari), della registrazione da parte degli utenti, delle azioni effettuate sui vari account (**EDIT**, **DELETE**...) così come le azioni compiute dall'amministratore e la rilevazione dei tentativi di assalto **brute-force**.
- **Nginx:** E' possibile configurare Nginx in maniera tale da registrare qualsiasi richiesta in **entrata** che viene opportunamente redirezionata. Esso, inoltre si occupa di loggare anche tutti gli **errori** associati alle richieste effettuate così come eventuali **elaborazioni** non corrette.
- **Vault:** Esso registra l'azione di **sealing/unsealing** così come le modifiche apportate ai vari **engine** che è possibile abilitare e modificare, la generazione di **token** e i **login** effettuati sulla dashboard corrispondente.

AU-3: Contenuto dei record di auditing

Assicurarsi che le registrazioni di audit contengano informazioni che stabiliscano quanto segue:

- a) Quale tipo di evento si è verificato;
- b) Quando si è verificato l'evento;
- c) Dove si è verificato l'evento;
- d) Fonte dell'evento;
- e) Esito dell'evento;
- f) Identità di individui, soggetti o oggetti/entità associati all'evento.

Keycloak utilizza un formatter di logging basato sul framework JBoss Logging che genera i record di testo il cui formato è:

%d{yyyy-MM-dd HH:mm:ss,SSS} %-5p [%c] (%t) %s%e%n

- **%-5p** indica che vengono loggati tutti i livelli
- **%c** Visualizza il nome della categoria di registro.
- **%t** nome del thread
- **%s** è il messaggio di log
- **%e** è il messaggio dell'eccezione

AU-3: Contenuto dei record di auditing

Formato dei log di **Nginx**:

```
93.148.109.100 - - [14/Dec/2023:16:12:54 +0000] "GET /api/callForApplications/guest/getLast HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"  
93.148.109.100 - - [14/Dec/2023:16:13:09 +0000] "GET /api/callForApplications/guest/getLast HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"  
/var/log/nginx #
```

Formato dei log di **Vault**:

```
/vault/data/audit # cat logs.txt  
{"time": "2023-12-19T11:38:20.046095639Z", "type": "request", "auth": {"token_type": "default"}, "request": {"id": "4fbf738b-0b0b-d736-4ced-7557343cb1ba", "operation": "update", "namespace": {"id": "root"}, "path": "sys/audit/test"}},  
{"time": "2023-12-19T11:38:20.047656564Z", "type": "response", "auth": {"client_token": "hmac-sha256:3ffa24d2d118ecb31d733c53b71eb7ab910650b9be1fcc76ef7bde14b408d78a", "accessor": "hmac-sha256:b67e383c36d6242ed85fdc8fa903710f057f6569395eee10fd5c503e6b759289", "display_name": "root", "policies": ["root"], "token_policies": ["root"], "policy_results": {"allowed": true, "granting_policies": [{"name": "root", "namespace_id": "root", "type": "acl"}]}}, "token_type": "service", "token_issue_time": "2023-10-20T18:42:58Z"}, "request": {"id": "89174057-042a-5ca5-a932-13a81520d381", "client_id": "ODHqvq2D77kL2/JTPSZkTMJbkFVmUuOTzMi0"}
```

Le entries dei log mostrate contengono le informazioni richieste dal **Security Control**.

AU-3:(1): Informazioni di auditing addizionali

Generare record di auditing contenenti informazioni aggiuntive:

In particolare grazie ai log specificati in **Nginx** è possibile tener traccia del destinatario delle richieste effettuate (Keycloak, back-end, Admin-back-end).

Allo stesso modo i log di **Keycloak** consentono di distinguere ed identificare utenti che realizzano specifiche operazioni.

