

## Autenticazione

Quando si vuole creare o partecipare ad una partita è necessario disporre di un account. L'accesso è la prima operazione che viene richiesta quando si avvia l'applicativo "Il Paroliere".

Per eseguire l'accesso è necessario possedere un account; un account è formato da:

- **nickname**: pseudonimo per identificare una persona;
- **password**: password di sicurezza che solo l'utente conosce;
- **mail**: indirizzo di recapito per l'utente;
- **data autenticazione**: identifica mediante una data il momento in cui è stato attivato l'account.

nickname	password	mail	data autenticazione
Gandalf	hjfgfhsjghfjkghd	gandalf19@gmail.com	12/02/2019

Non è buona norma memorizzare le password in chiaro all'interno del DB; è necessario utilizzare un sistema per criptare la password senza che possa essere svelata. Si necessita quindi di un algoritmo non reversibile.

Esempi di algoritmi non reversibili sono: **MD5** e **SHA256**.

andare a memorizzare la password mediante un algoritmo non reversibile rende "impossibile" (molto difficoltoso) risalire alla password originale mantenendo memorizzata all'interno del DB una stringa di lunghezza costante (formata da ? caratteri).

(La rappresentazione degli utenti potrà variare in base a campi che le statistiche richiedono).

## Registrazione

Mediante un'apposita schermata, dell'interfaccia "Il Paroliere", sarà possibile immettere i propri dati affinché la registrazione parta.

Si andranno ad inserire:

- **nickname**: (univoco nel DB degli utenti);
- **mail**: composta da `<indirizzo>@<dominio>.<it/org/com/...>`  
(univoca nel DB degli utenti);
- **password**: lunghezza minima di 8 caratteri ( ed altre caratteristiche se si volesse portare l'utente alla scelta di una password sicura).

Una volta inseriti si andrà a cliccare su di un apposito bottone (“Completa Registrazione”) dove sarà possibile completare la registrazione.

Cliccato sull'apposito bottone non si sarà ufficialmente nel DB degli utenti registrati: bisognerà confermare, entro 10 minuti dall'invio dei dati, la propria identità attraverso la verifica via mail.

Viene di fatti recapitata una mail col seguente messaggio:

da:	<a href="mailto:IlParoliere@noreply.com">IlParoliere@noreply.com</a>
oggetto:	completamento registrazione
Gentile, la preghiamo di completare la registrazione al servizio “Il Paroliere” facendo un click su questo link: <a href="https://www.conferma.it/username/il_paroliere/confirm.html">https://www.conferma.it/username/il_paroliere/confirm.html</a>  In questo modo potrai iniziare a giocare al gioco online “Il Paroliere”.	

Cliccando sul link (o anche un bottone) sarà possibile completare la registrazione.

## Reset Password

Può capitare che si dimentichi la propria password. Il paroliere mette a disposizione un servizio per reimpostare la password.

All'avvio del client “Il Paroliere” sarà presente (in basso a destra... bho) la voce “reimposta password”; cliccandoci sopra si verrà reindirizzati in una schermata dove, inserendo l'indirizzo email/username sarà possibile ripristinare la password.

Inserita la mail/username verrà inviata una password temporanea tramite la quale accedere al servizio per reimpostare la password.

(sarebbe comodo fare l'MD5 sulla vecchia password e sovra-scriverla)

## Casi Estremi

Se un utente appena registrato che non ha ancora confermato via mail la propria identità non ricorda la password può usufruire comunque del servizio di reimpostazione della password.

(nonostante sia un completo deficiente; mettendo a repentaglio la sicurezza del proprio account)

## Osservazioni

Sicuramente sarà necessaria una scissione fra **Utenti Autenticati** e **Utenti in attesa di autenticazione**: un utente non autenticato passa come autenticato se conferma la mail.

Un utente è autenticato nel momento in cui si trova fra gli utenti autenticati. Gli utenti non autenticati sono in attesa che vengano autenticati (via mail) e presentano la data e l'ora in cui hanno iniziato la procedura di registrazione.

nickname	password	mail	data iscrizione
Gandalf	hjfgfhsjghfjkghd	gandalf19@gmail.com	12/02/2019 - 14:20

Quando si ha la conferma dell'autenticazione si inseriscono i dati relativi all'utente non autenticato nella sezione utenti autenticati.

## Implementazione

Affinché risulti semplice ed efficace è necessario adottare sistemi di astrazione; uno dei sistemi di astrazione che SQL fornisce sono le viste.

è possibile creare anche viste parametriche.

è possibile creare transazioni, nel caso di passaggi critici all'interno del gioco/registrazione.

Le operazioni verranno quindi incapsulate all'interno di viste affinché all'interno del programma non venga mai citata la struttura del DB.

Così facendo è possibile cambiare la struttura del DB (e/o le viste senza) aggiornare i client.

Saranno necessari funzionalità come:

- **ResettaPassword** ( nickname/mail )
- **VisualizzaDataAutenticazione** ( nickname/mail )
- **VerificaUtente** ( nickname/mail, password )
- **RegistraUtente** ( nickname, mail, password )
- **èAutenticato** ( nickname/mail )
- ecc...

Alla creazione dello schema è utile impostare dei vincoli affinché non sia possibile, neanche forzatamente, inserire dati che causerebbero inconsistenza nel DB.

La rimozione per utenti che non hanno rispettato i limiti di tempo per l'autenticazione avverrà mediante una “*routine SQL/function trigger*”, che provvederà a cancellare coloro che hanno superato i limiti di tempo imposti.

(routine impostata per essere eseguita ogni 10 minuti (?))

PostgreSQL non implementa nativamente routine o function trigger basate sul tempo (es. ogni ora, ogni 10 minuti, ecc... ) è necessario adottare componenti esterni, come **cron** o **pg\_agent**.

(da verificare se è possibile adottare questi componenti esterni)

I vincoli presenti sugli attributi dovrebbero essere inseriti separatamente allo schema, poiché si perderebbe di vista la leggibilità del codice SQL. Inoltre, essendo possibile assegnare nomi ai vincoli, diverrebbe più chiaro e leggibile il significato di un vincolo.

Il server mail si collegherà all'account istituzionale fornitoci per operare nel progetto; avrà le seguenti caratteristiche:

- **mail:** la mail verrà scritta su di un file e caricata per completare il testo del messaggio. Così facendo il testo del messaggio sarà indipendente dal servizio di invio mail e facilmente modificabile;
- **servizio di invio:** il servizio di invio mail adottato è ovviamente SMTP;
- **invio mail di conferma:** quando nell'applicativo "Il Paroliere" si andrà ad effettuare la registrazione si provvederà ad inviare la mail di conferma:
  - utilizzando "Il Paroliere": una volta confermato l'inserimento dell'utente nella sezione "utenti da autenticare" richiamerà il servizio di invio mail;
  - utilizzando il server mail: il server mail ciclicamente visualizza se nel DB sono presenti utenti da utenticare e ciclicamente fa partire delle mail (ogni 5 minuti (?)) per evitare che alcuni account non vengano autenticati in tempo);
  - altri sistemi attualmente sconosciuti.
- **autenticazione:** la mail conterrà un link sul quale cliccare affinché sia possibile autenticare l'account; il link porterà o ad una richiesta SQL per l'avvenuta autenticazione o ad una pagina di conferma (server HTTP)