AU-8: Time Stamps

- a) Utilizzare un clock interno per la generazione dei timestamps dei log records.
 - b) Registrare i timestamp per i record di audit che soddisfano [granularità definita dall'organizzazione della misurazione del tempo] e che utilizzano il Coordinated Universal Time, hanno un offset temporale locale fissato dal Coordinated Universal Time o che includono l'offset orario locale come parte del timestamp.
-

Tutti i log al loro interno posseggono il timestamp con granularità a microsecondi e sono generati a partire dal **UNIX-CLOCK**.

AU-9: Protezione delle informazioni di auditing

- a) Proteggere le informazioni di audit e gli strumenti di registrazione degli audit da accessi, modifiche e cancellazioni non autorizzati;
 - b) Avvisare [Assegnazione: personale o ruoli definiti dall'organizzazione] in caso di rilevamento di accesso, modifica o cancellazione non autorizzati delle informazioni di audit.
-

Tutti i file di log sono accessibili sono all'utente amministratore proprietario della **Droplet** deployata, in quanto risulta l'unico in possesso delle credenziali di accesso alla piattaforma e ai singoli containers. Il che porta anche al soddisfacimento del controllo **AU-9(4): ACCESS BY SUBSET OF PRIVILEGED USERS**

AU-11: Conservazione dei record di Audit

Conservare i record di audit per [periodo di tempo definito dall'organizzazione coerente con la politica di conservazione dei record] per fornire supporto per le indagini successive agli incidenti e per soddisfare i requisiti di conservazione delle informazioni regolamentari e organizzative.

I record generati da **Nginx** e **Vault** risultano persistenti mentre quelli generati da **Keycloak** presentano una data di scadenza configurabile dalla console di amministrazione.

AU-12: Generazione dei record di Audit

- a) Fornire la capacità di generare record di audit per i tipi di eventi che il sistema è in grado di verificare, come definito in AU-2a sui componenti del sistema;
 - b) Consentire a [personale o ruoli definiti dall'organizzazione] di selezionare i tipi di eventi che devono essere registrati da componenti specifici del sistema;
 - c) Generare record di audit per i tipi di evento definiti in AU-2c che includano il contenuto del record di audit definito in AU-3.
-

Il controllo è stato implementato così come mostrato in **AU-2**. Inoltre, grazie al soddisfacimento del controllo **AU-8** con cui i log vengono generati a partire dallo stesso clock risulta verificato anche il controllo **AU-12(1)** (**Compilare i record di audit da [componenti di sistema definiti dall'organizzazione] in una traccia di audit a livello di sistema (logico o fisico) correlata al tempo**)

Overview e ulteriori Controlli

“Audit And Accountability” Control Family

NIST Risk Management Framework SP 800-53 Rev. 5.1

I controlli applicati seguendo le linee guida definite dal NIST consentono di raggiungere una protezione del sistema complessivo fino ad un livello moderate, eccezion fatta per :

Controlli non realizzati:

- **AU-5: RESPONSE TO AUDIT LOGGING PROCESS FAILURES:**

- a) *Avvisare [personale o ruoli definiti dall'organizzazione] entro [periodo di tempo definito dall'organizzazione] in caso di errore del processo di registrazione dell'audit;*
b) *Eseguire le seguenti azioni aggiuntive: [azioni aggiuntive definite dall'organizzazione].*

- **AU-6: AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING**

- a) *Rivedere e analizzare i record di audit del sistema [frequenza definita dall'organizzazione] per le indicazioni di [attività inappropriata o insolita definita dall'organizzazione] e il potenziale impatto dell'attività inappropriata o insolita;*
b) *Riferire i risultati a [personale o ruoli definiti dall'organizzazione];*
c) *adeguare il livello di revisione, analisi e comunicazione dei record di audit all'interno del sistema in caso di cambiamento del rischio sulla base di informazioni in materia di applicazione della legge, informazioni di intelligence o altre fonti di informazione credibili.*

BANDIUNINA

Secure Systems Design

Thanks for
your attention !



UNIVERSITÀ DEGLI STUDI DI NAPOLI
FEDERICO II